<table>
<thead>
<tr>
<th>Chapter</th>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Getting Started</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>1.1 Requirements</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>1.2 Installation</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>1.3 Upgrades &amp; Maintenance</td>
<td>53</td>
</tr>
<tr>
<td></td>
<td>1.4 Additional Configuration Options</td>
<td>74</td>
</tr>
<tr>
<td></td>
<td>1.5 Initial Appliance Setup</td>
<td>84</td>
</tr>
<tr>
<td></td>
<td>1.6 Core Functionality</td>
<td>86</td>
</tr>
<tr>
<td>2</td>
<td>Operations</td>
<td>105</td>
</tr>
<tr>
<td></td>
<td>2.1 Dashboard</td>
<td>105</td>
</tr>
<tr>
<td></td>
<td>2.2 Reports</td>
<td>105</td>
</tr>
<tr>
<td></td>
<td>2.3 Analytics</td>
<td>110</td>
</tr>
<tr>
<td></td>
<td>2.4 Guidance</td>
<td>132</td>
</tr>
<tr>
<td></td>
<td>2.5 Wiki</td>
<td>135</td>
</tr>
<tr>
<td></td>
<td>2.6 Costing</td>
<td>136</td>
</tr>
<tr>
<td></td>
<td>2.7 Approvals</td>
<td>150</td>
</tr>
<tr>
<td></td>
<td>2.8 Activity</td>
<td>153</td>
</tr>
<tr>
<td>3</td>
<td>Provisioning</td>
<td>155</td>
</tr>
<tr>
<td></td>
<td>3.1 Requirements</td>
<td>155</td>
</tr>
<tr>
<td></td>
<td>3.2 Provisioning Concepts</td>
<td>161</td>
</tr>
<tr>
<td></td>
<td>3.3 Catalog</td>
<td>162</td>
</tr>
<tr>
<td></td>
<td>3.4 Instances</td>
<td>166</td>
</tr>
<tr>
<td></td>
<td>3.5 Apps</td>
<td>170</td>
</tr>
<tr>
<td></td>
<td>3.6 Jobs</td>
<td>174</td>
</tr>
<tr>
<td></td>
<td>3.7 Executions</td>
<td>181</td>
</tr>
<tr>
<td></td>
<td>3.8 Code</td>
<td>181</td>
</tr>
<tr>
<td>4</td>
<td>Library</td>
<td>189</td>
</tr>
<tr>
<td></td>
<td>4.1 Automation</td>
<td>189</td>
</tr>
<tr>
<td></td>
<td>4.2 Blueprints</td>
<td>208</td>
</tr>
<tr>
<td></td>
<td>4.3 Virtual Images</td>
<td>235</td>
</tr>
<tr>
<td></td>
<td>4.4 Options</td>
<td>240</td>
</tr>
<tr>
<td></td>
<td>4.5 Templates</td>
<td>256</td>
</tr>
<tr>
<td></td>
<td>4.6 Library Integrations</td>
<td>260</td>
</tr>
<tr>
<td></td>
<td>4.7 Variables</td>
<td>260</td>
</tr>
<tr>
<td>5</td>
<td>Infrastructure</td>
<td>281</td>
</tr>
<tr>
<td></td>
<td>5.1 Groups</td>
<td>281</td>
</tr>
<tr>
<td></td>
<td>5.2 Clouds</td>
<td>284</td>
</tr>
</tbody>
</table>
### 5.3 Clusters

5.4 Compute

5.5 Network

5.6 Load Balancers

5.7 Storage

5.8 Key Pairs & Certificates

5.9 Boot

### 6 Backups

6.1 Initial Backups Setup

6.2 Configuring Backups during Provisioning

6.3 Summary

6.4 Backups

6.5 Managing Backups

### 7 Monitoring

7.1 Overview

### 8 Tools

8.1 Cypher

8.2 Archives

8.3 Image Builder

8.4 VDI Pools

### 9 Administration

9.1 Tenants

9.2 Identity Sources

9.3 Plans & Pricing

9.4 Roles

9.5 Users & User Groups

9.6 Integrations

9.7 Policies

9.8 Health

9.9 Settings

9.10 User Settings

### 10 Personas

10.1 Service Catalog Persona

10.2 Virtual Desktop Persona

10.3 Configuring Persona Access

10.4 Accessing Alternate Personas

### 11 Troubleshooting

11.1 Ansible Troubleshooting

11.2 Attaching Logs to Case

11.3 Blank Dashboard

11.4 CLI Troubleshooting

11.5 Cannot Login

11.6 Common Ports & Requirements

11.7 Deleting Instances

11.8 How to un-manage an Instance/VM/Host

11.9 MySQL Too many connections error

11.10 Morpheus Agent Install Troubleshooting

11.11 Morpheus UI not loading after upgrade or reconfigure

11.12 Remote Console
Important: 5.3.4 contains major UI navigation structure changes. Please refer to the v5.3.4 Release Notes and Navigation Updates reference table before upgrading.

v5.3.4 Release Notes
1.1 Requirements

Morpheus is a software based appliance installation capable of orchestrating many clouds and hypervisors. Before an installation is started it is important to understand some of the base requirements.

In the simplest configuration Morpheus needs one Appliance Server. The Appliance Server, by default, contains all the components necessary to orchestrate both VMs and containers. To get started some base requirements are recommended:

1.1.1 Base Requirements

<table>
<thead>
<tr>
<th>OS</th>
<th>Version(s)</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Linux</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>CentOS</td>
<td>7.x, 8.x</td>
<td></td>
</tr>
<tr>
<td>Debian</td>
<td>9,10,11</td>
<td>FreeRDP 2.0 is not compatible with Debian 9. Guacd will remain at 1.0.0 for Appliances running on 9.</td>
</tr>
<tr>
<td>RHEL</td>
<td>7.x, 8.x</td>
<td></td>
</tr>
<tr>
<td>SUSE SLES</td>
<td>12, 15</td>
<td></td>
</tr>
<tr>
<td>Ubuntu</td>
<td>16.04, 18.04, 20.04</td>
<td>14.04 is no longer supported for Appliance OS. Existing Appliances on 14.04 must upgrade to 16.04 or 18.04 PRIOR to upgrading to v4.2.1. Note: 14.04 is still supported by the Morpheus Agent.</td>
</tr>
</tbody>
</table>

- **Memory**: 16 GB recommended for default installations. 8 GB minimum required with 4 GB+ available storage swap space
- **Storage**: 200 GB storage minimum (see Storage Considerations below)
- **CPU**: 4-core, 1.4 GHz (or better), 64-bit CPU recommended for all-in-one systems. For a distributed-tier installation, it’s recommended each tier have 2-core, 1.4 GHz (or better), 64-bit CPU
- Network connectivity from your users to the appliance over TCP 443 (HTTPS)
- Superuser privileges via the *sudo* command for the user installing the Morpheus appliance package
Morpheus Documentation

- Access to base `yum` or `apt` repositories. `codeready` (codeready-builder-for-rhel-8-x86_64-rpms) repo access is required for RHEL 8+ appliances and access to the Optional RPMs repo is required for RHEL 7.x

- An appliance license is required for any operations involving provisioning

- Current major web browsers supporting modern standards, such as Google Chrome, Mozilla Firefox, Apple Safari, and Microsoft Edge are supported

- Internet Connectivity (optional)
  - To download from Morpheus’ public docker repositories and system Virtual Image catalog
  - Offline installation requires installing the supplemental package in addition to the regular installation package. Local `yum/apt` repo access still required for offline installations.

Note: Access to `yum` and `apt` repos is still required for offline installations.

- VM and Host Agent Install (optional)
  - Inbound connectivity access from provisioned VMs and container hosts on port 443 (Agent install and communication). Port 80 may be required for older `apt` distros.
  - An Appliance URL that is accessible/resolvable to all managed hosts. It is necessary for all hosts that are managed by Morpheus to be able to communicate with the appliance server ip on port 443. This URL is configured under Administration > Settings.

Note: Ubuntu 16.10 is not currently supported.

1.1.2 Storage Considerations

Upon initial installation Morpheus takes up less than 10 GB of space, however Morpheus Services, Virtual Images, Backups, Logs, stats, and user-uploaded and imported data require adequate space on the Morpheus Appliance(s) based on appliance configuration and activity. Morpheus recommends at least 200 GB as a general figure to start from but storage needs will vary dramatically based on each specific use case. In some cases, significantly more space will be needed.

Important: It is the customer’s responsibility to ensure adequate storage space per configuration and use case. The appliance should be properly monitored to ensure it does not run low on disk space.

Default Paths

```
/opt/morpheus  Morpheus Application and Services Files
/var/opt/morpheus User, Application and Services Data, including default config Elasticsearch, RabbitMQ and Database data, and default Virtual Image path.
/var/log  Morpheus Service logs
/tmp/morpheus  Working directory for Backups
```
Images

Virtual Images can be uploaded to Morpheus Storage Providers for use across Clouds. By default when no Storage Provider has been added, images will write to `/var/opt/morpheus/morpheus-ui/vms`. Please ensure adequate space when uploading Images using local file paths.

Backups

Morpheus can offload snapshots when performing backups to local or other Storage Providers. By default when no Storage Provider has been added, backups will write to `/tmp/morpheus/backups/`. When using a none NFS Storage provider, the backup file(s) must be written to `/tmp/morpheus/working/` before they can be zipped, sent to the destination Storage provider such as S3, and then removed from `/tmp/morpheus/working/`. Please ensure adequate space in `/tmp/morpheus/` when offloading Backups.

Migrations

When performing a Hypervisor to Hypervisor migration, such as VMware to AWS, Virtual Images are written to local storage before conversion and/or upload to the target hypervisor. Please ensure adequate space in `/var/opt/morpheus/morpheus-ui/vms` or other configured local Storage Provider paths when performing Migrations.

VM Logs and Stats

When using Morpheus with a locally-installed Elasticsearch configuration, VM, Container, Host and Appliance logs and stats are stored in Elasticsearch. Please ensure adequate space in `/var`, specifically `/var/opt/morpheus/elasticsearch` in relation to the number of Instances reporting logs, log frequency, and log retention count. With partition space at 85% filled or higher (by default), Elasticsearch will enter an unhealthy state and the Morpheus appliance will not function properly.

Morpheus Services Logs

Logs for services local to the Morpheus Appliance, such as the Morpheus UI, elasticsearch, rabbitmq, mysql, nginx and guacd are written to `/var/log/morpheus/`. Current logs are rotated nightly, zipped, and files older than 30 days are automatically removed. Misconfigured services, ports and permissions can cause excessive log file sizes.

1.1.3 Network Connectivity

Morpheus primarily operates via communication with its Agent that is installed on all managed VMs or docker hosts. This is a lightweight agent responsible for aggregating logs and stats and sending them back to the client with minimal network traffic overhead. It also is capable of processing instructions related to provisioning and deployments instigated by the appliance server.

The Morpheus Agent exists for both Linux and Windows-based platforms and opens NO ports on the guest operating system. Instead it makes an outbound SSL (HTTPS/WSS) connection to the appliance server. This is what is known as the appliance url during configuration (in Administration > Settings). When the Agent is started it automatically makes this connection and securely authenticates. Therefore, it is necessary for all VMs and docker based hosts that are managed by Morpheus to be able to reach the appliance server IP on port 443.

Morpheus has numerous methods to execute Agent installation, including zero open port methods.
1.1.4 Components

The Appliance Server automatically installs several components for the operation of Morpheus. This includes:

- RabbitMQ (Messaging)
- MySQL (Logistical Data store)
- Elasticsearch (Logs / Metrics store)
- Tomcat (Morpheus Application)
- Nginx (Web frontend)
- Guacamole (Remote console service for clientless remote console)
- Check Server (Monitoring Agent for custom checks added via UI)

All of these are installed in an isolated way using chef zero to /opt/morpheus. It is also important to note these services can be offloaded to separate servers or clusters as desired. For details check the installation section and high availability.

1.1.5 Common Ports & Requirements

The following chart is useful for troubleshooting Agent install, Static IP assignment, Remote Console connectivity, and Image transfers.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Method</th>
<th>OS</th>
<th>Source Destination</th>
<th>Port</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Communication</td>
<td>All</td>
<td>All</td>
<td>Node</td>
<td>443</td>
<td>DNS Resolution from node to appliance url</td>
</tr>
<tr>
<td>Agent Install</td>
<td>All</td>
<td>Linux</td>
<td>Node</td>
<td>80</td>
<td>Used for appliance yum and apt repos</td>
</tr>
<tr>
<td>SSH</td>
<td>Linux</td>
<td>Appliance</td>
<td>Node</td>
<td>22</td>
<td>DNS Resolution from node to appliance url</td>
</tr>
<tr>
<td>WinRM</td>
<td>Windows</td>
<td>Appliance</td>
<td>Node</td>
<td>5985</td>
<td>Not required for agent installation in VMware</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>vCenter and vCloud Director type clouds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Otherwise, access from Morpheus App Nodes to Instance Node on 5985</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Virtual Images configured</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SSH Enabled on Virtual Image (winrm quickconfig)</td>
</tr>
<tr>
<td>Cloud-init</td>
<td>Linux</td>
<td></td>
<td></td>
<td></td>
<td>Cloud-init installed on template/image</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Cloud-init settings populated in User Settings or in Administration &gt; Settings &gt; Provisioning</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Agent install mode set to Cloud-Init in Cloud Settings</td>
</tr>
<tr>
<td>Cloudbase-init</td>
<td>Windows</td>
<td></td>
<td></td>
<td></td>
<td>Cloudbase-init installed on template/image</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Cloud-init settings populated in User Settings or in Administration &gt; Settings &gt; Provisioning</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Agent install mode set to Cloud-Init in Cloud Settings</td>
</tr>
<tr>
<td>VMtools</td>
<td>All</td>
<td></td>
<td></td>
<td></td>
<td>VMtools installed on template</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Cloud-init settings populated in Morpheus user settings or in Administration &gt; Settings &gt; Provisioning</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>when using Static IP’s</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Existing User credentials entered on Virtual Image when using DHCP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RPC mode set to VMtools in VMware cloud settings.</td>
</tr>
<tr>
<td>Static IP Assignment</td>
<td>Cloud-Init</td>
<td>All</td>
<td></td>
<td></td>
<td>Network configured in Morpheus (Gateway, Primary and Secondary DNS, CIDR populated, DHCP disabled)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Cloud-init/Cloudbase-init installed on</td>
</tr>
</tbody>
</table>
## 1.1.6 Communication Data

The following table contains communication information, including frequency and configurability between Morpheus and its supported technology integrations.

<table>
<thead>
<tr>
<th>Source</th>
<th>Push/Pull</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Foundry App Check</td>
<td>Server Pull</td>
<td>Cloud Foundry Applications that exist within Morpheus</td>
</tr>
<tr>
<td>Docker Container Check</td>
<td>Server Pull</td>
<td>Docker containers that exist within Morpheus</td>
</tr>
<tr>
<td>Elastic Search Check</td>
<td>Server Pull</td>
<td>Elastic Search application</td>
</tr>
<tr>
<td>Microsoft SQL Server Check</td>
<td>Server Pull</td>
<td>Microsoft SQL application</td>
</tr>
<tr>
<td>Mongo Check</td>
<td>Server Pull</td>
<td>Mongo DB application</td>
</tr>
<tr>
<td>MySQL Check</td>
<td>Server Pull</td>
<td>MySQL application</td>
</tr>
<tr>
<td>Postgres Check</td>
<td>Server Pull</td>
<td>Postgres application</td>
</tr>
<tr>
<td>Push API Check</td>
<td>Client Push</td>
<td>Morpheus API</td>
</tr>
<tr>
<td>Rabbit MQ Check</td>
<td>Server Pull</td>
<td>Rabbit MQ application</td>
</tr>
<tr>
<td>Redis Check</td>
<td>Server Pull</td>
<td>Redis application</td>
</tr>
<tr>
<td>Riak Check</td>
<td>Server Pull</td>
<td>Riak application</td>
</tr>
<tr>
<td>SNMP Check</td>
<td>Server Pull</td>
<td>SNMP</td>
</tr>
<tr>
<td>Socket Check</td>
<td>Server Pull</td>
<td>Web Socket</td>
</tr>
<tr>
<td>Virtual Machine Check</td>
<td>Server Pull</td>
<td>Virtual Machine that exists within Morpheus</td>
</tr>
<tr>
<td>Web Check</td>
<td>Server Pull (GET) or Server Push (POST)</td>
<td>Web application</td>
</tr>
<tr>
<td>Public Cloud Integration</td>
<td>Server Pull</td>
<td>Alibaba Cloud</td>
</tr>
<tr>
<td>Public Cloud Integration</td>
<td>Server Pull</td>
<td>Amazon AWS</td>
</tr>
<tr>
<td>Public Cloud Integration</td>
<td>Server Pull</td>
<td>Amazon AWS GovCloud</td>
</tr>
<tr>
<td>Public Cloud Integration</td>
<td>Server Pull</td>
<td>DigitalOcean</td>
</tr>
<tr>
<td>Public Cloud Integration</td>
<td>Server Pull</td>
<td>Google Cloud Platform</td>
</tr>
<tr>
<td>Public Cloud Integration</td>
<td>Server Pull</td>
<td>Huawei Cloud</td>
</tr>
<tr>
<td>Public Cloud Integration</td>
<td>Server Pull</td>
<td>IBM Cloud</td>
</tr>
<tr>
<td>Public Cloud Integration</td>
<td>Server Pull</td>
<td>Microsoft Azure</td>
</tr>
<tr>
<td>Public Cloud Integration</td>
<td>Server Pull</td>
<td>Open Telekom Cloud</td>
</tr>
<tr>
<td>Public Cloud Integration</td>
<td>Server Pull</td>
<td>Oracle Public Cloud</td>
</tr>
<tr>
<td>Public Cloud Integration</td>
<td>Server Pull</td>
<td>UpCloud</td>
</tr>
<tr>
<td>Public Cloud Integration</td>
<td>Server Pull</td>
<td>VMware on AWS</td>
</tr>
<tr>
<td>Private Cloud Integration</td>
<td>Server Pull</td>
<td>Cisco UCS Manager</td>
</tr>
<tr>
<td>Private Cloud Integration</td>
<td>Server Pull</td>
<td>Dell EMC</td>
</tr>
<tr>
<td>Private Cloud Integration</td>
<td>Server Pull</td>
<td>HPE</td>
</tr>
<tr>
<td>Private Cloud Integration</td>
<td>Server Pull</td>
<td>HPE OneView</td>
</tr>
<tr>
<td>Private Cloud Integration</td>
<td>Server Pull</td>
<td>KVM</td>
</tr>
<tr>
<td>Private Cloud Integration</td>
<td>Server Pull</td>
<td>MacStadium</td>
</tr>
<tr>
<td>Private Cloud Integration</td>
<td>Server Pull</td>
<td>Microsoft Azure Stack</td>
</tr>
<tr>
<td>Private Cloud Integration</td>
<td>Server Pull</td>
<td>Microsoft Hyper-V</td>
</tr>
<tr>
<td>Private Cloud Integration</td>
<td>Server Pull</td>
<td>Microsoft SCVMM</td>
</tr>
<tr>
<td>Private Cloud Integration</td>
<td>Server Pull</td>
<td>Nutanix Acropolis</td>
</tr>
<tr>
<td>Private Cloud Integration</td>
<td>Server Pull</td>
<td>Openstack</td>
</tr>
<tr>
<td>Private Cloud Integration</td>
<td>Server Pull</td>
<td>Oracle VM</td>
</tr>
<tr>
<td>Private Cloud Integration</td>
<td>Server Pull</td>
<td>Pivotal Cloud Foundry</td>
</tr>
<tr>
<td>Private Cloud Integration</td>
<td>Server Pull</td>
<td>Supermicro</td>
</tr>
<tr>
<td>Private Cloud Integration</td>
<td>Server Pull</td>
<td>VMware vCloud Director</td>
</tr>
<tr>
<td>Private Cloud Integration</td>
<td>Server Pull</td>
<td>VMware ESXi</td>
</tr>
<tr>
<td>Private Cloud Integration</td>
<td>Server Pull</td>
<td>VMware Fusion</td>
</tr>
</tbody>
</table>

---

Table 3: Continues on next page
<table>
<thead>
<tr>
<th>Source</th>
<th>Push/Pull</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private Cloud Integration</td>
<td>Server Pull</td>
<td>VMware vCenter</td>
</tr>
<tr>
<td>Private Cloud Integration</td>
<td>Server Pull</td>
<td>Xen Server</td>
</tr>
<tr>
<td>Automation Integration</td>
<td></td>
<td>Ansible</td>
</tr>
<tr>
<td>Automation Integration</td>
<td>Server Pull</td>
<td>Ansible Tower</td>
</tr>
<tr>
<td>Automation Integration</td>
<td>Server Pull</td>
<td>Chef</td>
</tr>
<tr>
<td>Automation Integration</td>
<td>Server Pull</td>
<td>Puppet</td>
</tr>
<tr>
<td>Automation Integration</td>
<td>Server Pull</td>
<td>Salt</td>
</tr>
<tr>
<td>Automation Integration</td>
<td></td>
<td>Terraform</td>
</tr>
<tr>
<td>Automation Integration</td>
<td>Server Pull</td>
<td>vRealize Orchestrator</td>
</tr>
<tr>
<td>Backup Integration</td>
<td>Server Pull</td>
<td>Commvault</td>
</tr>
<tr>
<td>Backup Integration</td>
<td>Server Pull</td>
<td>Veeam</td>
</tr>
<tr>
<td>Backup Integration</td>
<td>Server Pull</td>
<td>Rubrik</td>
</tr>
<tr>
<td>Backup Integration</td>
<td>Server Pull</td>
<td>Zerto</td>
</tr>
<tr>
<td>Backup Integration</td>
<td>Server Pull</td>
<td>Avamar</td>
</tr>
<tr>
<td>Build Integration</td>
<td>Server Pull</td>
<td>Jenkins</td>
</tr>
<tr>
<td>Container Integration</td>
<td>Server Pull</td>
<td>Docker</td>
</tr>
<tr>
<td>Container Integration</td>
<td></td>
<td>Docker Registry</td>
</tr>
<tr>
<td>Container Integration</td>
<td>Server Pull</td>
<td>Kubernetes</td>
</tr>
<tr>
<td>Deployment Integration</td>
<td>Server Pull</td>
<td>Git/Github</td>
</tr>
<tr>
<td>DNS Integration</td>
<td>Server Pull</td>
<td>AWS Route53</td>
</tr>
<tr>
<td>DNS Integration</td>
<td>Server Pull</td>
<td>Microsoft DNS</td>
</tr>
<tr>
<td>DNS Integration</td>
<td>Server Pull</td>
<td>PowerDNS</td>
</tr>
<tr>
<td>Identity Management Integration</td>
<td>Server Pull</td>
<td>Microsoft AD</td>
</tr>
<tr>
<td>Identity Management Integration</td>
<td>Server Pull</td>
<td>OneLogin</td>
</tr>
<tr>
<td>Identity Management Integration</td>
<td>Server Pull</td>
<td>Okta</td>
</tr>
<tr>
<td>Identity Management Integration</td>
<td>Server Pull</td>
<td>Jump Cloud</td>
</tr>
<tr>
<td>Identity Management Integration</td>
<td>Server Pull</td>
<td>LDAP</td>
</tr>
<tr>
<td>Identity Management Integration</td>
<td>Server Pull</td>
<td>SAML</td>
</tr>
<tr>
<td>Identity Management Integration</td>
<td>Server Pull</td>
<td>Infoblox</td>
</tr>
<tr>
<td>IPAM Integration</td>
<td>Server Pull</td>
<td>phpIPAM</td>
</tr>
<tr>
<td>IPAM Integration</td>
<td>Server Pull</td>
<td>Bluecat</td>
</tr>
<tr>
<td>IPAM Integration</td>
<td>Server Pull</td>
<td>SolarWinds</td>
</tr>
<tr>
<td>ITSM Integration</td>
<td>Server Pull</td>
<td>ServiceNow</td>
</tr>
<tr>
<td>ITSM Integration</td>
<td>Server Pull</td>
<td>Cherwell</td>
</tr>
<tr>
<td>ITSM Integration</td>
<td>Server Pull</td>
<td>Remedy</td>
</tr>
<tr>
<td>Key &amp; Certificate Integration</td>
<td>Server Pull</td>
<td>Venafi</td>
</tr>
<tr>
<td>Load Balancer Integration</td>
<td>Server Pull</td>
<td>AzureLB</td>
</tr>
<tr>
<td>Load Balancer Integration</td>
<td>Server Pull</td>
<td>F5 BigIP</td>
</tr>
<tr>
<td>Load Balancer Integration</td>
<td>Server Pull</td>
<td>Citrix NetScaler</td>
</tr>
<tr>
<td>Logging Integration</td>
<td></td>
<td>Syslog</td>
</tr>
<tr>
<td>Monitoring Integration</td>
<td>Server Pull</td>
<td>ServiceNow</td>
</tr>
<tr>
<td>Monitoring Integration</td>
<td></td>
<td>AppDynamics</td>
</tr>
<tr>
<td>Monitoring Integration</td>
<td></td>
<td>NewRelic</td>
</tr>
<tr>
<td>Network Integration</td>
<td>Server Pull</td>
<td>NSX-T</td>
</tr>
<tr>
<td>Network Integration</td>
<td>Server Pull</td>
<td>NSX-V</td>
</tr>
<tr>
<td>Network Integration</td>
<td>Server Pull</td>
<td>Cisco ACI</td>
</tr>
<tr>
<td>Network Integration</td>
<td>Server Pull</td>
<td>Unisys Stealth</td>
</tr>
<tr>
<td>Storage Integration</td>
<td>Server Pull</td>
<td>3Par</td>
</tr>
<tr>
<td>Storage Integration</td>
<td>Server Pull</td>
<td>Azure Storage</td>
</tr>
</tbody>
</table>

### 1.1. Requirements

<table>
<thead>
<tr>
<th><strong>Requirement</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage Integration</td>
<td>Server Pull 3Par</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Source</strong></th>
<th><strong>Push/Pull</strong></th>
<th><strong>Destination</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Private Cloud Integration</td>
<td>Server Pull</td>
<td>VMware vCenter</td>
</tr>
<tr>
<td>Private Cloud Integration</td>
<td>Server Pull</td>
<td>Xen Server</td>
</tr>
<tr>
<td>Automation Integration</td>
<td>Server Pull</td>
<td>Ansible</td>
</tr>
<tr>
<td>Automation Integration</td>
<td>Server Pull</td>
<td>Ansible Tower</td>
</tr>
<tr>
<td>Automation Integration</td>
<td>Server Pull</td>
<td>Chef</td>
</tr>
<tr>
<td>Automation Integration</td>
<td>Server Pull</td>
<td>Puppet</td>
</tr>
<tr>
<td>Automation Integration</td>
<td>Server Pull</td>
<td>Salt</td>
</tr>
<tr>
<td>Automation Integration</td>
<td>Server Pull</td>
<td>Terraform</td>
</tr>
<tr>
<td>Automation Integration</td>
<td>Server Pull</td>
<td>vRealize Orchestrator</td>
</tr>
<tr>
<td>Backup Integration</td>
<td>Server Pull</td>
<td>Commvault</td>
</tr>
<tr>
<td>Backup Integration</td>
<td>Server Pull</td>
<td>Veeam</td>
</tr>
<tr>
<td>Backup Integration</td>
<td>Server Pull</td>
<td>Rubrik</td>
</tr>
<tr>
<td>Backup Integration</td>
<td>Server Pull</td>
<td>Zerto</td>
</tr>
<tr>
<td>Backup Integration</td>
<td>Server Pull</td>
<td>Avamar</td>
</tr>
<tr>
<td>Build Integration</td>
<td>Server Pull</td>
<td>Jenkins</td>
</tr>
<tr>
<td>Container Integration</td>
<td>Server Pull</td>
<td>Docker</td>
</tr>
<tr>
<td>Container Integration</td>
<td>Server Pull</td>
<td>Docker Registry</td>
</tr>
<tr>
<td>Container Integration</td>
<td>Server Pull</td>
<td>Kubernetes</td>
</tr>
<tr>
<td>Deployment Integration</td>
<td>Server Pull</td>
<td>Git/Github</td>
</tr>
<tr>
<td>DNS Integration</td>
<td>Server Pull</td>
<td>AWS Route53</td>
</tr>
<tr>
<td>DNS Integration</td>
<td>Server Pull</td>
<td>Microsoft DNS</td>
</tr>
<tr>
<td>DNS Integration</td>
<td>Server Pull</td>
<td>PowerDNS</td>
</tr>
<tr>
<td>Identity Management Integration</td>
<td>Server Pull</td>
<td>Microsoft AD</td>
</tr>
<tr>
<td>Identity Management Integration</td>
<td>Server Pull</td>
<td>OneLogin</td>
</tr>
<tr>
<td>Identity Management Integration</td>
<td>Server Pull</td>
<td>Okta</td>
</tr>
<tr>
<td>Identity Management Integration</td>
<td>Server Pull</td>
<td>Jump Cloud</td>
</tr>
<tr>
<td>Identity Management Integration</td>
<td>Server Pull</td>
<td>LDAP</td>
</tr>
<tr>
<td>Identity Management Integration</td>
<td>Server Pull</td>
<td>SAML</td>
</tr>
<tr>
<td>Identity Management Integration</td>
<td>Server Pull</td>
<td>Infoblox</td>
</tr>
<tr>
<td>IPAM Integration</td>
<td>Server Pull</td>
<td>phpIPAM</td>
</tr>
<tr>
<td>IPAM Integration</td>
<td>Server Pull</td>
<td>Bluecat</td>
</tr>
<tr>
<td>IPAM Integration</td>
<td>Server Pull</td>
<td>SolarWinds</td>
</tr>
<tr>
<td>ITSM Integration</td>
<td>Server Pull</td>
<td>ServiceNow</td>
</tr>
<tr>
<td>ITSM Integration</td>
<td>Server Pull</td>
<td>Cherwell</td>
</tr>
<tr>
<td>ITSM Integration</td>
<td>Server Pull</td>
<td>Remedy</td>
</tr>
<tr>
<td>Key &amp; Certificate Integration</td>
<td>Server Pull</td>
<td>Venafi</td>
</tr>
<tr>
<td>Load Balancer Integration</td>
<td>Server Pull</td>
<td>AzureLB</td>
</tr>
<tr>
<td>Load Balancer Integration</td>
<td>Server Pull</td>
<td>F5 BigIP</td>
</tr>
<tr>
<td>Load Balancer Integration</td>
<td>Server Pull</td>
<td>Citrix NetScaler</td>
</tr>
<tr>
<td>Logging Integration</td>
<td></td>
<td>Syslog</td>
</tr>
<tr>
<td>Monitoring Integration</td>
<td>Server Pull</td>
<td>ServiceNow</td>
</tr>
<tr>
<td>Monitoring Integration</td>
<td></td>
<td>AppDynamics</td>
</tr>
<tr>
<td>Monitoring Integration</td>
<td></td>
<td>NewRelic</td>
</tr>
<tr>
<td>Network Integration</td>
<td>Server Pull</td>
<td>NSX-T</td>
</tr>
<tr>
<td>Network Integration</td>
<td>Server Pull</td>
<td>NSX-V</td>
</tr>
<tr>
<td>Network Integration</td>
<td>Server Pull</td>
<td>Cisco ACI</td>
</tr>
<tr>
<td>Network Integration</td>
<td>Server Pull</td>
<td>Unisys Stealth</td>
</tr>
<tr>
<td>Storage Integration</td>
<td>Server Pull</td>
<td>3Par</td>
</tr>
<tr>
<td>Storage Integration</td>
<td>Server Pull</td>
<td>Azure Storage</td>
</tr>
</tbody>
</table>
### Table 3 – continued from previous page

<table>
<thead>
<tr>
<th>Source</th>
<th>Push/Pull</th>
<th>Destination</th>
<th>Description</th>
<th>Default Interval</th>
<th>Configurable Internal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage Integration</td>
<td>Server Pull</td>
<td>Dell ECS</td>
<td>Updating storage metadata</td>
<td>10 Minutes</td>
<td>No</td>
</tr>
<tr>
<td>Storage Integration</td>
<td>Server Pull</td>
<td>Isilon</td>
<td>Updating storage metadata</td>
<td>10 Minutes</td>
<td>No</td>
</tr>
<tr>
<td>Morpheus Agent</td>
<td>Agent Pull</td>
<td>Application Tier</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 1.1.7 SELinux

If not required by organizational policy, we recommend setting SELinux to “Permissive” or “Disabled” modes to prevent any unnecessary security-related issues. Morpheus versions 3.6.0 and higher do support “Enforcing” mode if it is required by your organization due to IT policies. Set the mode appropriately prior to running the Morpheus installer and it will make the required changes based on your chosen SELinux context.

**Important:** Setting SELinux to “Enforcing” mode requires policies to be configured correctly in order for the Morpheus appliance to function correctly.

### 1.1.8 Supported Locales

Morpheus supports a number of different UI locales, including:

- English
- French
- German
- Spanish
- Chinese (Simplified)
- Portuguese (Brazil)
- Korean
- Italian

The full list of supported locales can be viewed within the Morpheus UI via the “Default Appliance Locale” select list within Administration Settings.

#### Switching Locales

The language of text in the Morpheus UI can be changed by telling the Morpheus server which locale to use. A Locale is made up of a language code and a country code. For example “en_US” is the code for US English, whilst “en_GB” is the code for British English. When using the Morpheus UI software through a client, the Morpheus UI software server will send the UI text back to the client using the appropriate static Language Pack. All translations returned via Morpheus Internationalization have been made and approved prior to the Morpheus UI version release.

**Via Locale Settings in the Morpheus UI:** An application wide default locale can be configured within the Master Tenant under Administration -> Settings -> Default Appliance Locale. An individual Morpheus user can configure a preferred locale within their user settings. Using a locale setting is the preferred method for switching the Morpheus UI language.

**Via the Accept-Language HTTP header:** The Accept-Language request HTTP header advertises which languages the client is able to understand, and which locale variant is preferred. Most browsers will by default send a “Accept-Language” HTTP header when visiting websites. The value of Accept-Language will match the configured preference.
of the browser’s user language/locale settings. The Morpheus UI will automatically detect the Accept-Language header and return the UI text from the corresponding Language Pack where possible. If there is no matching Language Pack the English US language pack is displayed in the UI. If an application locale or user locale setting has been configured in the Morpheus UI, then this will override the user’s browser preferences.

**Via the “lang” query parameter:** Morpheus has the capability to switch locales by passing a parameter called “lang” to the Morpheus UI request. For example, “operations/dashboard?lang=de” will switch the locale preference to German. Morpheus will automatically switch the user’s locale and store it in a cookie so subsequent requests will have the new header. If a user is unauthenticated then the user’s locale will be reset. To switch a locale back to English pass “?lang=en” as a query parameter in the Morpheus UI request.

**Note:** Many of Morpheus’ language packs are generated by our clients. For that reason, we cannot guarantee accuracy and completeness of the translation. As new UI elements are added, existing language sets may not have immediate updates to keep pace with application changes. If you would like to contribute to a new or existing language pack, contact your account team or Morpheus support. Contributed content will be included within the next application version.

### 1.2 Installation

#### 1.2.1 Installation Overview

**Important:** Morpheus v4.2.0 enhanced security configuration restricts incoming appliance connections to TLS v1.2, potentially impacting front-end load balancer monitoring/health checks that support only TLS v1.1 or lower, as well as Morpheus Agent installations for Windows nodes using .net versions that do not support TLS v1.2. Refer to TLS

Morpheus comes packaged as a **debian** or **yum** based package. The default configuration installs all required services on a single vm or bare metal Host. Morpheus can be configured in a distributed architecture to use one or multiple external services, and multiple application Hosts can be configured for High Availability configurations.

All components required for Morpheus are installed and configured by default during the Morpheus reconfigure command. The Morpheus config file, `morpheus.rb`, can optionally be configured to point the Morpheus App to external services (distributed configuration).

Morpheus can optionally be configured to use external Database, Messaging, and/or Search Tiers. This means instead of installing, for example, MySQL on the same host as the Morpheus App, the Morpheus configuration file (morpheus.rb) is setup to point to an external MySQL host, cluster or service, and MySQL will not be installed or configured on the Appliance Host.

**Install Packages**

Morpheus Release Package urls can be obtained from https://morpheushub.com
Configuration Options

- **Single Host (All-In-One/default)** All tiers running on a single host. The reconfigure process installs all required services. This is the default configuration.

- **Single Hosts with Distributed Service(s)** Transactional Database, Non-Transactional Database, and/or Message tiers are externalized, with the remaining services on a single host. The reconfigure process installs all services not set to false in `/etc/morpheus/morpheus.rb`.

- **Clustered Hosts with Distributed Transactional Database (3-Node HA)** Application, Message, and Non-Transactional tiers are installed and clustered on three or more hosts, with all three hosts pointing to externalized database tier. The reconfigure process installs all services except MySQL.

- **App Host(s) with Distributed Services (Full HA)** Application tier is installed on one or more hosts. All UI hosts point to externalized Transactional Database, Non-Transactional Database, and Message Tiers. The reconfigure process installs only Application services.

Distributed Configurations

Morpheus provides a wide array of options when it comes to deployment architectures. It can start as a simple one machine instance where all services run on the same machine, or it can be split off into individual services per machine and configured in a high availability configuration, either in the same region or cross-region. Naturally, high availability can grow more complicated, depending on the configuration you want to do and this article will cover the basic concepts of the Morpheus HA architecture that can be used in a wide array of configurations.

There are four primary tiers of services represented within the Morpheus appliance. They are the Application Tier, Transactional Database Tier, Non-Transactional Database Tier, and Message Tier. Each of these tiers have their own recommendations for High availability deployments that we need to cover.

**Application Tier**

The application tier is easily installed with the same Debian or yum repository package that Morpheus is normally distributed with. Advanced configuration allows for the additional tiers to be skipped and leave only the “stateless” services that need run. These stateless services include Nginx and Tomcat. These machines should also have at least 8gb of Memory. They can be configured across all regions and placed behind a central load-balancer or Geo based load-balancer. They typically connect to all other tiers as none of the other tiers talk to each other besides through the central application tier. One final piece when it comes to setting up the Application tier is a shared storage means is necessary when it comes to maintaining things like deployment archives, virtual image catalogs, backups, etc. These can be externalized to an object storage service such as Amazon S3 or Openstack Swiftstack as well. If not using those options a simple NFS cluster can also be used to handle the shared storage structure.

**Transactional Database Tier**

The Transactional database tier usually consists of a MySQL compatible database. It is recommended that a lockable clustered configuration be used (Currently Percona XtraDB Cluster is the most recommended in Permissive Mode). There are several documents online related to configuring and setting up an XtraDB Cluster but it most simply can be laid out in a many master configuration. There can be some nodes setup with replication delay as well as some with no replication delay. It is common practice to have no replication delay within the same region and allow some replication delay cross region. This does increase the risk of job run overlap between the 2 regions however, the concurrent operations typically self-correct and this is a non-issue.
Non-Transactional Database Tier

The Non-Transactional tier consists of an ElasticSearch (version 7.6.0) cluster. Elastic Search is used for log aggregation data and temporal aggregation data (essentially stats, metrics, and logs). This enables for a high write throughput at scale. ElasticSearch is a Clustered database meaning all nodes no matter the region need to be connected to each other over what they call a “Transport” protocol. It is fairly simple to get setup as all nodes are identical. It is also a Java-based system and does require a sizable chunk of memory for larger data sets. 8 GB is recommended and more nodes can be added to scale either horizontally or vertically.

Messaging Tier

The Messaging tier is an AMQP based tier along with STOMP Protocol (used for agent communication). The primary model recommended is to use RabbitMQ for queue services. RabbitMQ is also a cluster-based queuing system and needs at least 3 instances for HA configurations. This is due to elections in the failover scenarios RabbitMQ can manage. If doing a cross-region HA RabbitMQ cluster, it is recommended to have at least 3 Rabbit queue clusters per region. Typically to handle HA a RabbitMQ cluster should be placed between a load balancer and the front-end application server to handle cross host connections. The ports necessary to forward in a Rabbit MQ cluster are (5672, and 61613). A RabbitMQ cluster can run on smaller memory machines depending on how frequent large requests bursts occur. 4 - 8 GB of Memory is recommended to start.

Pros/Cons

Single Host

Advantages

• Simple Installation - Morpheus Installs all required services
• Simple Configuration - Morpheus configures all required services
• Simple Maintenance - All service connections and credentials are local - All logs are local - All Data is local (by default)
• Not dependent on network connections for vital services - Facilitates speed and reliability

Disadvantages

• Single point of failure
• Individual services cannot be scaled
• Upgrades require (minimal) downtime
• Single region

Single Hosts with Distributed Service(s)

Advantages

• Individual services can be scaled
• Managed Services such as RDS can be utilized

Disadvantages

• Single region
• External services require additional configuration and maintenance
• Morpheus is subject to network performance, configuration and availability
• Increased Installation time possible

Clustered Hosts with Distributed Transactional Database

Advantages
• Database can be scaled vertically and/or horizontally
• Managed Services such as RDS can be utilized
• Zero down time upgrades
• No single point of failure
• RabbitMQ and Elasticsearch Clusters

Disadvantages
• External Database services requires additional configuration and maintenance
• App Host Clustering requires additional configuration and maintenance
• Extended Installation time
• Increased Infrastructure requirements
• Load Balancer required to front App Hosts
• Shared Storage configuration required

App Host(s) with Distributed Services

Advantages
• Individual services can be scaled vertically and/or horizontally
• Managed Services such as RDS can be utilized
• Zero down time upgrades
• No single point of failure
• Multi region support

Disadvantages
• External services require additional configuration and maintenance
• Extended Installation time
• Increased Infrastructure Requirements
• Increased Networking requirements
• Load Balancer required to front App Hosts
• Shared Storage configuration required
• Rabbit Load balancer required
1.2.2 Single Node Installation

Single Node Install Overview

In a Single Host/All-in-one configuration, all components required for Morpheus are automatically installed and configured during the Morpheus reconfigure command.

Appliance Host

- Application
  - Morpheus App
- Web Server/Proxy
  - NGINX
- Database
  - MySQL
- Messaging
  - RabbitMQ
- Search
  - Elasticsearch
- Console
  - Guacamole
• Monitoring
  – Check Server

Default Paths

Morpheus follows several install location conventions. Below is a list of the system paths.

Important: Altering the default system paths is not supported and may break functionality.

• Installation Location: /opt/morpheus
• Log Location: /var/log/morpheus
  – Morpheus-UI: /var/log/morpheus/morpheus-ui
  – MySQL: /var/log/morpheus/mysql
  – NginX: /var/log/morpheus/nginx
  – Check Server: /var/log/morpheus/check-server
  – Elastic Search: /var/log/morpheus/elasticsearch
  – RabbitMQ: /var/log/morpheus/rabbitmq
• User-defined install/config: /etc/morpheus/morpheus.rb

Single Node Install on CentOS

Note: Appliance Package links are available at https://morpheushub.com in the downloads section.

Quick Install

1. Install the Appliance package and run `sudo morpheus-ctl reconfigure`.

That is it. After the reconfigure completes, Morpheus will start and be available at `https://your_machine_name` in a minute or few.

Step-by-step Install Instructions

1. Ensure the Morpheus Appliance host meets the minimum Requirements
2. Download the target version `.rpm` package for installation in a directory of your choosing. The package can be removed after successful installation.

   ```bash
   wget https://downloads.morpheusdata.com/path/to/morpheus-appliance-$version.rpm
   ```

3. Validate the package checksum matches source checksums. For example:

   ```bash
   sha256sum morpheus-appliance-$version.rpm
   ```

4. Next install the rpm package
5. By default the appliance_url uses the machines hostname, ie https://your_machine_name. The default url can be changed by editing /etc/morpheus/morpheus.rb and changing the value of appliance_url. Additional Appliance configuration options are available below.

Appliance Configuration Options **Click to Expand/Hide**

Morpheus allows for additional advanced customizations for system managed services within the morpheus.rb file located in /etc/morpheus/morpheus.rb. Below is a list of the supported items available in the morpheus.rb file.

**Note:** Service configuration settings are not applicable for externalized services such as external mysql/percona, elasticsearch or rabbitmq clusters. Only connection settings are applicable for external services. Additionally, to configure Morpheus to utilize alternate ports for SSL, you may have to take additional configuration steps. If simply appending a port to your appliance_url value doesn’t work, consult the related article in our KnowledgeBase.

```ruby
app['encrypted_key_suffix'] = 'suffix'
appliance_url 'https://morpheus.appliance-url.com'
    # Appending alternate port to appliance_url is supported. ie 'https://
    # morpheus.appliance-url.com:8443'
    # The appliance_url cannot exceed 64 characters
    # The appliance_url must not contain a trailing '/'.
ellasticsearch['enable'] = true
ellasticsearch['es_hosts'] = {'127.0.0.1' => 9200}
ellasticsearch['host'] = "127.0.0.1"
ellasticsearch['use_tls'] = false
ellasticsearch['auth_user'] = 'morpheus-es-user'
ellasticsearch['auth_password'] = 'xxxxxxxxxxxxxxxx'
edelasticsearch['log_dir'] = '/var/log/morpheus/elasticsearch'
edelasticsearch['memory_alloc_arena_max'] = 2
edelasticsearch['memory_map_max'] = 65536
edelasticsearch['memory_map_threshold'] = 131072
edelasticsearch['memory_top_pad'] = 131072
edelasticsearch['memory_trim_threshold'] = 131072
edelasticsearch['open_files'] = 204800
guacd['guacamole_enabled'] = false
logging['svlogd_num'] = 30 # keep 30 rotated log files
logging['svlogd_size'] = 209715200 # 200 MB in bytes
logging['svlogd_timeout'] = 86400 # rotate after 24 hours in seconds
mysql['enable'] = true
mysql['host'] = {'127.0.0.1' => 3306}
mysql['use_tls'] = false
mysql['morpheus_db_user'] = 'morpheus-db-user'
mysql['morpheus_db'] = 'xxxxxxxxxxxxxxxx'
mysql['mysql_url_overide'] = 'jdbc:mysql://10.30.20.10:3306,10.30.20.11:3306/morpheusdb?autoReconnect=true&useUnicode=true&characterEncoding=utf8&failOverReadOnly=false&useSSL=false'
```

(continues on next page)
Valid for Internal/System mysql service only

```plaintext
mysql['tmp_dir'] = '/tmp/mysql'
mysql['log_dir'] = '/var/log/morpheus/mysql'
mysql['max_active'] = 100  # The combined value off all app node max_active values must be lower than max_connections setting in mysql
mysql['max_allowed_packet'] = 67108864
mysql['max_connections'] = 151
```

```plaintext
nginx['cache_max_size'] = '5000m'
nginx['enable'] = true
nginx['loading_pages']['failure_page_h1'] = 'Morpheus Server Error'
nginx['loading_pages']['failure_page_h2'] = 'Please contact your system administrator for assistance.'
nginx['loading_pages']['failure_page_title'] = 'Morpheus Server Error'
nginx['loading_pages']['loading_page_h1'] = 'Morpheus Loading'
nginx['loading_pages']['loading_page_h2'] = 'please wait'
nginx['loading_pages']['loading_page_title'] = 'Morpheus Loading'
nginx['max_loops'] = 60  # seconds
nginx['loading_pages']['timeout_page'] = '/timeout.html'
nginx['loading_pages']['timeout_page_h1'] = 'Timeout waiting for Morpheus to load, click below to try again.'
nginx['loading_pages']['timeout_page_title'] = 'Morpheus timeout, please try again...'
```

```plaintext
nginx['ssl_ciphers'] = "ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:
DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:
ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256:
ECDHE-RSA-AES256-SHA:
DHE-RSA-AES256-SHA384:DHE-RSA-AES128-SHA256:
DHE-RSA-AES128-SHA:
SHA256:
SHA1:
MD5:
RC4"
```

```plaintext
nginx['ssl_company_name'] = "Morpheus, LLC"
nginx['ssl_country_name'] = "US"
nginx['ssl_email_address'] = "personal@email.com"
nginx['ssl_locality_name'] = "San Mateo"
nginx['ssl_organizational_unit_name'] = "DevOps"
```

```plaintext
rabbitmq['enable'] = true
rabbitmq['host'] = '127.0.0.1'
rabbitmq['port'] = '5672'
rabbitmq['queue_user'] = 'morpheus-rmq-user'
rabbitmq['queue_user_password'] = 'xxxxxxxxxxxxxxxx'
rabbitmq['vhost'] = 'morpheus'
```

Valid for Internal/System rabbitmq service only
6. After all configuration options have been set, run:

```
sudo morpheus-ctl reconfigure
```

**Note:** Configuration options can be updated after the initial reconfigure by editing `/etc/morpheus/morpheus.rb` and running `sudo morpheus-ctl reconfigure` again. Appliance and other services may need to be restarted depending on configuration changes.

7. Once the installation is complete the morpheus-ui service will automatically start up and be available shortly. To monitor the UI startup process, run `morpheus-ctl tail morpheus-ui` and look for the ascii logo accompanied by the install version and start time:

```
timestamp: __ ___ __
timestamp: / |/ /__ _______ / / ___ __ _____
timestamp: / /|_/ / _ / __/ _ / _ / -_) // (_-<
timestamp: /_/ /_
```

```
timestamp: ****************************************
timestamp: Version: |morphver|
timestamp: Start Time: xxx xxx xxx 00:00:00 UTC 2021
timestamp: ****************************************
```

There are additional install settings that can be viewed in the **Additional Configuration Options** section.

Once the browser is pointed to the appliance a first time setup wizard will be presented. Please follow the on screen instructions by creating the master account. From there you will be presented with the license settings page where a license can be applied for use (if a license is required you may request one or purchase one by contacting your sales representative).

More details on setting up infrastructure can be found throughout this guide.

**Tip:** If any issues occur it may be prudent to check the morpheus log for details at `/var/log/morpheus/morpheus-ui/current`. 

---

rabbitmq['heartbeat'] = nil
rabbitmq['log_dir'] = '/var/log/morpheus/rabbitmq'
rabbitmq['nodename'] = 'rabbit@localhost'
rabbitmq['port'] = '5672'
rabbitmq['use_tls'] = false

repo['repo_host_url'] = 'https://downloads.morpheusdata.com'

ui['http_client_connect_timeout'] = 10000 # in seconds
ui['http_client_connect_timeout'] = 600000 # in seconds
ui['kerberos_config'] = nil
ui['kerberos_login_config'] = nil
ui['log_dir'] = '/var/log/morpheus/morpheus-ui'
ui['max_memory_mb'] = nil
ui['memory_alloc_arena_max'] = 2
ui['memory_map_max'] = 65536
ui['memory_map_threshold'] = 131072
ui['memory_top_pad'] = 131072
ui['memory_trim_threshold'] = 131072
ui['vm_images_cdn_url'] = 'https://morpheus-images.morpheusdata.com'
Morpheus Documentation

Single Node Install on Debian/Ubuntu

To get started installing Morpheus on Ubuntu or Debian a few preparatory items should be addressed first.

1. First make sure the apt repository is up to date by running  `sudo apt-get update`. It is advisable to verify the assigned hostname of the machine is self-resolvable.

   **Important:** If the machine is unable to resolve its own hostname `nslookup hostname` some installation commands will be unable to verify service health during installation and fail.

1. Next simply download the relevant `.deb` package for installation. This package can be acquired from [https://morpheushub.com](https://morpheushub.com) downloads section.

   **Tip:** Use the `wget` command to directly download the package to your appliance server. i.e. `wget https://downloads.morpheusdata.com/path/to/package/morpheus-appliance_x.x.x-1_amd64.deb`

1. Next we must install the package onto the machine and configure the morpheus services:

   ```
sudo dpkg -i morpheus-appliance_x.x.x-1_amd64.deb
sudo morpheus-ctl reconfigure
   ```

2. Once the installation is complete the web interface will automatically start up. By default it will be resolvable at `https://your_machine_name` and in many cases this may not be resolvable from your browser. The url can be changed by editing `/etc/morpheus/morpheus.rb` and changing the value of `appliance_url`. After this has been changed simply run:

   ```
sudo morpheus-ctl reconfigure
sudo morpheus-ctl stop morpheus-ui
sudo morpheus-ctl start morpheus-ui
   ```

   **Note:** The `morpheus-ui` can take 2-3 minutes to startup before it becomes available.

There are additional install settings that can be viewed in the **Additional Configuration Options** section.

Once the browser is pointed to the appliance a first time setup wizard will be presented. Please follow the on screen instructions by creating the master account. From there you will be presented with the license settings page where a license can be applied for use (if a license is required you may request one or purchase one by contacting your sales representative).

More details on setting up infrastructure can be found throughout this guide.

**Tip:** If any issues occur it may be prudent to check the morpheus log for details at `/var/log/morpheus/morpheus-ui/current`. 

---

20 Chapter 1. Getting Started
Single Node Install on RHEL

To get started installing Morpheus on RHEL/RedHat a few prerequisite items are required.

1. Configure firewalld to allow access from users on 443 (Or remove firewall if not required).
2. Make sure the machine is self resolvable to its own hostname.
3. For RHEL 7.x, the Optional RPMs repo needs to be added for Reconfigure to succeed. It does not need to be added For RHEL 8.x, as the Optional RPMs repo is now part of the appstream repo that is enabled by default in RHEL 8.x.
   • RHEL 7.x Amazon: yum-config-manager --enable rhel-7-server-rhui-optional-rpms
   • RHEL 7.x: yum-config-manager --enable rhel-7-server-optional-rpms

Note: For Amazon users a Redhat subscription is not required if the appropriate yum REGION repository is added instead as demonstrated above.

The RedHat Enterprise Linux server needs to be registered and activated with Redhat subscription. The server optional rpms repo needs to be enabled as well.

To check if the server has been activated please run the subscription-manager version. Subscription manager will return the version plus the python dependency version.

If the server has not been registered and activated then the subscription manager version will return the below message.

```
sudo subscription-manager version
server type: This system is currently not registered
subscription management server: 0.9.51.24.-1
subscription-manager: 1.10.14-7.el7 python-rhsm: 1.10.12-2.el7
```

When a server has been registered and activated with Redhat the subscription manager will return the below message.

```
sudo subscription-manager version
server type: Red Hat Subscription Management
subscription management server: 0.9.51.24-1
subscription-manager: 1.10.14-7.el7 python-rhsm: 1.10.12-2.el7
```

If the subscription manager re-turns the message This system is currently not registered please follow the below steps to register the server.

Tip: To register the server you will need to have sudo permissions [Member of the Wheel group] or root access to the server. You will also need your Redhat registered email address and password.

```
subscription-manager register
```

```
sudo subscription-manager register
Username: redhat@example.com
Password: . subscription-manager auto --attach
```

Note: This can take a minute to complete
sudo subscription-manager attach --auto

Installed Product Current Status: Product Name: Red Hat Enterprise Linux
Server Status: Subscribed

To check to see if the RHEL server has the Red Hat Enterprise Linux 7 Server - Optional (RPMs) repo enabled please run the following command to return the repo status.

**Tip:** To check the server repos you will need to have sudo permissions [Member of the Wheel group] or root access to the server.

```bash
sudo yum repolist all | grep "rhel-7-server-optional-rpms" rhel-7-server-optional-rpms/7Server/x86_64 disabled
```

If the repo status was returned as disabled then you will need to enable the repo using the subscription manager like below.

```bash
sudo subscription-manager repos --enable rhel-7-server-optional-rpms
Repository 'rhel-7-server-optional-rpms' is enabled for this system.
```

The message *Repo 'rhel-7-server-optional-rpms' is enabled for this system.* will appear after enabling the repo. This will confirm that the repo has been enabled.

Next simply download the relevant .rpm package for installation. This package can be acquired from morpheushub.com.

**Tip:** Use the `wget` command to directly download the package to your appliance server. i.e. `wget https://downloads.morpheusdata.com/path/to/package.rpm`

Next we must install the package onto the machine and configure the morpheus services:

```bash
sudo rpm -i morpheus-appliance_x.x.x-1_amd64.rpm
sudo morpheus-ctl reconfigure
```

Once the installation is complete the web interface will automatically start up. By default it will be resolvable at `https://your_machine_name` and in many cases this may not be resolvable from your browser. The url can be changed by editing `/etc/morpheus/morpheus.rb` and changing the value of `appliance_url`. After this has been changed simply run:

```bash
sudo morpheus-ctl reconfigure
sudo morpheus-ctl stop morpheus-ui
sudo morpheus-ctl start morpheus-ui
```

**Note:** The `morpheus-ui` can take 2-3 minutes to startup before it becomes available.

There are additional install settings that can be viewed in the *Additional Configuration Options* section.

Once the browser is pointed to the appliance a first time setup wizard will be presented. Please follow the on screen instructions by creating the master account. From there you will be presented with the license settings page where a license can be applied for use (if a license is required you may request one or purchase one by contacting your sales representative).

More details on setting up infrastructure can be found throughout this guide.
Tip: If any issues occur it may be prudent to check the morpheus log for details at `/var/log/morpheus/morpheus-ui/current`.

### 1.2.3 Distributed Installation Overview

Morpheus provides a wide array of options when it comes to deployment architectures. It can start as a simple one machine instance where all services run on the same machine, or it can be split off into individual services per machine and configured in a high availability configuration, either in the same region or cross-region. Naturally, high availability can grow more complicated, depending on the configuration you want to do and this article will cover the basic concepts of the Morpheus HA architecture that can be used in a wide array of configurations.

There are four primary tiers of services represented within the Morpheus appliance. They are the App Tier, Transactional Database Tier, Non-Transactional Database Tier, and Message Tier. Each of these tiers have their own recommendations for High availability deployments that we need to cover.

**Important:** This is a sample configuration only. Customer configurations and requirements will vary.

### Application Tier

The application tier is easily installed with the same debian or yum repository package that Morpheus is normally distributed with. Advanced configuration allows for the additional tiers to be skipped and leave only the “stateless” services that need run. These stateless services include Nginx and Tomcat. These machines should also have at least 8gb of Memory. They can be configured across all regions and placed behind a central load-balancer or Geo based load-balancer. They typically connect to all other tiers as none of the other tiers talk to each other besides through the central application tier. One final piece when it comes to setting up the Application tier is a shared storage means is necessary when it comes to maintaining things like deployment archives, virtual image catalogs, backups, etc. These can be externalized to an object storage service such as Amazon S3 or Openstack Swiftstack as well. If not using those options a simple NFS cluster can also be used to handle the shared storage structure.

### Transactional Database Tier

The Transactional database tier usually consists of a MySQL compatible database. It is recommended that a lockable clustered configuration be used (Currently Percona XtraDB Cluster is the most recommended in Permissive Mode). There are several documents online related to configuring and setting up an XtraDB Cluster but it most simply can be laid out in a many master configuration. There can be some nodes setup with replication delay as well as some with no replication delay. It is common practice to have no replication delay within the same region and allow some replication delay cross region. This does increase the risk of job run overlap between the 2 regions however, the concurrent operations typically self-correct and this is a non-issue.
Non-Transactional Database Tier

The Non-Transactional tier consists of an ElasticSearch (version 7.6.0) cluster. Elastic Search is used for log aggregation data and temporal aggregation data (essentially stats, metrics, and logs). This enables for a high write throughput at scale. ElasticSearch is a Clustered database meaning all nodes no matter the region need to be connected to each other over what they call a “Transport” protocol. It is fairly simple to get setup as all nodes are identical. It is also a java based system and does require a sizable chunk of memory for larger data sets. 8 GB is recommended and more nodes can be added to scale either horizontally or vertically.

Messaging Tier

The Messaging tier is an AMQP based tier along with STOMP Protocol (used for agent communication). The primary model recommended is to use RabbitMQ for queue services. RabbitMQ is also a cluster-based queuing system and needs at least 3 instances for HA configurations. This is due to elections in the failover scenarios RabbitMQ can manage. If doing a cross-region HA RabbitMQ cluster it is recommended to have at least 3 Rabbit queue clusters per region. Typically to handle HA a RabbitMQ cluster should be placed between a load balancer and the front-end application server to handle cross host connections. The ports necessary to forward in a Rabbit MQ cluster are (5672, and 61613). A rabbitmq cluster can run on smaller memory machines depending on how frequent large request bursts occur. 4 - 8 GB of Memory is recommended to start.

1.2.4 3-Node HA Install

Distributed App Nodes with Externalized DB

Assumptions

This guide assumes the following:

- The Baremetal nodes cannot access the public internet
- The base OS is RHEL 7.x
- Shortname versions of hostnames will be resolvable
- All nodes have access to a shared volume for /var/opt/morpheus/morpheus-ui. This can be done as a post startup step.
- This configuration will support the complete loss of a single node, but no more. Specifically the Elasticsearch tier requires at least two nodes to always be clustered.
Default Locations

Morpheus follows several install location conventions. Below is a list of system defaults for convenient management:

- **Installation Location:** /opt/morpheus
- **Log Location:** /var/log/morpheus
  - Morpheus-UI: /var/log/morpheus/morpheus-ui
  - NginX: /var/log/morpheus/nginx
  - Check Server: /var/log/morpheus/check-server
  - Elastic Search: /var/log/morpheus/elasticsearch
  - RabbitMQ: /var/log/morpheus/rabbitmq
- **User-defined install/config:** /etc/morpheus/morpheus.rb

Database Cluster Setup (Percona XtraDB Cluster)

Out of the box Morpheus uses MySQL but Morpheus supports any MySQL-compliant database. There are many ways to set up a highly available, MySQL dialect-based database. One which has found favor with many of our customers is Percona’s XtraDB Cluster. Percona’s product is based off of Galera’s WSREP Clustering, which is also supported.

**Important:** Currently, you must use a v5.7-compatible version of MySQL/Percona. Complete compatibility information is available in the Compatibility and Breaking Changes page. Additional configuration for Percona Clusters with TLS enabled is required. Refer to Percona TLS Configuration in our full HA docs for details.
Storage Requirements

- 30 GB storage minimum for each database node. This should be monitored and increased if the Morpheus database requires more space.

After database installation ensure that the minimum storage requirement is available for the mysql tmpdir. By default mysql will write temporary files in “/tmp”. The mysql tmpdir configuration can be modified using the following steps for each database node:

1. Create the new directory.

   ```
   mkdir /path/to/mysql/tmp/directory
   chown -R mysql:mysql /path/to/mysql/tmp/directory
   ```

2. Edit /etc/my.cnf.

   ```
   [mysqld]
   tmpdir=/path/to/mysql/tmp/directory
   ```

**Important:** Failing to provide sufficient storage to the mysql tmpdir can result in failed database migrations and Morpheus upgrades.

Permission Requirements

Once you have your database installed and configured:

1. The Morpheus appliance uses the utf8 character set and the UTC+0 timezone. Set the variables below on your external database clusters to prevent timestamp errors from being thrown later in Morpheus UI. For all distributions, the configuration is set in /etc/my.cnf for each database node.

   ```
   [mysql]
   default-character-set = utf8
   [mysqld]
   default_time_zone = "+00:00"
   ```

2. Create the Database you will be using with morpheus.

   ```
   mysql> CREATE DATABASE morpheus CHARACTER SET utf8 COLLATE utf8_general_ci;
   mysql> show databases;
   ```

3. Next create your morpheus database user. The user needs to be either at the IP address of the morpheus application server or use '@%’ within the user name to allow the user to login from anywhere.

   ```
   mysql> CREATE USER '$morpheus_db_user_name'@'$source_ip' IDENTIFIED BY '$morpheus_db_user_pw';
   ```

4. Next Grant your new morpheus user permissions to the database.

   ```
   mysql> GRANT ALL PRIVILEGES ON morpheus_db_name.* TO 'morpheus_db_user'@'$source_ip' IDENTIFIED BY 'morpheus_db_user_pw' with grant option;
   ```

(continues on next page)
mysql> GRANT SELECT, PROCESS, SHOW DATABASES, SUPER ON *.* TO 'morpheus_db_user'@'$$source_ip' IDENTIFIED BY 'morpheus_db_user_pw';

mysql> FLUSH PRIVILEGES;

5. Checking Permissions for your user.

SHOW GRANTS FOR '$morpheus_db_user_name'@'$source_ip';

App Node Installation

1. First begin by downloading and installing the requisite Morpheus packages to the Morpheus nodes.

Note: For offline or nodes that cannot reach https://downloads.morpheusdata.com, both the standard and supplemental packages will need to be transferred and then installed on the Morpheus nodes.

All Nodes

[root@node-(1/2/3) ~]# wget https://example/path/morpheus-appliance-ver-1.el7.x86_64.rpm
[root@node-(1/2/3) ~]# rpm -i morpheus-appliance-offline-ver-1.noarch.rpm

2. Do NOT run reconfigure yet. The Morpheus configuration file must be edited prior to the initial reconfigure.

3. Next you will need to edit the Morpheus configuration file /etc/morpheus/morpheus.rb on each node.

Node 1

```
appliance_url 'https://morpheus1.localdomain'
elasticsearch['es_hosts'] = {'10.100.10.121' => 9200, '10.100.10.122' => 9200, '10.100.10.123' => 9200}
elasticsearch['node_name'] = '10.100.10.121'
elasticsearch['host'] = '0.0.0.0'
rabbitmq['host'] = '0.0.0.0'
rabbitmq['nodename'] = 'rabbit@node01'
mysql['enable'] = false
mysql['host'] = '10.100.10.111'
mysql['morpheus_db'] = 'morpheusdb'
mysql['morpheus_db_user'] = 'morpheus'
mysql['morpheus_password'] = 'password'
```

Node 2

```
appliance_url 'https://morpheus2.localdomain'
elasticsearch['es_hosts'] = {'10.100.10.121' => 9200, '10.100.10.122' => 9200, '10.100.10.123' => 9200}
elasticsearch['node_name'] = '10.100.10.122'
elasticsearch['host'] = '0.0.0.0'
rabbitmq['host'] = '0.0.0.0'
rabbitmq['nodename'] = 'rabbit@node02'
mysql['enable'] = false
mysql['host'] = '10.100.10.111'
mysql['morpheus_db'] = 'morpheusdb'
mysql['morpheus_db_user'] = 'morpheus'
mysql['morpheus_password'] = 'password'
```
Node 3

```
appliance_url 'https://morpheus3.localdomain'
elasticsearch['es_hosts'] = {'10.100.10.121' => 9200, '10.100.10.122' => 9200, '10.100.10.123' => 9200}
elasticsearch['node_name'] = '10.100.10.123'
elasticsearch['host'] = '0.0.0.0'
rabbitmq['host'] = '0.0.0.0'
rabbitmq['nodename'] = 'rabbit@node03'
mysql['enable'] = false
mysql['host'] = '10.100.10.111'
mysql['morpheus_db'] = 'morpheusdb'
mysql['morpheus_db_user'] = 'morpheus'
mysql['morpheus_password'] = 'password'
```

**Important:** The elasticsearch node names set in `elasticsearch['node_name']` must match the host entries in `elasticsearch['es_hosts']`. `node_name` is used for `node.name` and `es_hosts` is used for `cluster.initial_master_nodes` in the generated `elasticsearch.yml` config. Node names that do not match entries in `cluster.initial_master_nodes` will cause clustering issues.

4. Reconfigure on all nodes

All Nodes

```
[root@node-[1/2/3] ~] morpheus-ctl reconfigure
```

Morpheus will come up on all nodes and Elasticsearch will auto-cluster. The only item left is the manual clustering of RabbitMQ.

**Clustering RabbitMQ**

1. Select one of the nodes to be your Source Of Truth (SOT) for RabbitMQ clustering (Node 1 for this example). On the nodes that are **NOT** the SOT (Nodes 2 & 3 in this example), begin by stopping the UI and RabbitMQ.

Node 2

```
[root@node-2 ~] morpheus-ctl stop morpheus-ui
[root@node-2 ~] source /opt/morpheus/embedded/rabbitmq/.profile
[root@node-2 ~] rabbitmqctl stop_app
[root@node-2 ~] morpheus-ctl stop rabbitmq
```

Node 3

```
[root@node-3 ~] morpheus-ctl stop morpheus-ui
[root@node-3 ~] source /opt/morpheus/embedded/rabbitmq/.profile
[root@node-3 ~] rabbitmqctl stop_app
[root@node-3 ~] morpheus-ctl stop rabbitmq
```

2. Then on the SOT node, we need to copy the secrets for RabbitMQ.

Begin by copying secrets from the SOT node to the other nodes.

Node 1
3. Then copy the erlang.cookie from the SOT node to the other nodes

Node 1

[root@node-1 ~] cat /opt/morpheus/embedded/rabbitmq/.erlang.cookie

# 754363AD864649RD63D28

Node 2

[root@node-2 ~] vi /opt/morpheus/embedded/rabbitmq/.erlang.cookie

# node-1_erlang_cookie

Nodes 3

[root@node-3 ~] vi /opt/morpheus/embedded/rabbitmq/.erlang.cookie

# node-1_erlang_cookie

4. Once the secrets and cookie are copied from node-1 to nodes 2 & 3, run a reconfigure on nodes 2 & 3.

Node 2

[root@node-2 ~] morpheus-ctl reconfigure

Node 3

[root@node-3 ~] morpheus-ctl reconfigure
5. Next we will join nodes 2 & 3 to the cluster.

**Important**: The commands below must be run at root

### Node 2

```
[root@node-2 ~]# morpheus-ctl stop rabbitmq
[root@node-2 ~]# morpheus-ctl start rabbitmq
[root@node-2 ~]# source /opt/morpheus/embedded/rabbitmq/.profile
[root@node-2 ~]# rabbitmqctl stop_app
Stopping node 'rabbit@node-2' ...
[root@node-2 ~]# rabbitmqctl join_cluster rabbit@node-1
Clustering node 'rabbit@node-2' with 'rabbit@node-1' ...
[root@node-2 ~]# rabbitmqctl start_app
Starting node 'rabbit@node-2' ...
[root@node-2 ~]#
```

### Node 3

```
[root@node-3 ~]# morpheus-ctl stop rabbitmq
[root@node-3 ~]# morpheus-ctl start rabbitmq
[root@node-3 ~]# source /opt/morpheus/embedded/rabbitmq/.profile
[root@node-3 ~]# rabbitmqctl stop_app
Stopping node 'rabbit@node-3' ...
[root@node-3 ~]# rabbitmqctl join_cluster rabbit@node-1
Clustering node 'rabbit@node-3' with 'rabbit@node-1' ...
[root@node-3 ~]# rabbitmqctl start_app
Starting node 'rabbit@node-3' ...
[root@node-3 ~]#
```

**Note**: If you receive an error unable to connect to epmd (port 4369) on node-1: nxdomain (non-existing domain) make sure to add all IPs and short (non-fqdn) hostnames to the etc/hosts file to ensure each node can resolve the other hostnames.

6. Next reconfigure Nodes 2 & 3

### Node 2

```
[root@node-2 ~] morpheus-ctl reconfigure
```

### Node 3
7. The last thing to do is start the Morpheus UI on the two nodes that are NOT the SOT node.

Node 2

```
[root@node-2 ~] morpheus-ctl start morpheus-ui
```

Node 3

```
[root@node-3 ~] morpheus-ctl start morpheus-ui
```

8. You will be able to verify that the UI services have restarted properly by inspecting the logfiles. A standard practice after running a restart is to tail the UI log file.

```
root@node-1/2/3 ~]# morpheus-ctl tail morpheus-ui
```

**Database Migration**

If your new installation is part of a migration then you need to move the data from your original Morpheus database to your new one. This is easily accomplished by using a stateful dump.

1. To begin this, stop the Morpheus UI on your original Morpheus server:

```
[root@node-old ~]# morpheus-ctl stop morpheus-ui
```

2. Once this is done you can safely export. To access the MySQL shell we will need the password for the Morpheus DB user. We can find this in the morpheus-secrets file:

```
[root@node-old ~]# cat /etc/morpheus/morpheus-secrets.json

{
    "mysql": {
        "root_password": "***REDACTED***",
        "morpheus_password": "***REDACTED***",
        "ops_password": "***REDACTED***"
    },
    "rabbitmq": {
        "morpheus_password": "***REDACTED***",
        "queue_user_password": "***REDACTED***",
        "cookie": "***REDACTED***"
    },
    "vm-images": {
        "s3": {
            "aws_access_id": "***REDACTED***",
            "aws_secret_key": "***REDACTED***"
        }
    }
}
```
3. Take note of this password as it will be used to invoke a dump. Morpheus provides embedded binaries for this task. Invoke it via the embedded path and specify the host. In this example we are using the Morpheus database on MySQL listening on localhost. Enter the password copied from the previous step when prompted:

```
[root@node-old ~]# /opt/morpheus/embedded/mysql/bin/mysqldump -u morpheus -h 127.0.0.1 morpheus -p > /tmp/morpheus_backup.sql
```

Enter password:

This file needs to be pushed to the new Morpheus Installation’s backend. Depending on the GRANTS in the new MySQL backend, this will likely require moving this file to one of the new Morpheus frontend servers.

4. Once the file is in place it can be imported into the backend. Begin by ensuring the Morpheus UI service is stopped on all of the application servers:

```
[root@node-1 ~]# morpheus-ctl stop morpheus-ui
[root@node-2 ~]# morpheus-ctl stop morpheus-ui
[root@node-3 ~]# morpheus-ctl stop morpheus-ui
```

5. Then you can import the MySQL dump into the target database using the embedded MySQL binaries, specifying the database host, and entering the password for the Morpheus user when prompted:

```
[root@node-1 ~]# /opt/morpheus/embedded/mysql/bin/mysql -u morpheus -h 10.130.2.38 morpheus -p < /tmp/morpheus_backup.sql
```

Enter password:

---

**Recovery**

If a node happens to crash most of the time Morpheus will start upon boot of the server and the services will self-recover. However, there can be cases where RabbitMQ and Elasticsearch are unable to recover in a clean fashion and require minor manual intervention. Regardless, it is considered best practice when recovering a restart to perform some manual health checks.

```
[root@node-1 ~]# morpheus-ctl status
run: check-server: (pid 17808) 7714s; run: log: (pid 549) 8401s
run: elasticsearch: (pid 19207) 5326s; run: log: (pid 565) 8401s
run: guacd: (pid 601) 8401s; run: log: (pid 573) 8401s
run: morpheus-ui: (pid 17976) 7633s; run: log: (pid 555) 8401s
run: nginx: (pid 581) 8401s; run: log: (pid 544) 8401s
run: rabbitmq: (pid 17850) 7708s; run: log: (pid 542) 8401s
```

But, a status can report false positives if, say, RabbitMQ is in a boot loop or Elasticsearch is up, but not able to join the cluster. It is always advisable to tail the logs of the services to investigate their health.

```
[root@node-1 ~]# morpheus-ctl tail rabbitmq
[root@node-1 ~]# morpheus-ctl tail elasticsearch
```

To minimize disruption to the user interface, it is advisable to remedy Elasticsearch clustering first. Due to write locking in Elasticsearch it can be required to restart other nodes in the cluster to allow the recovering node to join.
Begin by determining which Elasticsearch node became the master during the outage. On one of the two other nodes (not the recovered node):

```
[root@node-2 ~]# curl localhost:9200/_cat/nodes
node-1 10.100.10.121 7 47 0.21 d * morpheus1
localhost 127.0.0.1 4 30 0.32 d m morpheus2
```

The master is determined by identifying the row with the ‘*’ in it. SSH to this node (if different) and restart Elasticsearch.

```
[root@node-1 ~]# morpheus-ctl restart elasticsearch
```

Go to the other of the two ‘up’ nodes and run the curl command again. If the output contains three nodes then Elasticsearch has been recovered and you can move on to re-clustering RabbitMQ. Otherwise you will see output that contains only the node itself:

```
[root@node-2 ~]# curl localhost:9200/_cat/nodes
localhost 127.0.0.1 4 30 0.32 d * morpheus2
```

If this is the case then restart Elasticsearch on this node as well:

```
[root@node-2 ~]# morpheus-ctl restart elasticsearch
```

After this you should be able to run the curl command and see all three nodes have rejoined the cluster:

```
[root@node-2 ~]# curl localhost:9200/_cat/nodes
node-1 10.100.10.121 9 53 0.31 d * morpheus1
localhost 127.0.0.1 7 32 0.22 d m morpheus2
node-3 10.100.10.123 3 28 0.02 d m morpheus3
```

The most frequent case of restart errors for RabbitMQ is with epmd failing to restart. Morpheus’s recommendation is to ensure the epmd process is running and daemonized by starting it:

```
[root@node-1 ~]# /opt/morpheus/embedded/lib/erlang/erts-5.10.4/bin/epmd -daemon
```

And then restarting RabbitMQ:

```
[root@node-1 ~]# morpheus-ctl restart rabbitmq
```

And then restarting the Morpheus UI service:

```
[root@node-1 ~]# morpheus-ctl restart morpheus-ui
```

Again, it is always advisable to monitor the startup to ensure the Morpheus Application is starting without error:

```
[root@node-1 ~]# morpheus-ctl tail morpheus-ui
```

Recovery Thoughts/Further Discussion: If Morpheus UI cannot connect to RabbitMQ, Elasticsearch or the database tier it will fail to start. The Morpheus UI logs can indicate if this is the case.

Aside from RabbitMQ, there can be issues with false positives concerning Elasticsearch’s running status. The biggest challenge with Elasticsearch, for instance, is that a restarted node has trouble joining the ES cluster. This is fine in the case of ES, though, because the minimum_master_nodes setting will not allow the un-joined singleton to be consumed until it joins. Morpheus will still start if it can reach the other two ES hosts, which are still clustered.

The challenge with RabbitMQ is that it is load balanced behind Morpheus for requests, but each Morpheus application server needs to bootstrap the RabbitMQ tied into it. Thus, if it cannot reach its own RabbitMQ startup for it will fail.
Similarly, if a Morpheus UI service cannot reach the database, startup will fail. However, if the database is externalized and failover is configured for Master/Master, then there should be ample opportunity for Morpheus to connect to the database tier.

Because Morpheus can start even though the Elasticsearch node on the same host fails to join the cluster, it is advisable to investigate the health of ES on the restarted node after the services are up. This can be done by accessing the endpoint with curl and inspecting the output. The status should be “green” and number of nodes should be “3”:

```
[root@node-1 ~]# curl localhost:9200/_cluster/health?pretty=true
{
  "cluster_name" : "morpheus",
  "status" : "green",
  "timed_out" : false,
  "number_of_nodes" : 3,
  "number_of_data_nodes" : 3,
  "active_primary_shards" : 110,
  "active_shards" : 220,
  "relocating_shards" : 0,
  "initializing_shards" : 0,
  "unassigned_shards" : 0,
  "number_of_pending_tasks" : 0,
  "number_of_in_flight_fetch" : 0
}
```

If this is not the case it is worth investigating the Elasticsearch logs to understand why the singleton node is having trouble joining the cluster. These can be found at `/var/log/morpheus/elasticsearch/current`

Outside of these stateful tiers, the “morpheus-ctl status” command will not output a “run” status unless the service is successfully running. If a stateless service reports a failure to run, the logs should be investigated and/or sent to Morpheus for additional support. Logs for all Morpheus embedded services are found in `/var/log/morpheus`.

### 1.2.5 Full HA Install

**Full HA Install Overview**

- **App Host(s) with Distributed Services (Full HA)** Application tier is installed on one or more hosts. All UI hosts point to externalized Transactional Database, Non-Transactional Database, and Message Tiers. The reconfigure process installs only Application services.
1.2. Installation
Minimum Nodes

For Full High-Availability configurations, RabbitMQ, Elasticsearch and MySQL (Galera/Percona) must be configured in minimum 3 Node Clusters, and 2 or more App Nodes are required.

Note: VM requirements assume local services. VM count requirements are not applicable when using hosted services such as AWS RDS MySQL.

Minimum 11 Nodes

- 2+ Application Hosts
- 3 Node RabbitMQ Cluster
- 3 Node Elasticsearch Cluster
- 3 Node Galera/Percona Cluster

Important: Asynchronous Active/Active and Active/Passive Database configurations are not supported for HA configurations. A minimum 3 node MySQL Cluster with synchronous multi-master replication is required for Database Clusters. Morpheus recommends Percona XtraDB Clusters with synchronous multi-master replication. Asynchronous Active/Passive can be used but is not considered an HA configuration.

Important: For Clusters with more than 3 Nodes, always use an odd number of nodes (3, 5, 7 etc) to ensure Quorum.

Shared Storage

For configurations with 2 or more Applications Nodes, Shared Storage is required between the app nodes for /var/opt/morpheus/morpheus-ui/*. Local Storage File Shares will need to be copied to a shared file system so all assets are available on all App nodes.

Shared Assets

- Logos
- Uploaded Virtual Images
- Deployment Uploads
- Ansible
- Terraform
- Morpheus Backups

Note: Backups, deployment and virtual image storage locations can be overridden within the Morpheus-ui.
Port Requirements

<table>
<thead>
<tr>
<th>Service</th>
<th>Source</th>
<th>Destination</th>
<th>Port(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Morpheus</td>
<td>Application Node</td>
<td>mySQL</td>
<td>3306</td>
</tr>
<tr>
<td>Morpheus</td>
<td>Application Node</td>
<td>Elasticsearch</td>
<td>9200; 9300</td>
</tr>
<tr>
<td>Morpheus</td>
<td>Application Node</td>
<td>RabbitMQ</td>
<td>5672; 61613</td>
</tr>
<tr>
<td>Morpheus</td>
<td>Application Node</td>
<td>YUM or APT</td>
<td>443</td>
</tr>
<tr>
<td>Elasticsearch</td>
<td>Elasticsearch</td>
<td>Elasticsearch</td>
<td>9200; 9300</td>
</tr>
<tr>
<td>mySQL</td>
<td>mySQL</td>
<td>mySQL</td>
<td>3306;4444;4567;4560</td>
</tr>
<tr>
<td>RabbitMQ</td>
<td>RabbitMQ</td>
<td>RabbitMQ</td>
<td>4369,5672/5671(SSL),61613/61614,25672/25671(SSL)</td>
</tr>
</tbody>
</table>

- Application Tier
  - Messaging Tier
    - 5672
    - TCP
    - AMQP non-TLS connections

- Application Tier
  - Messaging Tier
    - 5671
    - TCP
    - AMQPS TLS enabled connections

- Application Tier
  - Messaging Tier
    - 61613
    - TCP
    - STOMP Plugin connections (Required only for Morpheus versions 4.2.1 or prior)

- Application Tier
  - Messaging Tier
    - 61614
    - TCP
    - STOMP Plugin TLS enabled connections (Required only for Morpheus versions 4.2.1 or prior)

- Messaging Tier
  - Messaging Tier
    - 25672
    - TCP
    - Inter-node and CLI tool communication

- Administrator Web Browser
  - RabbitMQ Server Management
    - 15672
TCP
Management plugin

• Administrator Web Browser
  RabbitMQ Server Management
  15671
  TCP
  Management plugin SSL

• Messaging Tier Cluster Node
  Messaging Tier Cluster Node
  4369
  TCP
  erlang (epmd) peer discovery service used by RabbitMQ nodes and CLI tools

Default Locations

Morpheus follows several install location conventions. Below is a list of system defaults for convenient management:

• Installation Location: /opt/morpheus

• Log Location: /var/log/morpheus
  • Morpheus-UI: /var/log/morpheus/morpheus-ui
  • NGINX: /var/log/morpheus/nginx
  • Check Server: /var/log/morpheus/check-server

• User-defined install/config: /etc/morpheus/morpheus.rb

Percona XtraDB Cluster

Out of the box Morpheus uses MySQL but Morpheus supports any MySQL compliant database. There are many ways to set up a highly available, MySQL dialect based database. One which has found favor with many of our customers is Percona’s XtraDB Cluster. Percona’s product is based off of Galera’s WSREP Clustering, which is also supported.

Important: Currently, you must use a v5.7-compatible version of MySQL/Percona. Complete compatibility information is available in the Compatibility and Breaking Changes page.
Storage Requirements

- 30 GB storage minimum for each database node. This should be monitored and increased if the Morpheus database requires more space.

After database installation ensure that the minimum storage requirement is available for the mysql tmpdir. By default mysql will write temporary files in “/tmp”. The mysql tmpdir configuration can be modified using the following steps for each database node:

1. Create the new directory.

   mkdir /path/to/mysql/tmp/directory
   chown -R mysql:mysql /path/to/mysql/tmp/directory

1. Edit /etc/my.cnf.

   [mysqld]
   tmpdir=/path/to/mysql/tmp/directory

**Important:** Failing to provide sufficient storage to the mysql tmpdir can result in failed database migrations and Morpheus upgrades.

Permission Requirements

Percona requires the following ports for the cluster nodes. Please create the appropriate firewall rules on your Percona nodes.

- 3306
- 4444
- 4567
- 4568

Configure SElinux (optional)

When SELinux is set to Enforcing, by default it will block Percona Cluster communication.

To allow Percona XtraDB Cluster functionality when SELinux is Enforcing, run the following on each Database Node:

1. Install SELinux utilities

   [root]# yum install -y policycoreutils-python.x86_64

2. Configure Percona ports for SELinux:

   [root]# semanage port -m -t mysqld_port_t -p tcp 4444
   [root]# semanage port -m -t mysqld_port_t -p tcp 4567
   [root]# semanage port -a -t mysqld_port_t -p tcp 4568

3. Create the policy file PXC.te
4. Compile and load the SELinux policy

```bash
[root]# vi PXC.te
module PXC 1.0;
require {
    type unconfined_t;
    type mysqld_t;
    type unconfined_service_t;
    type tmp_t;
    type sysctl_net_t;
    type kernel_t;
    type mysqld_safe_t;
    class process { getattr setpgid ];
    class unix_stream_socket connectto;
    class system module_request;
    class file { getattr open read write ];
    class dir search;
}

#============= mysqld_t ==============
allow mysqld_t kernel_t:system module_request;
allow mysqld_t self:process { getattr setpgid ];
allow mysqld_t self:unix_stream_socket connectto;
allow mysqld_t sysctl_net_t:dir search;
allow mysqld_t sysctl_net_t:file { getattr open read ];
allow mysqld_t tmp_t:file write;
```

Add Percona Repo

1. Add the percona repo to your Linux Distro.

```bash
```

2. The below commands will clean the repos and update the server.

```bash
[root]# yum clean all
[root]# yum update -y --skip-broken
```
Installing Percona XtraDB Cluster

Installation and configuration of Percona XtraDB Cluster on CentOS/RHEL 7.

**Important:** This is a sample configuration only. Customer configurations and requirements will vary.

1. Install the Percona XtraDB Cluster software and its dependences.

   ```
   [root]# yum install -y Percona-XtraDB-Cluster-57
   ```

2. Enable the mysql service so that the service started at boot.

   ```
   [root]# systemctl enable mysql
   ```

3. Start mysql

   ```
   [root]# systemctl start mysql
   ```

4. Log into the mysql server and set a new password. To get the temporary root mysql password you will need to run the below command. The command will print the password to the screen. Copy the password.

   ```
   [root]# grep 'temporary password' /var/log/mysqld.log
   ```

5. Login to mysql

   ```
   [root]# mysql -u root -p
   password: 'enter password copied above'
   ```

6. Change the root user password to the mysql db

   ```
   mysql> ALTER USER 'root'@'localhost' IDENTIFIED BY 'rootPassword';
   ```

7. Create the sstuser user and grant the permissions.

   ```
   mysql> CREATE USER 'sstuser'@'localhost' IDENTIFIED BY 'sstUserPassword';
   ```

   **Note:** The sstuser and password will be used in the /etc/my.cnf configuration.

   ```
   mysql> GRANT RELOAD, LOCK TABLES, PROCESS, REPLICATION CLIENT ON *.* TO 'sstuser'@'localhost';
   mysql> FLUSH PRIVILEGES;
   ```

8. Exit mysql then stop the mysql services:

   ```
   mysql> exit
   Bye
   [root]# systemctl stop mysql.service
   ```

9. Install Percona on to the other nodes using the same steps.

   Once the service is stopped on all nodes move onto the next step.
Add [mysqld] to my.cnf in /etc/

1. Add the following to /etc/my.cnf. The node_name and node_address needs to be unique on each of the nodes.

   **DB Node 1**

   ```
   [root]# vi /etc/my.cnf

   [mysqld]
   # pxc_encrypt_cluster_traffic=ON (optional, for TLS only)
   max_connections = 451
   max_allowed_packet = 256M
   wsrep_provider=/usr/lib64/galera3/libgalera_smm.so
   wsrep_provider_options="cert.optimistic_pa=NO"
   wsrep_certification_rules='OPTIMIZED'
   wsrep_cluster_name=morpheusdb-cluster
   wsrep_cluster_address=gcomm://10.30.20.10,10.30.20.11,10.30.20.12
   wsrep_node_name=morpheus-db-node01
   wsrep_node_address=10.30.20.10
   wsrep_sst_method=xtrabackup-v2
   wsrep_sst_auth=sstuser:sstUserPassword
   pxc_strict_mode=PERMISSIVE
   wsrep_sync_wait=2
   skip-log-bin
   default_storage_engine=InnoDB
   innodb_autoinc_lock_mode=2
   default-character-set = utf8
   default_time_zone = "+00:00"
   ```

   **DB Node 2**

   ```
   [root]# vi /etc/my.cnf

   [mysqld]
   # pxc_encrypt_cluster_traffic=ON (optional, for TLS only)
   max_connections = 451
   max_allowed_packet = 256M
   wsrep_provider=/usr/lib64/galera3/libgalera_smm.so
   wsrep_provider_options="cert.optimistic_pa=NO"
   wsrep_certification_rules='OPTIMIZED'
   wsrep_cluster_name=morpheusdb-cluster
   wsrep_cluster_address=gcomm://10.30.20.10,10.30.20.11,10.30.20.12
   # for wsrep_cluster_address=gcomm://Enter the IP address of the primary node first then remaining nodes. Separating the ip addresses with commas
   wsrep_node_name=morpheus-db-node02
   wsrep_node_address=10.30.20.11
   wsrep_sst_method=xtrabackup-v2
   wsrep_sst_auth=sstuser:sstUserPassword
   pxc_strict_mode=PERMISSIVE
   ```
**DB Node 3**

```
[root]# vi /etc/my.cnf

[mysqld]
# pxc_encrypt_cluster_traffic=ON (optional, for TLS only)
max_connections = 451
max_allowed_packet = 256M
wsrep_provider=/usr/lib64/galera3/libgalera_smm.so
wsrep_provider_options="cert.optimistic_pa=NO"
wsrep_certification_rules='OPTIMIZED'
wsrep_cluster_name=morpheusdb-cluster
wsrep_cluster_address=gcomm://10.30.20.10,10.30.20.11,10.30.20.12

# for wsrep_cluster_address=gcomm://Enter the IP address of the primary node
    → first then remaining nodes. Separating the ip addresses with commas

wsrep_node_name=morpheus-db-node03
wsrep_node_address=10.30.20.12
wsrep_sst_method=xtrabackup-v2
wsrep_sst_auth=sstuser:sstUserPassword
pxc_strict_mode=PERMISSIVE
wsrep_sync_wait=2

skip-log-bin
default_storage_engine=InnoDB
innodb_autoinc_lock_mode=2
default-character-set = utf8
default_time_zone = "+00:00"
```

**Note:** The default setting on Morpheus app nodes for `max_active` database connections is 150. For this example we are setting `max_connections = 451` to account for 3 maximum simultaneous morpheus app node connections. If `max_active` is configured higher on the app nodes, or the number of app nodes is not 3, adjust accordingly for your configuration.

2. Save `/etc/my.cnf`

1.2. Installation
Bootstrap DB Node 01

**Important:** Ensure mysql.service is stopped prior to bootstrap.

1. To bootstrap the first node in the cluster run the below command.

   ```
   systemctl start mysql@bootstrap.service
   ```

   **Note:** The mysql service will start during the bootstrap.

   **Note:** Startup failures are commonly caused by misconfigured /etc/my.cnf files. Also verify `safe_to_bootstrap` is set to 1 on Node 01 in /var/lib/mysql/trace/trace.*.

Configure Morpheus Database and User

1. Create the Database you will be using with morpheus.

   Login to mysql on Node 01:

   ```
   mysql -u root -p
   password:
   mysql> CREATE DATABASE morpheus CHARACTER SET utf8 COLLATE utf8_general_ci;
   mysql> show databases;
   ```

2. Next create your morpheus database user. This is the user the morpheus app nodes will auth with mysql.

   ```
   mysql> CREATE USER 'morpheusDbUser'@'%' IDENTIFIED BY 'morpheusDbUserPassword';
   ```

3. Next Grant your new morpheus user permissions.

   ```
   mysql> GRANT ALL PRIVILEGES ON *.* TO 'morpheusDbUser'@'%' IDENTIFIED BY 'morpheusDbUserPassword';
   mysql> FLUSH PRIVILEGES;
   ```

   **Important:** If you grant privileges to the morpheusDbUser to only the morpheusdb database, you will also need to GRANT SELECT, PROCESS, SHOW DATABASES, SUPER ON PRIVILEGES to the morpheusDbUser on *.* for the Appliance Health service.

   ```
   mysql> exit
   ```
Copy SSL Files to other nodes (optional, for TLS only)

During initialization of Node 01 the required pem files will be generated in /var/lib/mysql. The ca.pem, server-cert.pem and server-key.pem files need to match on all nodes in the cluster.

1. Copy the following files from Node 01 to the same path (default is /var/lib/mysql) on Node 02 and Node 03:

   /var/lib/mysql/ca.pem  
   /var/lib/mysql/server-cert.pem  
   /var/lib/mysql/server-key.pem

   .. important:: Ensure all 3 files match on all 3 nodes, including path, owner and permissions.

   .. note:: The generated certificate is self signed. Consult Percona documentation for [mysqld] and SSL file configuration when providing your own.

Start the Remaining Nodes

1. Start mysql on Node 02 and Node 03

   [root]# systemctl start mysql.service

   The services will automatically join the cluster using the sstuser we created earlier.

   Note: Startup failures are commonly caused by misconfigured /etc/my.cnf files.

Verify Configuration

1. Verify SELinux is not rejecting any db cluster communication by running the below on all db nodes:

   [root@allDbNodes]# grep -i denied /var/log/audit/audit.log | grep mysqld_t

   If there are any results, address the source or update the SELinux Policy to resolve.

2. Update SELinux if necessary

   [root@allDbNodes]# rm -f PXC.*  
   [root@allDbNodes]# grep -i denied /var/log/audit/audit.log | grep mysqld_t |  
   audit2allow -M PXC  
   [root@allDbNodes]# semodule -i PXC.pp

3. To verify all nodes joined the cluster, on any db node login to mysql and run show status like 'wsrep%';

   [root@anyDbNode]# mysql -u root -p
   mysql> show status like 'wsrep%';

4. Verify wsrep_cluster_size is 3 and wsrepIncoming_addresses lists all 3 node ip addresses.

5. From all Morpheus app nodes, verify that you can login to all 3 database nodes
Morpheus Documentation

```
[root@allAppNodes] cd
[root@appNode01]# ./mysql -u morpheusDbUser -p -h 10.30.20.10
[root@appNode02]# ./mysql -u morpheusDbUser -p -h 10.30.20.11
[root@appNode03]# ./mysql -u morpheusDbUser -p -h 10.30.20.12
```

If you are unable to login to mysql from an app node, ensure credentials are correct, privileges have been granted, and mysql is running.

To validate network accessibility, use telnet to verify app node can reach db nodes on 3306:
telnet 10.30.20.10 3306

Once you have your database installed and configured:

1. Create the Database you will be using with morpheus.

```
mysql> CREATE DATABASE morpheus CHARACTER SET utf8 COLLATE utf8_general_ci;
mysql> show databases;
```

2. Next create your morpheus database user. The user needs to be either at the IP address of the morpheus application server or use @'%' within the user name to allow the user to login from anywhere.

```
mysql> CREATE USER '$morpheus_db_user_name'@'$source_ip' IDENTIFIED BY '$morpheus_db_user_pw';
```

3. Next Grant your new morpheus user permissions to the database.

```
mysql> GRANT ALL PRIVILEGES ON morpheus_db_name.* TO 'morpheus_db_user'@'
    \$source_ip' IDENTIFIED BY 'morpheus_db_user_pw' with grant option;

mysql> GRANT SELECT, PROCESS, SHOW DATABASES, SUPER ON *.* TO 'morpheus_db_user'
    \$source_ip' IDENTIFIED BY 'morpheus_db_user_pw';

mysql> FLUSH PRIVILEGES;
```

4. Checking Permissions for your user.

```
SHOW GRANTS FOR '$morpheus_db_user_name'@'$source_ip';
```

RabbitMQ Cluster

An HA deployment will also include a Highly Available RabbitMQ. This can be achieved through RabbitMQ's HA-Mirrored Queues on at least 3, independent nodes. To accomplish this we recommend following Pivotal’s documentation on RabbitMQ here: https://www.rabbitmq.com/ha.html and https://www.rabbitmq.com/clustering.html

Install RabbitMQ on the 3 nodes and create a cluster.

**Note:** For the most up to date RPM package we recommend using this link: :link: https://www.rabbitmq.com/install-rpm.html#downloads

**Important:** Morpheus connects to AMQP over 5672 or 5671(SSL) and 61613 or 61614(SSL)
RabbitMQ Installation and Configuration

**Important:** This is a sample configuration only. Customer configurations and requirements will vary.

RabbitMQ requires Erlang to be installed, the exact version will depend on which version of RabbitMQ you’re installing on your queue-tier nodes. Click the link below to expand a compatibility table for RabbitMQ and Erlang. Note that Morpheus is compatible with RabbitMQ 3.5.x and higher, however, versions 3.7.x and earlier have reached their end of life and RabbitMQ does not encourage their use. If needed, a compatibility table for these sunsetted versions is in RabbitMQ documentation.

### RabbitMQ/Erlang Compatibility Table

<table>
<thead>
<tr>
<th>RabbitMQ Version</th>
<th>Minimum Required Erlang/OTP</th>
<th>Maximum Supported Erlang/OTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>23.2</td>
<td>24.x</td>
</tr>
<tr>
<td>3.8.16 - 3.8.19</td>
<td>23.2</td>
<td>24.x</td>
</tr>
<tr>
<td>3.8.9 - 3.8.15</td>
<td>22.3</td>
<td>23.x</td>
</tr>
<tr>
<td>3.8.4 - 3.8.8</td>
<td>21.3</td>
<td>23.x</td>
</tr>
<tr>
<td>3.8.0 - 3.8.3</td>
<td>21.3</td>
<td>22.x</td>
</tr>
</tbody>
</table>

1. Install epel-release and erlang

```bash
yum install epel-release
yum install erlang
```

2. Install RabbitMQ on all 3 Nodes

```bash
rpm --import https://www.rabbitmq.com/rabbitmq-release-signing-key.asc
yum -y install rabbitmq-server-3.6.12-1.el7.noarch.rpm
chkconfig rabbitmq-server on
rabbitmq-server -detached
```

3. Copy the erlang.cookie from Node 1

```bash
cat /var/lib/rabbitmq/.erlang.cookie
```

# Copy the .erlang.cookie value

4. Overwrite `/var/lib/rabbitmq/.erlang.cookie` on Nodes 2 & 3 with value from Node 1 and change its permissions using the follow commands:

```bash
chown rabbitmq:rabbitmq /var/lib/rabbitmq/*
chmod 400 /var/lib/rabbitmq/.erlang.cookie
```

5. Edit `/etc/hosts` file on all 3 nodes to refer to shortnames of the other nodes

Example for node 1 (adjust for nodes 2 and 3):
6. Run the following commands on Node 2 and on Node 3 to join them to the Cluster:

```
rabbitmqctl stop
rabbitmq-server -detached
rabbitmqctl stop_app
rabbitmqctl join_cluster rabbit@<<node 1 shortname>>
rabbitmqctl start_app
```

7. On Node 1, create vhost and add Admin user for Morpheus

```
rabbitmqctl add_vhost morpheus
rabbitmqctl add_user <<admin username>> <<password>>
rabbitmqctl set_permissions -p morpheus <<admin username>> ".*" ".*" ".*"
rabbitmqctl set_user_tags <<admin username>> administrator
```

8. On All Nodes, enable stomp and management plugins:

```
rabbitmq-plugins enable rabbitmq_stomp
rabbitmq-plugins enable rabbitmq_management
```

9. On Node 1, add the required Rabbitmq Policies. The policies will propagate to all nodes.

```
rabbitmqctl set_policy -p morpheus --apply-to queues --priority 2 statCommands
  "statCommands.*" '{"expires":1800000, "ha-mode":"all"}"
rabbitmqctl set_policy -p morpheus --apply-to queues --priority 2
  "morpheusAgentActions" "morpheusAgentActions.*" '{"expires":1800000, "ha-mode":"all"}"
rabbitmqctl set_policy -p morpheus --apply-to all --priority 1
  ha ".*" '{"ha-mode":"all"}"
```

---

**Elasticsearch**

Sample Install of 3 node Elasticsearch Cluster on CentOS 7

**Important:** This is a sample configuration only. Customer configurations and requirements will vary.

**Important:** Morpheus v4.1.2+ requires Elasticsearch v7.x.
Requirements

1. Three Existing CentOS 7+ nodes accessible to the Morpheus Appliance
2. Install Java on each node

   You can install the latest OpenJDK with the command:

   ```bash
   sudo yum install java-1.8.0-openjdk.x86_64
   ```

   To verify your JRE is installed and can be used, run the command:

   ```bash
   java -version
   ```

   The result should look like this:

   ```
   Output of java -version
   openjdk version "1.8.0_65"
   OpenJDK Runtime Environment (build 1.8.0_65-b17)
   OpenJDK 64-Bit Server VM (build 25.65-b01, mixed mode)
   ```

Install Elasticsearch 7.x

**Important:** This is an example Elasticsearch Upgrade for reference only, and is not indicative of the upgrade procedure for every environment/user/customer/configuration.

1. On each ES node run the following to install Elasticsearch.

   ```bash
   rpm --import https://artifacts.elastic.co/GPG-KEY-elasticsearch
   wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-7.6.2-x86_64.rpm
   sudo rpm -Uhv elasticsearch-7.6.2-x86_64.rpm
   ```

2. If necessary, update permissions for the specified log and data paths

   ```bash
   sudo chown -R elasticsearch:elasticsearch /var/log/elasticsearch/
   sudo chown -R elasticsearch:elasticsearch /usr/share/elasticsearch/
   ```

3. Edit `/etc/elasticsearch/elasticsearch.yml` and update each node configuration accordingly.

   Please note several attributes differ in 7.x from 5.x.

   **Node 1 Example (customer configurations will vary)**

   ```bash
   sudo vi /etc/elasticsearch/elasticsearch.yml
   ```

   #Sample elasticsearch.yml config. Adjusting values in elasticsearch.yml for each node in the cluster.
   #Note: Sample only, user configurations and requirements will vary.

   node.name: "es-node-01" ##unique name of this node
   network.host: 10.30.22.152 ##ip of this node
   http.port: 9200

   (continues on next page)
discovery.seed_hosts: ["10.30.22.152","10.30.22.153","10.30.22.154"] ## add all cluster node ip's
cluster.initial_master_nodes: ["10.30.22.152","10.30.22.153","10.30.22.154"] ## add all cluster node ip's
path.logs: /var/log/elasticsearch ## Or your preferred location.
path.data: /usr/share/elasticsearch/ ## Or your preferred location.
discovery.zen.minimum_master_nodes: 2

Node 2 Example (customer configurations will vary)

```
sudo vi /etc/elasticsearch/elasticsearch.yml

#Sample elasticsearch.yml config. Adjusting values in elasticsearch.yml for each node in the cluster.
#Note: Sample only, user configurations and requirements will vary.
node.name: "es-node-02" ##unique name of this node
network.host: 10.30.22.153 ##ip of this node
http.port: 9200
discovery.seed_hosts: ["10.30.22.152","10.30.22.153","10.30.22.154"] ## add all cluster node ip's
cluster.initial_master_nodes: ["10.30.22.152","10.30.22.153","10.30.22.154"] ## add all cluster node ip's
path.logs: /var/log/elasticsearch ## Or your preferred location.
path.data: /usr/share/elasticsearch/ ## Or your preferred location.
discovery.zen.minimum_master_nodes: 2
```

Node 3 Example (customer configurations will vary)

```
sudo vi /etc/elasticsearch/elasticsearch.yml

#Sample elasticsearch.yml config. Adjusting values in elasticsearch.yml for each node in the cluster.
#Note: Sample only, user configurations and requirements will vary.
node.name: "es-node-03" ##unique name of this node
network.host: 10.30.22.154 ##ip of this node
http.port: 9200
discovery.seed_hosts: ["10.30.22.152","10.30.22.153","10.30.22.154"] ## add all cluster node ip's
cluster.initial_master_nodes: ["10.30.22.152","10.30.22.153","10.30.22.154"] ## add all cluster node ip's
path.logs: /var/log/elasticsearch ## Or your preferred location.
path.data: /usr/share/elasticsearch/ ## Or your preferred location.
discovery.zen.minimum_master_nodes: 2
```

4. Save elasticsearch.yml
5. Start Elasticsearch on each node.

```
sudo service elasticsearch start
```
6. Verify cluster health

```
curl http://localhost:9200/_cluster/health
```

(continues on next page)
curl http://node_ip:9200/_cluster/health

Application Tier

Morpheus configuration is controlled by a configuration file located at /etc/morpheus/morpheus.rb. This file is read when you run morpheus-ctl reconfigure after installing the appliance package. Each section is tied to a deployment tier: database is mysql, message queue is rabbitmq, search index is elasticsearch. There are no entries for the web and application tiers since those are part of the core application server where the configuration file resides.

1. Download and install the Morpheus Appliance Package
2. Next we must install the package onto the machine and configure the morpheus services:
   ```bash
   sudo rpm -i morpheus-appliance-x.x.x-1.x86_64.rpm
   ```
3. After installing and prior to reconfiguring, edit the morpheus.rb file
   ```bash
   sudo vi /etc/morpheus/morpheus.rb
   ```
4. Change the values to match your configured services:

   **Note:** The values below are examples. Update hosts, ports, usernames and password with your specifications. Only include entries for services you wish to externalize.

   ```ruby
   mysql['enable'] = false
   mysql['host'] = {'10.30.20.139' => 3306, '10.30.20.153' => 3306, '10.30.20.196' => 3306}
   mysql['morpheus_db'] = 'morpheusdb'
   mysql['morpheus_db_user'] = 'dbuser'
   mysql['morpheus_password'] = 'dbuserpassword'
   rabbitmq['enable'] = false
   rabbitmq['vhost'] = 'morpheus'
   rabbitmq['queue_user'] = 'lbuser'
   rabbitmq['queue_user_password'] = 'lbuserpassword'
   rabbitmq['host'] = 'rabbitvip'
   rabbitmq['port'] = '5672'
   rabbitmq['heartbeat'] = 50
   elasticsearch['enable'] = false
   elasticsearch['cluster'] = 'esclustername'
   elasticsearch['es_hosts'] = {'10.30.20.91' => 9200, '10.30.20.149' => 9200, '10.30.20.165' => 9200}
   elasticsearch['use_tls'] = true
   elasticsearch['auth_user'] = 'morpheus-user'
   elasticsearch['auth_password'] = 'xxxxxxxxxxxxxxxx'
   ```
5. Reconfigure Morpheus
   ```bash
   sudo morpheus-ctl reconfigure
   ```
Shared Storage

For configurations with 2 or more Applications Nodes, Shared Storage is required between the app nodes. Local Storage File Shares will need to be copied to a shared file system so all assets are available on all App nodes.

Assets

- White label images
- Uploaded virtual images
- Deploy uploads
- Ansible Plays
- Terraform
- Morpheus backups

Tip: Backups, deployments and virtual image storage locations can be overridden within the Morpheus-ui. You can find more information on storage here: Storage

To copy the morpheus-ui directory to the shared storage follow the below steps:

1. SSH into the Appliance
2. sudo su (or login as root)
3. cd into /var/opt/morpheus/
4. Backup morpheus-ui directory by running the command below. This will create a new directory in /var/opt/morpheus/ called morpheus-ui-bkp and copy the contents of morpheus-ui into the new directory

   ```
   cp -r morpheus-ui morpheus-ui-bkp
   ```

5. Move morpheus-ui to your shared storage. Example below:

   ```
   mv morpheus-ui /nfs/appliance-files/
   ```

6. Mount your shared storage volume to /var/opt/morpheus/morpheus-ui. How you mount it is dependent on what kind of storage it is. If you mount the volume after the package install, but before the reconfigure, then you don’t need to copy anything to a backup.

7. SSH into the second Appliance and then Backup morpheus-ui directory by running

   ```
   cp -r morpheus-ui morpheus-ui-bkp
   ```

Tip: When adding additional nodes you will only need to run step 6 and 7

Important: NFS mounts require sync option when using Ansible integration with Morpheus Agent command bus execution enabled.
1.3 Upgrades & Maintenance

1.3.1 Upgrading

**Warning:** Morpheus v5.3.4 contains new node and VM node packages that require 3.5GB of storage. It is safe to run `sudo rm -Rf /var/opt/morpheus/package-repos/*` after v5.3.4 package installation and before reconfigure to clean old node and vm node packages from the package-repo when room is needed.

**Upgrading Overview**

**Morpheus Packages**

Morpheus Release Package urls can be obtained from [https://morpheushub.com](https://morpheushub.com)

**Upgrade Requirements**

**Warning:** Morpheus v5.3.4 contains new node and VM node packages that require 3.5GB of storage. It is safe to run `sudo rm -Rf /var/opt/morpheus/package-repos/*` after v5.3.4 package installation and before reconfigure to clean old node and VM node packages from the package-repo when appliance free space is needed.

- Only appliances running Morpheus v4.2.0 or higher can upgrade to v5.3.4

**Important:** BACKUP YOUR DATABASE before the upgrade! You can use the appliance backup job in Morpheus, then rollback and restore your appliance if needed. Make sure you download the backup before you do the upgrade!

- For firewall/proxy/acl considerations, the domain for Appliance, Supplemental and Agent packages was changed recently to [https://downloads.morpheusdata.com](https://downloads.morpheusdata.com) from [https://downloads.gomorpheus.com](https://downloads.gomorpheus.com). Please update ACL’s to allow access to [https://downloads.morpheusdata.com](https://downloads.morpheusdata.com) when necessary.

**v5.3.4 Compatibility & Breaking Changes**

When installing and upgrading to Morpheus v5.3.4, refer to the following to ensure compatibility.

**Breaking Changes**

- **4.2.1+:** Appliance: OS: Ubuntu 14.04 has reached its end of life (EOL) and is no longer supported as a Morpheus Appliance Host Operating System. Any Morpheus Appliance running on 14.04 must be upgraded to 16.04, 18.04 or 20.04 BEFORE upgrading to 4.2.1+. Upgrades on 14.04 will not succeed
- **4.2.1+:** Clouds: VirtualBox, VirtuSteam, and MetaCloud Cloud Types are no longer supported or available
- **4.2.1+:** Puppet: Morpheus integration now supports version 6+. Puppet versions prior to 6 are no longer supported
• 4.2.1+: Tasks: Python: Virtual environment are now used for Python Tasks. **Note:** `virtualenv` is required on all Appliance App nodes

• 4.2.4: For appliances with externalized MySQL databases, due to MySQL deprecation of the “EDT” timezone you may need to update your database timezone to UTC or another compatible value. If this is not done, you will receive errors referencing timezone and Morpheus will not start. Morpheus should handle this change automatically for all-in-one appliances.

• 5.0.0+: When upgrading to 5.0.0+ from 4.x.x, any bearer tokens that have been generated are deleted which requires users to request new bearer tokens

• 5.2.1 & 4.2.5: API: Metadata: Metadata tags now referred to as `tags` and labels now referred to as `labels`. Previously metadata tags were referred to as `metadata` and labels were referred to as `tags`

• 5.2.3+: `codeready` (`codeready-builder-for-rhel-8-x86_64-rpms`) repo access required for RHEL 8+ Appliances, replacing the previous PowerTools/powertools requirement

• 5.2.6, 5.3.1: Appliance & Agent java version updated to `8u292-b10`. jdk8u292 disables TLS 1.0 and 1.1 by default

• 5.2.9: OpenStack v2 Identity API is deprecated as of v5.2.9 (and is removed as of v5.3.3)

• 5.3.2+: `Provisioning → Deployments` has been moved to `Provisioning → Code → Deployments`

• 5.3.2+: The local code repository path moved from `/var/opt/morpheus/morpheus-ui/repo` to `/var/opt/morpheus/morpheus-local/repo` to reduce potential shared storage issues and performance restrictions. The reconfigure process creates the folders and sets the paths in application.yml, no manual intervention is needed unless symlinks exist on `/var/opt/morpheus/morpheus-ui/repo/git` which will need to be removed prior to reconfiguring 5.3.2. The old `/var/opt/morpheus/morpheus-ui/repo` path will be automatically deleted in a future release but can be manually recursively deleted at any time for storage reclamation.

• 5.3.3: Support for OpenStack v2 Identity API is removed

• 5.3.4: Major UI navigation structure changes. Refer to the Navigation Updates reference table

---

**Morpheus Application OS**

Morpheus can be installed on the following platforms. Please note the table below is for Morpheus Application OS support, not Morpheus Agent OS Support.

**Important:** Existing Morpheus Appliances on 14.04 must upgrade to 16.04, 18.04 or 20.04 PRIOR to upgrading to v4.2+.

**Note:** If CentOS 8.2 is pinned to 8.2.2004 vault, the PowerTools repository will need to be pinned to 8.2.2004 to access freerdp-libs 2.0.0
Table 4: Supported Appliance Operating Systems

<table>
<thead>
<tr>
<th>OS</th>
<th>Version(s)</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Linux</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>CentOS</td>
<td>7.x, 8.x</td>
<td>If CentOS 8.2 is pinned to 8.2.2004 vault, the PowerTools repository will need to be pinned to 8.2.2004 to access freerdp-libs 2.0.0</td>
</tr>
<tr>
<td>Debian</td>
<td>9,10,11</td>
<td>FreeRDP 2.0 is not compatible with Debian 9. guacd will remain at 1.0.0 for Appliances running on Debian 9.</td>
</tr>
<tr>
<td>RHEL</td>
<td>7.x, 8.x</td>
<td></td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server (SLES)</td>
<td>12, 15</td>
<td></td>
</tr>
<tr>
<td>Ubuntu</td>
<td>16.04, 18.04, 20.04</td>
<td>14.04 is no longer supported for Appliance OS. Existing Appliances on 14.04 must upgrade to 16.04, 18.04 or 20.04 PRIOR to upgrading to v4.2.1+. Note: 14.04 is still supported by the Morpheus Agent.</td>
</tr>
</tbody>
</table>

Services

v5.3.4 Service Version Changes

- Java upgraded to 8u312-b07
- MySQL upgraded to 5.7.35
- Nginx upgraded to 1.20.1
- RabbitMQ upgraded to 3.9.8
- Tomcat upgraded to 9.0.54

v5.3.4 Service Version Compatibility

When externalizing MySQL, Elasticsearch and/or RabbitMQ services, the following versions are compatible with version Morpheus v5.3.4

<table>
<thead>
<tr>
<th>Service</th>
<th>Compatible Branch</th>
<th>Morpheus Installer Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>MySQL</td>
<td>v5.7</td>
<td>v5.7.35</td>
</tr>
<tr>
<td>MySQL (FIPS)</td>
<td>v5.7</td>
<td>v5.7.35</td>
</tr>
<tr>
<td>Percona</td>
<td>5.7, WSREP 31</td>
<td>n/a</td>
</tr>
<tr>
<td>Elasticsearch</td>
<td>v7.x</td>
<td>v7.8.1</td>
</tr>
<tr>
<td>RabbitMQ</td>
<td>v3.5-3.9</td>
<td>v3.9.8</td>
</tr>
<tr>
<td>Tomcat</td>
<td></td>
<td>v9.0.54</td>
</tr>
<tr>
<td>Nginx</td>
<td></td>
<td>v1.20.1</td>
</tr>
<tr>
<td>OpenSSL</td>
<td></td>
<td>1.1.1k, 1.0.2u (FIPS)</td>
</tr>
<tr>
<td>Java</td>
<td></td>
<td>v8u312-b07</td>
</tr>
<tr>
<td>Java (macOS agent)</td>
<td></td>
<td>v8u302-b08</td>
</tr>
</tbody>
</table>
Security

CVEs Addressed

- CVE-2021-23369

Upgrade Paths & Methods

The following table shows supported version upgrade paths and methods.

- Some Features and Fixes in the From version may not be included in the To version due to From version being released after the To version.

Integrations

Note: Current iterations of Amazon AWS, Microsoft Azure, Google Cloud Platform, Digital Ocean, HPE OneView, OpenTelekom Cloud, IBM Bluemix, Softlayer and UpCloud are all supported.
<table>
<thead>
<tr>
<th>Integration</th>
<th>Supported Version(s)</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ansible</td>
<td>2.7.x</td>
<td></td>
</tr>
<tr>
<td>Ansible Tower</td>
<td>3.8.x</td>
<td></td>
</tr>
<tr>
<td>App Dynamics</td>
<td>4.5.x</td>
<td></td>
</tr>
<tr>
<td>Azure Stack</td>
<td>2002 back to 1908</td>
<td>2019-03-01-hybrid api-profile version used which is supported in 1908 and later Azure Stack versions</td>
</tr>
<tr>
<td>Cisco ACI</td>
<td>3.10</td>
<td></td>
</tr>
<tr>
<td>Citrix Netscaler</td>
<td>v12.1</td>
<td></td>
</tr>
<tr>
<td>Commvault</td>
<td>v11 sp 19</td>
<td></td>
</tr>
<tr>
<td>F5 Big-IP</td>
<td>11.4+</td>
<td></td>
</tr>
<tr>
<td>Infoblox</td>
<td>Latest Versions Supported</td>
<td></td>
</tr>
<tr>
<td>Jenkins</td>
<td>2.x</td>
<td></td>
</tr>
<tr>
<td>Kubernetes</td>
<td>1.x</td>
<td></td>
</tr>
<tr>
<td>Microsoft Hyper-V</td>
<td>2012R2, 2016, 2019</td>
<td></td>
</tr>
<tr>
<td>Nutanix AHV</td>
<td>5.0 - 5.10 Note: Prism Central is not a supported endpoint</td>
<td>In 5.5 - 5.7 if Prism Central is managing Prism Element, image creation will not function due to PC Image Management.</td>
</tr>
<tr>
<td>Openstack</td>
<td>Latest Versions Supported</td>
<td>When creating an OpenStack integration, select the latest available from the OS Version dropdown menu when running a later version</td>
</tr>
<tr>
<td>Rubrik</td>
<td>4.2</td>
<td></td>
</tr>
<tr>
<td>SCVMM</td>
<td>2016, 2019</td>
<td></td>
</tr>
<tr>
<td>ServiceNow</td>
<td>Orlando, Paris, Quebec, Rome</td>
<td></td>
</tr>
<tr>
<td>Terraform</td>
<td>v0.11.x, v0.12.18+, 0.13.x, 0.14.x</td>
<td></td>
</tr>
<tr>
<td>vCloud Director</td>
<td>8.20, 9.1, 9.5, 9.7, 10.0, 10.2</td>
<td>vCD 9.7+ supported on API v31, vCD 10.2+ supported on API v34.0</td>
</tr>
<tr>
<td>Veeam</td>
<td>9.5u3, 9.5u4, 10, 11</td>
<td></td>
</tr>
<tr>
<td>VMware ESXi</td>
<td>5.5, 6.0, 6.5, 6.7, 7</td>
<td></td>
</tr>
<tr>
<td>VMware Fusion</td>
<td>8, 9, 10+</td>
<td></td>
</tr>
<tr>
<td>VMware NSX</td>
<td>-V, -T v3.1.1</td>
<td></td>
</tr>
<tr>
<td>VMware vCenter</td>
<td>5.5, 6.0, 6.5, 6.7, 7</td>
<td></td>
</tr>
<tr>
<td>XenServer</td>
<td>7.x</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** Non-listed versions may be compatible but are not verified.
Morpheus Documentation

Single Node/AIO Appliance Upgrades

Important: Only appliances running Morpheus v4.2.0 or higher can upgrade to v5.3.4. Always backup your database before running any upgrade.

The following covers upgrading Single Node or AIO (All-In-One) Appliance configurations.

Debian / Ubuntu

**Warning:** Morpheus v5.3.4 contains new node and VM node packages that require 3.5GB of storage. It is safe to run `sudo rm -Rf /var/opt/morpheus/package-repos/*` after v5.3.4 package installation and before reconfigure to clean old node and vm node packages from the package-repo when room is needed.

To upgrade Morpheus running on Ubuntu/Debian, download new deb package, stop the morpheus-ui, install the new deb package, then reconfigure.

```bash
sudo wget https://packageUrl.morpheus-appliance_x.x.x-x_amd64.deb
sudo morpheus-ctl stop morpheus-ui
sudo dpkg -i morpheus-appliance_x.x.x-1_amd64.deb
sudo morpheus-ctl reconfigure
```

All services will automatically start during the reconfigure process. After the reconfigure has succeeded, tail the ui service to watch ui startup logs with `morpheus-ctl tail morpheus-ui`.

**Note:** Services will be stopped during package installation and started during the reconfigure process, including the morpheus-ui service. If the reconfigure process is interrupted or fails, the morpheus-ui service may need to be manually started or restarted. In certain situations if another service hangs on starting during reconfigure, run `systemctl restart morpheus-runsvdir` then reconfigure and restart morpheus-ui if successful.

After the morpheus-ui service finishes loading, the upgrade is complete.

CentOS / RHEL / Amazon / SLES

**Warning:** Morpheus v5.3.4 contains new node and VM node packages that require 3.5GB of storage. It is safe to run `sudo rm -Rf /var/opt/morpheus/package-repos/*` after v5.3.4 package installation and before reconfigure to clean old node and vm node packages from the package-repo when room is needed.

To upgrade Morpheus running on CentOS, RHEL, Amazon or SLES, download and install the new rpm package, stop the morpheus-ui, reconfigure and then start the morpheus-ui:

```bash
sudo wget https://packageUrl.morpheus-appliance-x.x.x-x_x86_64.rpm
sudo morpheus-ctl stop morpheus-ui
```

(continues on next page)
All services will automatically start during the reconfigure process. After the reconfigure has succeeded, tail the ui service to watch ui startup logs with `morpheus-ctl tail morpheus-ui`.

**Note:** Services will be stopped during package installation and started during the reconfigure process, including the morpheus-ui service. If the reconfigure process is interrupted or fails, the morpheus-ui service may need to be manually started or restarted. In certain situations if another service hangs on starting during reconfigure, run `systemctl restart morpheus-runsvdir` then reconfigure and restart `morpheus-ui` if successful.

After the morpheus-ui service finishes loading, the upgrade is complete.

### 3-Node HA Upgrade

3-Node HA Appliances represent 3 App nodes with local RabbitMQ and Elasticsearch services clustered across the app nodes, and an external Galera/Percona MySQL cluster.

**Morpheus Packages**

Morpheus Release Package urls can be obtained from [https://morpheushub.com](https://morpheushub.com)

Refer to [v5.3.4 Compatibility & Breaking Changes](#) for any 3-node variations using externalized MySQL, Elasticsearch and/or RabbitMQ version requirements.

**Upgrade Instructions**

### 3-Node HA Debian / Ubuntu Upgrade

The following covers upgrading the Morpheus App nodes in 3 Node HA configurations to v5.3.4.

**Warning:** As a best practice, always backup your database prior to any upgrade.

**Important:** The following is only for “3 Node HA” Architecture configurations.
Morpheus Documentation

Morpheus Packages

Morpheus Release Package urls can be obtained from https://morpheushub.com

4.2.0+ > v5.3.4 Upgrade

**Warning:** Rolling upgrades are not supported for 4.2.x > 5.x upgrades

**Important:** Due to Database schema changes in v5.3.4 it is important to stop the morpheus-ui service on all app nodes prior to upgrade. Failure to do so may result in errors or database corruption.

**Warning:** Morpheus v5.3.4 contains new node and VM node packages that require 3.5GB of storage. It is safe to run `sudo rm -Rf /var/opt/morpheus/package-repos/*` after v5.3.4 package installation and before reconfigure to clean old node and vm node packages from the package-repo when room is needed.

1. Starting with Node 3, on All App Nodes, stop the morpheus-ui services via `morpheus-ctl stop morpheus-ui`. If you receive a timeout, run `morpheus-ctl graceful-kill morpheus-ui`.

   ```
   [root@app-server-3 ~]# morpheus-ctl stop morpheus-ui
   [root@app-server-2 ~]# morpheus-ctl stop morpheus-ui
   [root@app-server-1 ~]# morpheus-ctl stop morpheus-ui
   ```

2. Upgrade the deb package on Node 1, then run a Reconfigure on Node 1

   ```
   [root@app-server-1 ~]# sudo wget https://packageUrl.morpheus-appliance_x.x.x-x_→amd64.deb
   [root@app-server-1 ~]# sudo dpkg -i morpheus-appliance_x.x.x-1_amd64.deb
   [root@app-server-1 ~]# sudo morpheus-ctl reconfigure
   ```

   **Note:** All services will automatically be stopped and started during the reconfigure process. After the reconfigure has succeeded, tail the ui service to watch ui startup logs with `morpheus-ctl tail morpheus-ui`.

3. Once Node 1 upgrade has completed and the ui is available, upgrade the deb package on Node 2, then run a Reconfigure on Node 2.

   ```
   [root@app-server-2 ~]# sudo wget https://packageUrl.morpheus-appliance_x.x.x-x_→amd64.deb
   [root@app-server-2 ~]# sudo dpkg -i morpheus-appliance_x.x.x-1_amd64.deb
   [root@app-server-2 ~]# sudo morpheus-ctl reconfigure
   ```

4. Then upgrade the deb package on Node 3, and run a Reconfigure on Node 3

   ```
   [root@app-server-3 ~]# sudo wget https://packageUrl.morpheus-appliance_x.x.x-x_→amd64.deb
   [root@app-server-3 ~]# sudo dpkg -i morpheus-appliance_x.x.x-1_amd64.deb
   [root@app-server-3 ~]# sudo morpheus-ctl reconfigure
   ```
5. The upgrade is complete and the Morpheus-ui services should be running with clustered Elasticsearch and RabbitMQ services across the 3 nodes.

**Important:** If reconfigure after a rpm package upgrade stalls or hangs on starting a service (mysql, rabbitmq, elasticsearch ...) it is possible the `morpheus-runsvdir` service did not start or a process it was managing was manually shutdown or killed. To resolve, run `systemctl stop morpheus-runsvdir` then `systemctl start morpheus-runsvdir`, then run reconfigure again, `morpheus-ctl reconfigure`.

### 5.0.0+ > v5.3.4 Upgrade

**Note:** Rolling upgrades are supported for 5.x > v5.3.4 upgrades

**Warning:** Morpheus v5.3.4 contains new node and VM node packages that require 3.5GB of storage. It is safe to run `sudo rm -Rf /var/opt/morpheus/package-repos/*` after v5.3.4 package installation and before reconfigure to clean old node and vm node packages from the package-repo when room is needed.

1. Upgrade the deb package on Node 1, then run a Reconfigure on Node 1

   ```bash
   [root@app-server-1 ~]# sudo wget https://packageUrl.morpheus-appliance_x.x.x-x_→amd64.deb
   [root@app-server-1 ~]# sudo dpkg -i morpheus-appliance_x.x.x-1_amd64.deb
   [root@app-server-1 ~]# sudo morpheus-ctl stop morpheus-ui
   [root@app-server-1 ~]# sudo morpheus-ctl reconfigure
   [root@app-server-1 ~]# sudo morpheus-ctl start morpheus-ui
   ```

   After the reconfigure has succeeded, tail the ui service to watch ui startup logs with `morpheus-ctl tail morpheus-ui`. Once morpheus-ui is started, proceed to the next node.

2. Once Node 1 upgrade has completed and the ui is available, upgrade the deb package on Node 2, then run a Reconfigure on Node 2.

   ```bash
   [root@app-server-2 ~]# sudo wget https://packageUrl.morpheus-appliance_x.x.x-x_→amd64.deb
   [root@app-server-2 ~]# sudo dpkg -i morpheus-appliance_x.x.x-1_amd64.deb
   [root@app-server-2 ~]# sudo morpheus-ctl stop morpheus-ui
   [root@app-server-2 ~]# sudo morpheus-ctl reconfigure
   [root@app-server-2 ~]# sudo morpheus-ctl start morpheus-ui
   ```

   After the reconfigure has succeeded, tail the ui service to watch ui startup logs with `morpheus-ctl tail morpheus-ui`. Once morpheus-ui is started, proceed to the next node.

3. Once Node 2 upgrade has completed and the ui is available, upgrade the deb package on Node 3, and run a Reconfigure on Node 3.

   ```bash
   [root@app-server-3 ~]# sudo wget https://packageUrl.morpheus-appliance_x.x.x-x_→amd64.deb
   [root@app-server-3 ~]# sudo dpkg -i morpheus-appliance_x.x.x-1_amd64.deb
   [root@app-server-3 ~]# sudo morpheus-ctl stop morpheus-ui
   [root@app-server-3 ~]# sudo morpheus-ctl reconfigure
   ```

(continues on next page)
After the reconfigure has succeeded, tail the ui service to watch ui startup logs with `morpheus-ctl tail morpheus-ui`.

4. The upgrade is complete and the Morpheus-ui services should be running with clustered Elasticsearch and RabbitMQ services across the 3 nodes.

**Important:** If reconfigure after a rpm package upgrade stalls or hangs on starting a service (mysql, rabbitmq, elasticsearch ...) it is possible the `morpheus-runsvdir` service did not start or a process it was managing was manually shutdown or killed. To resolve, run `systemctl stop morpheus-runsvdir` then `systemctl start morpheus-runsvdir`, then run reconfigure again, `morpheus-ctl reconfigure`.

### 3-Node HA CentOS / RHEL Upgrade

The following covers upgrading the Morpheus App nodes in 3 Node HA configurations to v5.3.4.

**Warning:** As a best practice, always backup your database prior to any upgrade.

**Important:** The following is only for “3 Node HA” Architecture configurations.

#### Morpheus Packages

Morpheus Release Package urls can be obtained from [https://morpheushub.com](https://morpheushub.com)

**4.2.0+ > v5.3.4 Upgrade**

**Warning:** Rolling upgrades are not supported for 4.2.x > 5.x upgrades

**Important:** Due to Database schema changes in v5.3.4 it is important to stop the morpheus-ui service on all app nodes prior to upgrade. Failure to do so may result in errors or database corruption.

**Warning:** Morpheus v5.3.4 contains new node and VM node packages that require 3.5GB of storage. It is safe to run `sudo rm -Rf /var/opt/morpheus/package-repos/*` after v5.3.4 package installation and before reconfigure to clean old node and vm node packages from the package-repo when room is needed.

1. Starting with Node 3, on All App Nodes, stop the morpheus-ui services via `morpheus-ctl stop morpheus-ui`. If you receive a timeout, run `morpheus-ctl graceful-kill morpheus-ui`.
2. Upgrade the RPM package on Node 1, then run a Reconfigure on Node 1

```
[root@app-server-1 ~]# sudo wget https://packageUrl.morpheus-appliance-x.x.x-x.x86_64.rpm
[root@app-server-1 ~]# sudo rpm -Uhv morpheus-appliance-x.x.x-x.x86_64.rpm
[root@app-server-1 ~]# sudo morpheus-ctl reconfigure
```

**Note:** All services will automatically be stopped and started during the reconfigure process. After the reconfigure has succeeded, tail the ui service to watch ui startup logs with `morpheus-ctl tail morpheus-ui`.

3. Once Node 1 upgrade has completed and the ui is available, upgrade the RPM package on Node 2, then run a Reconfigure on Node 2.

```
[root@app-server-2 ~]# sudo wget https://packageUrl.morpheus-appliance-x.x.x-x.x86_64.rpm
[root@app-server-2 ~]# sudo rpm -Uhv morpheus-appliance-x.x.x-x.x86_64.rpm
[root@app-server-2 ~]# sudo morpheus-ctl reconfigure
```

4. Then upgrade the RPM package on Node 3, then run a Reconfigure on Node 3

```
[root@app-server-3 ~]# sudo wget https://packageUrl.morpheus-appliance-x.x.x-x.x86_64.rpm
[root@app-server-3 ~]# sudo rpm -Uhv morpheus-appliance-x.x.x-x.x86_64.rpm
[root@app-server-3 ~]# sudo morpheus-ctl reconfigure
```

5. The upgrade is complete and the Morpheus-ui services should be running with clustered Elasticsearch and RabbitMQ services across the 3 nodes.

**Important:** If reconfigure after a rpm package upgrade stalls or hangs on starting a service (mysql, rabbitmq, elasticsearch ...) it is possible the `morpheus-runsvdir` service did not start or a process it was managing was manually shutdown or killed. To resolve, run `systemctl stop morpheus-runsvdir` then `systemctl start morpheus-runsvdir`, then run reconfigure again, `morpheus-ctl reconfigure`. 
5.0.0+ > v5.3.4 Upgrade

Note: Rolling upgrades are supported for 5.x > v5.3.4 upgrades

Warning: Morpheus v5.3.4 contains new node and VM node packages that require 3.5GB of storage. It is safe to run `sudo rm -Rf /var/opt/morpheus/package-repos/*` after v5.3.4 package installation and before reconfigure to clean old node and vm node packages from the package-repo when room is needed.

1. Upgrade the RPM package on Node 1, then run a Reconfigure on Node 1

   ```
   [root@app-server-1 ~]# sudo wget https://packageUrl.morpheus-appliance-x.x.x-x.˓→x86_64.rpm
   [root@app-server-1 ~]# sudo rpm -Uhv morpheus-appliance-x.x.x-x.x86_64.rpm
   [root@app-server-1 ~]# sudo morpheus-ctl stop morpheus-ui
   [root@app-server-1 ~]# sudo morpheus-ctl reconfigure
   [root@app-server-1 ~]# sudo morpheus-ctl start morpheus-ui
   ```

   After the reconfigure has succeeded, tail the ui service to watch ui startup logs with `morpheus-ctl tail morpheus-ui`. Once morpheus-ui is started, proceed to the next node.

2. Once Node 1 upgrade has completed and the ui is available, upgrade the RPM package on Node 2, then run a Reconfigure on Node 2.

   ```
   [root@app-server-2 ~]# sudo wget https://packageUrl.morpheus-appliance-x.x.x-x.˓→x86_64.rpm
   [root@app-server-2 ~]# sudo rpm -Uhv morpheus-appliance-x.x.x-x.x86_64.rpm
   [root@app-server-1 ~]# sudo morpheus-ctl stop morpheus-ui
   [root@app-server-1 ~]# sudo morpheus-ctl reconfigure
   [root@app-server-1 ~]# sudo morpheus-ctl start morpheus-ui
   ```

   After the reconfigure has succeeded, tail the ui service to watch ui startup logs with `morpheus-ctl tail morpheus-ui`. Once morpheus-ui is started, proceed to the next node.

3. Then upgrade the RPM package on Node 3, then run a Reconfigure on Node 3

   ```
   [root@app-server-3 ~]# sudo wget https://packageUrl.morpheus-appliance-x.x.x-x.˓→x86_64.rpm
   [root@app-server-3 ~]# sudo rpm -Uhv morpheus-appliance-x.x.x-x.x86_64.rpm
   [root@app-server-1 ~]# sudo morpheus-ctl stop morpheus-ui
   [root@app-server-1 ~]# sudo morpheus-ctl reconfigure
   [root@app-server-1 ~]# sudo morpheus-ctl start morpheus-ui
   ```

   After the reconfigure has succeeded, tail the ui service to watch ui startup logs with `morpheus-ctl tail morpheus-ui`. Once morpheus-ui is started, proceed to the next node.

4. The upgrade is complete and the Morpheus-ui services should be running with clustered Elasticsearch and RabbitMQ services across the 3 nodes.

   **Important:** If reconfigure after a rpm package upgrade stalls or hangs on starting a service (mysql, rabbitmq, elasticsearch ...) it is possible the morpheus-runsvdir service did not start or a process it was managing was manually shutdown or killed. To resolve, run `systemctl stop morpheus-runsvdir` then `systemctl start morpheus-runsvdir`, then run reconfigure again, `morpheus-ctl reconfigure`. 

---

Chapter 1. Getting Started
Warning: Upgrades can add additional storage load on database nodes. Please refer to database storage requirements within 3-Node HA Install before upgrading.

Full HA Upgrade

Full HA configurations represent multiple app nodes with external (non-system) MySQL, RabbitMQ and Elasticsearch Clusters or Services.

Morpheus Packages

Morpheus Release Package urls can be obtained from https://morpheushub.com

Overview

When upgrading to v5.3.4 only services local to the Morpheus App node(s) will be upgraded. For fully distributed configurations (Full HA) where MySQL, RabbitMQ and Elasticsearch are external, the upgrade process will not upgrade these services.

Refer to v5.3.4 Compatibility & Breaking Changes for externalized MySQL, Elasticsearch and/or RabbitMQ version requirements.

Upgrade Instructions

Full HA Debian / Ubuntu Upgrade

The following covers upgrading the Morpheus App nodes in Full HA Architecture configurations to v5.3.4.

Important: The following is only for Full HA Architecture configurations, where MySQL, Elasticsearch and RabbitMQ services are external to the App nodes. The following steps assume 3 app nodes, adjust accordingly.

Morpheus Packages

Morpheus Release Package urls can be obtained from https://morpheushub.com

4.2.0+ > v5.3.4 Upgrade

Warning: Rolling upgrades are not supported for 4.2.x > 5.x upgrades

Important: Due to Database schema changes in v5.3.4 it is important to stop the morpheus-ui service on all app nodes prior to upgrade. Failure to do so may result in errors or database corruption. As a best practice, always backup your database prior to any upgrade.
Warning: Morpheus v5.3.4 contains new node and VM node packages that require 3.5GB of storage. It is safe to run `sudo rm -Rf /var/opt/morpheus/package-repos/*` after v5.3.4 package installation and before reconfigure to clean old node and vm node packages from the package-repo when room is needed.

1. Starting with App Node 3, on All App Nodes, stop the morpheus-ui services via `morpheus-ctl stop morpheus-ui`. If you receive a timeout, run `morpheus-ctl graceful-kill morpheus-ui`.

```
[root@app-server-3 ~]# morpheus-ctl stop morpheus-ui
[root@app-server-2 ~]# morpheus-ctl stop morpheus-ui
[root@app-server-1 ~]# morpheus-ctl stop morpheus-ui
```

2. Upgrade the deb package on App Node 1, then run a Reconfigure on App Node 1

```
[root@app-server-1 ~]# sudo wget https://packageUrl.morpheus-appliance_x.x.x-x_amd64.deb
[root@app-server-1 ~]# sudo dpkg -i morpheus-appliance_x.x.x-1_amd64.deb
[root@app-server-1 ~]# sudo morpheus-ctl stop morpheus-ui
[root@app-server-1 ~]# sudo morpheus-ctl reconfigure
[root@app-server-1 ~]# sudo morpheus-ctl start morpheus-ui
```

After the reconfigure has succeeded, tail the ui service to watch ui startup logs with `morpheus-ctl tail morpheus-ui`.

3. Once App Node 1 upgrade has completed and the ui is available, upgrade the deb package on App Node 2, then run a Reconfigure on App Node 2.

```
[root@app-server-2 ~]# sudo wget https://packageUrl.morpheus-appliance_x.x.x-x_amd64.deb
[root@app-server-2 ~]# sudo dpkg -i morpheus-appliance_x.x.x-1_amd64.deb
[root@app-server-1 ~]# sudo morpheus-ctl stop morpheus-ui
[root@app-server-1 ~]# sudo morpheus-ctl reconfigure
[root@app-server-1 ~]# sudo morpheus-ctl start morpheus-ui
```

After the reconfigure has succeeded, tail the ui service to watch ui startup logs with `morpheus-ctl tail morpheus-ui`.

4. Once App Node 2 upgrade has completed and the ui is available, upgrade the deb package on App Node 3, and run a Reconfigure on App Node 3.

```
[root@app-server-3 ~]# sudo wget https://packageUrl.morpheus-appliance_x.x.x-x_amd64.deb
[root@app-server-3 ~]# sudo dpkg -i morpheus-appliance_x.x.x-1_amd64.deb
[root@app-server-3 ~]# sudo morpheus-ctl reconfigure
```

5. The upgrade is complete and the Morpheus-ui services should be running on the three allocated nodes.

Important: If reconfigure after a rpm package upgrade stalls or hangs on starting a local service it is possible the `morpheus-runsvdir` service did not start or a process it was managing was manually shutdown or killed. To resolve, run `systemctl stop morpheus-runsvdir then systemctl start morpheus-runsvdir`, then run reconfigure again,`morpheus-ctl reconfigure`. 
5.0.0+ > v5.3.4 Upgrade

Note: Rolling upgrades are supported for 5.x > v5.3.4 upgrades

Warning: Morpheus v5.3.4 contains new node and VM node packages that require 3.5GB of storage. It is safe to run `sudo rm -Rf /var/opt/morpheus/package-repos/*` after v5.3.4 package installation and before reconfigure to clean old node and vm node packages from the package-repo when room is needed.

1. Starting with App Node 3, on All App Nodes, stop the morpheus-ui services via `morpheus-ctl stop morpheus-ui`. If you receive a timeout, run `morpheus-ctl graceful-kill morpheus-ui`.

2. Upgrade the deb package on App Node 1, then run a Reconfigure on App Node 1

   ```
   [root@app-server-1 ~]# sudo wget https://packageUrl.morpheus-appliance_x.x.x-x_amd64.deb
   [root@app-server-1 ~]# sudo dpkg -i morpheus-appliance_x.x.x-1_amd64.deb
   [root@app-server-1 ~]# sudo morpheus-ctl stop morpheus-ui
   [root@app-server-1 ~]# sudo morpheus-ctl reconfigure
   [root@app-server-1 ~]# sudo morpheus-ctl start morpheus-ui
   ```

   After the reconfigure has succeeded, tail the ui service to watch ui startup logs with `morpheus-ctl tail morpheus-ui`. Once morpheus-ui is started, proceed to the next node.

3. Once App Node 1 upgrade has completed and the ui is available, upgrade the deb package on App Node 2, then run a Reconfigure on App Node 2.

   ```
   [root@app-server-2 ~]# sudo wget https://packageUrl.morpheus-appliance_x.x.x-x_amd64.deb
   [root@app-server-2 ~]# sudo dpkg -i morpheus-appliance_x.x.x-1_amd64.deb
   [root@app-server-1 ~]# sudo morpheus-ctl stop morpheus-ui
   [root@app-server-1 ~]# sudo morpheus-ctl reconfigure
   [root@app-server-1 ~]# sudo morpheus-ctl start morpheus-ui
   ```

   After the reconfigure has succeeded, tail the ui service to watch ui startup logs with `morpheus-ctl tail morpheus-ui`. Once morpheus-ui is started, proceed to the next node.

4. Once App Node 2 upgrade has completed and the ui is available, upgrade the deb package on App Node 3, and run a Reconfigure on App Node 3

   ```
   [root@app-server-3 ~]# sudo wget https://packageUrl.morpheus-appliance_x.x.x-x_amd64.deb
   [root@app-server-3 ~]# sudo dpkg -i morpheus-appliance_x.x.x-1_amd64.deb
   [root@app-server-1 ~]# sudo morpheus-ctl stop morpheus-ui
   [root@app-server-1 ~]# sudo morpheus-ctl reconfigure
   [root@app-server-1 ~]# sudo morpheus-ctl start morpheus-ui
   ```

   After the reconfigure has succeeded, tail the ui service to watch ui startup logs with `morpheus-ctl tail morpheus-ui`. Once morpheus-ui is started, proceed to the next node.

5. The upgrade is complete and the Morpheus-ui services should be running on the three allocated nodes.

1.3. Upgrades & Maintenance
**Important:** If reconfigure after a rpm package upgrade stalls or hangs on starting a local service it is possible the `morpheus-runsvdir` service did not start or a process it was managing was manually shutdown or killed. To resolve, run `systemctl stop morpheus-runsvdir` then `systemctl start morpheus-runsvdir`, then run reconfigure again, `morpheus-ctl reconfigure`.

---

**Full HA RPM Upgrade**

The following covers upgrading the Morpheus App nodes in Full HA Architecture configurations to v5.3.4.

**Important:** The following is only for Full HA Architecture configurations, where MySQL, Elasticsearch and RabbitMQ services are external to the App nodes.

---

### 4.2.0+ > v5.3.4 Upgrade

**Warning:** Rolling upgrades are not supported for 4.2.x > 5.x upgrades

**Important:** Due to Database schema changes in v5.3.4 it is important to stop the morpheus-ui service on all app nodes prior to upgrade. Failure to do so may result in errors or database corruption. As a best practice, always backup your database prior to any upgrade.

**Warning:** Morpheus v5.3.4 contains new node and VM node packages that require 3.5GB of storage. It is safe to run `sudo rm -Rf /var/opt/morpheus/package-repos/*` after v5.3.4 package installation and before reconfigure to clean old node and vm node packages from the package-repo when room is needed.

1. Starting with App Node 3, on All App Nodes, stop the morpheus-ui services via `morpheus-ctl stop morpheus-ui`. If you receive a timeout, run `morpheus-ctl graceful-kill morpheus-ui`.

   ```
   [root@app-server-3 ~]# morpheus-ctl stop morpheus-ui
   [root@app-server-2 ~]# morpheus-ctl stop morpheus-ui
   [root@app-server-1 ~]# morpheus-ctl stop morpheus-ui
   ```

2. Upgrade the RPM package on App Node 1, then run a Reconfigure on App Node 1

   ```
   [root@app-server-1 ~]# sudo wget https://packageUrl.morpheus-appliance-x.x.x-x.x86_64.rpm
   [root@app-server-1 ~]# sudo rpm -Uhv morpheus-appliance-x.x.x-x.x86_64.rpm
   [root@app-server-1 ~]# sudo morpheus-ctl reconfigure
   ```

**Note:** All services will automatically be stopped and started during the reconfigure process. After the reconfigure has succeeded, tail the ui service to watch ui startup logs with `morpheus-ctl tail morpheus-ui`.
3. Once App Node 1 upgrade has completed and the ui is available, upgrade the RPM package on App Node 2, then run a Reconfigure on App Node 2.

```
[root@app-server-2 ~]# sudo wget https://packageUrl.morpheus-appliance-x.x.x-x.x86_64.rpm
[root@app-server-2 ~]# sudo rpm -Uhv morpheus-appliance-x.x.x-x.x86_64.rpm
[root@app-server-2 ~]# sudo morpheus-ctl reconfigure
```

4. Then upgrade the RPM package on App Node 3, then run a Reconfigure on App Node 3

```
[root@app-server-3 ~]# sudo wget https://packageUrl.morpheus-appliance-x.x.x-x.x86_64.rpm
[root@app-server-3 ~]# sudo rpm -Uhv morpheus-appliance-x.x.x-x.x86_64.rpm
[root@app-server-3 ~]# sudo morpheus-ctl reconfigure
```

5. The upgrade is complete and the Morpheus-ui services should be running with clustered Elasticsearch and RabbitMQ services across the 3 nodes.

**Important:** If reconfigure after a rpm package upgrade stalls or hangs on starting a local service it is possible the morpheus-runsvdir service did not start or a process it was managing was manually shutdown or killed. To resolve, run `systemctl stop morpheus-runsvdir` then `systemctl start morpheus-runsvdir`, then run reconfigure again, `morpheus-ctl reconfigure`.

### 5.0.0+ > v5.3.4 Upgrade

**Note:** Rolling upgrades are supported for 5.x > v5.3.4 upgrades

**Warning:** Morpheus v5.3.4 contains new node and VM node packages that require 3.5GB of storage. It is safe to run `sudo rm -Rf /var/opt/morpheus/package-repos/*` after v5.3.4 package installation and before reconfigure to clean old node and vm node packages from the package-repo when room is needed.

1. Upgrade the RPM package on App Node 1, then run a Reconfigure on App Node 1

```
[root@app-server-1 ~]# sudo wget https://packageUrl.morpheus-appliance-x.x.x-x.x86_64.rpm
[root@app-server-1 ~]# sudo rpm -Uhv morpheus-appliance-x.x.x-x.x86_64.rpm
[root@app-server-1 ~]# sudo morpheus-ctl stop morpheus-ui
[root@app-server-1 ~]# sudo morpheus-ctl reconfigure
[root@app-server-1 ~]# sudo morpheus-ctl start morpheus-ui
```

After the reconfigure has succeeded, tail the ui service to watch ui startup logs with `morpheus-ctl tail morpheus-ui`.

2. Once App Node 1 upgrade has completed and the ui is available, upgrade the RPM package on App Node 2, then run a Reconfigure on App Node 2.
After the reconfigure has succeeded, tail the ui service to watch ui startup logs with `morpheus-ctl tail morpheus-ui`.

3. Once App Node 2 upgrade has completed and the u is available, upgrade the RPM package on App Node 3, then run a Reconfigure on App Node 3

    [root@app-server-3 ~]# sudo wget https://packageUrl.morpheus-appliance-x.x.x-x.x86_64.rpm
    [root@app-server-3 ~]# sudo rpm -Uhv morpheus-appliance-x.x.x-x.x86_64.rpm
    [root@app-server-1 ~]# sudo morpheus-ctl stop morpheus-ui
    [root@app-server-1 ~]# sudo morpheus-ctl reconfigure
    [root@app-server-1 ~]# sudo morpheus-ctl start morpheus-ui

After the reconfigure has succeeded, tail the ui service to watch ui startup logs with `morpheus-ctl tail morpheus-ui`.

4. The upgrade is complete and the Morpheus-ui services should be running with clustered Elasticsearch and RabbitMQ services across the 3 nodes.

**Important:** If reconfigure after a rpm package upgrade stalls or hangs on starting a local service it is possible the `morpheus-runsvdir` service did not start or a process it was managing was manually shutdown or killed. To resolve, run `systemctl stop morpheus-runsvdir` then `systemctl start morpheus-runsvdir`, then run reconfigure again, `morpheus-ctl reconfigure`.

**Warning:** Upgrades can add additional storage load on database nodes. Please refer to database storage requirements within perconainstall before upgrading.

### 1.3.2 morpheus-ctl tips

`morpheus-ctl` is useful beyond reconfigures and starting the ui, and many commands can be run across all services, or scoped to a single service.

Some common commands include:

- **morpheus-ctl status** Lists all the installed services and their current status
- **morpheus-ctl start (service)** This starts all services if no service is specified, or starts the specified service. For example,
  
  • `morpheus-ctl start/stop/restart/kill` on an all-in-one appliance will start, stop, restart or kill mysql, elasticsearch, rabbitmq, check-server, guacd and the morpheus-ui, one by one.
  
  • `morpheus-ctl start/stop/restart/kill morpheus-ui` will only start, stop, restart or kill the morpheus-ui service, leaving the other service in their current state. Same goes for `morpheus-ctl start/stop/restart/kill mysql, morpheus-ctl start/stop/restart/kill elasticsearch` etc.

`morpheus-ctl` commands:
General Commands:

- cleanse
  Delete *all* morpheus data, and start from scratch.
- help
  Print this help message.
- reconfigure
  Reconfigure the application.
- show-config
  Show the configuration that would be generated by reconfigure.
- uninstall
  Kill all processes and uninstall the process supervisor (data will be preserved).

Service Management Commands:

- graceful-kill
  Attempt a graceful stop, then SIGKILL the entire process group.
- hup
  Send the services a HUP.
- int
  Send the services an INT.
- kill
  Send the services a KILL.
- once
  Start the services if they are down. Do not restart them if they stop.
- restart
  Stop the services if they are running, then start them again.
- service-list
  List all the services (enabled services appear with a *.)
- start
  Start services if they are down, and restart them if they stop.
- status
  Show the status of all the services.
- stop
  Stop the services, and do not restart them.
- tail
  Watch the service logs of all enabled services.
- term
  Send the services a TERM.

Elasticsearch Commands:

- elastic-util
  Backup/Restore ElasticSearch data

Firewall Commands:

- firewall-enable-blocking
  Enables firewall blocking mode.
1.3.3 Morpheus DB Migration

If your new installation is part of a migration or you need to move the data from your original Morpheus database, this is easily accomplished by using a stateful dump.

To begin this, stop the Morpheus UI on your original Morpheus server:

```
[root@app-server-old ~] morpheus-ctl stop morpheus-ui
```

Once this is done you can safely export. To access the MySQL shell we will need the password for the Morpheus DB user. We can find this in the morpheus-secrets file:

```
[root@app-server-old ~] cat /etc/morpheus/morpheus-secrets.json | grep morpheus_
˓→password
"morpheus_password": "451e122cr5d122asw3de5e1b", <--this one
"morpheus_password": "9b5vdj4de5awf87d",
```

Take note of the first `morpheus_password` as it will be used to invoke a dump. Morpheus provides embedded binaries for this task. Invoke it via the embedded path and specify the host. In this example we are using the morpheus database on the MySQL listening on localhost. Enter the password copied from the previous step when prompted:

```
[root@app-server-old ~] /opt/morpheus/embedded/mysql/bin/mysqldump -u morpheus -h 127.0.0.1 morpheus -p > /tmp/morpheus_backup.sql
Enter password:
```

This file needs to be pushed to the new Morpheus Installation's backend. Depending on the GRANTS in the new MySQL backend, this will likely require moving this file to one of the new Morpheus frontend servers.

Once the file is in place it can be imported into the backend. Begin by ensuring the Morpheus UI service is stopped on all of the application servers:

```
[root@app-server-new ~] morpheus-ctl stop morpheus-ui
```

Then you can import the MySQL dump into the target database using the embedded MySQL binaries, specifying the database host, and entering the password for the morpheus user when prompted:

```
[root@app-server-new ~] /opt/morpheus/embedded/mysql/bin/mysql -u morpheus -h 10.1.2.0.1 morpheus -p < /tmp/morpheus_backup.sql
Enter password:
```

The data from the old appliance is now replicated on the new appliance. Simply start the UI to complete the process:

```
[root@app-server-new ~] morpheus-ctl start morpheus-ui
```

With the migration complete, you will also need to update the stored password for the appliance backup job as the destination appliance will have a different dynamically-generated MySQL password. We can update that password value by altering the backup directly in the Morpheus database.

```
select * from backup where `name` ="Morpheus Appliance";
UPDATE `morpheus`.'backup' SET `ssh_host` = '127.0.0.1', `target_password` = 'its-a--secret' WHERE `id` = '1';
```
1.3.4 Scaling Morpheus Nodes

Morpheus App nodes can be scaled to accommodate additional load. Appliance nodes can be scaled vertically in centralized architectures, and both vertically and horizontally in distributed architectures.

Vertical Scaling

In all Appliance Architectures, Application nodes can be vertically scaled at any time, however a reconfigure must be performed for additional resources to be utilized by Morpheus on a node, which will result in the morpheus-ui restarting on the reconfiguring node.

Morpheus configures memory/ram utilization for services during the reconfigure process. If additional memory/ram is added to a Host or VM running the Morpheus App, the additional memory/ram will not be utilized by the Morpheus Application until a morpheus-ctl reconfigure command is ran and the additional memory/ram is recognized.

Important: When the morpheus-ctl reconfigure command detects changes on available memory/ram, it will restart the morpheus-ui service.

The impact on Availability depends on the Morpheus Appliance Architecture.

- **Centralized Appliances** Morpheus will be unavailable while the morpheus-ui restarts.
- **Distributed Appliances** Zero-down time can be achieved by Reconfiguring one App Node at a time, with proper Front-End Load Balancer configuration.

Horizontal Scaling

Additional Morpheus App Nodes can be added at any time to Fully Distributed Architectures.

- Configure Shared Storage paths for the new App Node(s)
- Install, but do not run the morpheus-ctl reconfigure command on the new App Node(s), using the same Morpheus version as the existing Appliance nodes.
- Copy the morpheus.rb from an existing App Node to the new App Node(s)
- Ensure permissions and network configuration for the new App Node(s) to access all MySQL and Elasticsearch nodes, and the RabbitMQ VIP.
- Ensure permissions and network configuration for all required UI services and Integrations, such as network access to ESXi hosts over 443 for Hypervisor console and/or image transfers.
- Add associated SSL files and configuration which is not on shared storage.
- Reconfigure the new App Node(s) via morpheus-ctl reconfigure
- Verify UI startup succeeded
- Add New App Node(s) to Front End Morpheus UI Load Balancer pool.

During morpheus-ctl reconfigure, the new App Node(s) will validate and be configured to use the existing tiers for the UI service. Upon successful reconfigure, the Morpheus service will be available on the App Node(s) with consistent data and capabilities.

Note: No services, including morpheus-ui, are required to be shut down on existing nodes when adding new App Nodes.
1.3.5 Morpheus UI war files

Pre-release or patched versions of the Morpheus UI are sometimes provided. To deploy the ui war on a Morpheus Appliance:

1. Download the war file to the target appliance

   
   `wget https://url/war_file`

   **Note:** If the war file is provided via a droplr link, ensure a `+` is added to end of droplr url or the file will not download

2. Backup current war file

   
   `sudo mv /opt/morpheus/lib/morpheus/morpheus-ui.war /opt/morpheus/lib/morpheus/morpheus-ui.bak.`

3. Move and rename new war file

   
   `sudo mv <file> /opt/morpheus/lib/morpheus/morpheus-ui.war`

4. Ensure war is owned by `morpheus-app`

   
   `sudo chown morpheus-app.morpheus-app /opt/morpheus/lib/morpheus/morpheus-ui.war`

5. Restart the Morpheus UI

   `sudo morpheus-ctl restart morpheus-ui`

The new ui war will load on startup!

1.4 Additional Configuration Options

1.4.1 Advanced morpheus.rb Settings

Morpheus allows for additional advanced customizations for system managed services within the morpheus.rb file located in `/etc/morpheus/morpheus.rb`. Below is a list of the supported items available in the morpheus.rb file.

**Note:** Service configuration settings are not applicable for externalized services such as external mysql/percona, elasticsearch or rabbitmq clusters. Only connection settings are applicable for external services. Additionally, to configure Morpheus to utilize alternate ports for SSL, you may have to take additional configuration steps. If simply appending a port to your `appliance_url` value doesn’t work, consult the related article in our KnowledgeBase.

```ruby
app['encrypted_key_suffix'] = 'suffix'
appliance_url 'https://morpheus.appliance-url.com'
  # Appending alternate port to appliance_url is supported. ie 'https://morpheus.appliance-url.com:8443'
  # The appliance_url cannot exceed 64 characters
  # The appliance_url must not contain a trailing `/`.
```
(continues on next page)
elasticsearch['enable'] = true
elasticsearch['es_hosts'] = {'127.0.0.1' => 9200}
elasticsearch['host'] = "127.0.0.1"
elasticsearch['use_tls'] = false
elasticsearch['auth_user'] = 'morpheus-es-user'
elasticsearch['auth_password'] = 'xxxxxxxxxxxxxxxx'
↓ Valid for Internal/System elasticsearch service only
elasticsearch['log_dir'] = '/var/log/morpheus/elasticsearch'
elasticsearch['memory_alloc_arena_max'] = 2
elasticsearch['memory_map_max'] = 65536
elasticsearch['memory_map_threshold'] = 131072
elasticsearch['memory_top_pad'] = 131072
elasticsearch['memory_trim_threshold'] = 131072
elasticsearch['open_files'] = 204800

guacd['guacamole_enabled'] = false
guacd['guacamole_enabled'] = false
logging['svlogd_num'] = 30 # keep 30 rotated log files
logging['svlogd_size'] = 209715200 # 200 MB in bytes
logging['svlogd_timeout'] = 86400 # rotate after 24 hours in seconds
mysql['enable'] = true
mysql['host'] = {'127.0.0.1' => 3306}
mysql['use_tls'] = false
mysql['morpheus_db_user'] = 'morpheus-db-user'
mysql['morpheus_db'] = 'xxxxxxxxxxxxxxxx'
↓ Valid for Internal/System mysql service only
mysql['tmp_dir'] = '/tmp/mysql'
mysql['log_dir'] = '/var/log/morpheus/mysql'
mysql['max_active'] = 100 # The combined value off all app node max_active values must be lower than max_connections setting in mysql
mysql['max_allowed_packet'] = 67108864
mysql['max_connections'] = 151
nginx['cache_max_size'] = '5000m'
nginx['enable'] = true
nginx['loading_pages']['failure_page_h1'] = 'Morpheus Server Error'
nginx['loading_pages']['failure_page_h2'] = 'Please contact your system administrator for assistance.'
nginx['loading_pages']['failure_page_title'] = 'Morpheus Server Error'
nginx['loading_pages']['iteration_time'] = 10000 # milliseconds
nginx['loading_pages']['loading_page_h1'] = 'Morpheus is Loading...' 
nginx['loading_pages']['loading_page_h2'] = 'please wait'
nginx['loading_pages']['loading_page_title'] = 'Morpheus Loading'
nginx['loading_pages']['max_loops'] = 60 # seconds
nginx['loading_pages']['timeout_page'] = '/timeout.html'
nginx['loading_pages']['timeout_page_h1'] = 'Timeout waiting for Morpheus to load,' 
nginx['loading_pages']['timeout_page_title'] = 'Morpheus timeout, please try again...'
Morpheus Documentation

(continued from previous page)

```
nginx['ssl_company_name'] = "Morpheus, LLC"
nginx['ssl_country_name'] = "US"
nginx['ssl_email_address'] = "personal@email.com"
nginx['ssl_locality_name'] = "San Mateo"
nginx['ssl_organizational_unit_name'] = "DevOps"
nginx['ssl_protocols'] = "TLSv1 TLSv1.1 TLSv1.2"
nginx['ssl_session_cache'] = "builtin:1000 shared:SSL:10m"
nginx['ssl_session_timeout'] = "5m"
nginx['ssl_state_name'] = "CA"
nginx['worker_connections'] = 10240
nginx['workers'] = integer calculated from number of cpus
nginx['log_format_name'] = 'custom'
nginx['log_format'] = '
    \$remote_addr - \$remote_user [\$time_local] \$request \n    \$status \$body_bytes_sent \$http_referer \n    \"$http_user_agent\" \n    \"$http_x_forwarded_for\" \n    rt=$request_time uct=$upstream_connect_time uht=$upstream_header_time urt=$upstream_response_time';

rabbitmq['enable'] = true
rabbitmq['host'] = '127.0.0.1'
rabbitmq['port'] = '5672'
rabbitmq['queue_user'] = 'morpheus-rmq-user'
rabbitmq['queue_user_password'] = 'xxxxxxxxxxxxxxxx'
rabbitmq['vhost'] = 'morpheus'

# Valid for Internal/System rabbitmq service only
rabbitmq['heartbeat'] = nil
rabbitmq['log_dir'] = '/var/log/morpheus/rabbitmq'
rabbitmq['nodename'] = 'rabbit@localhost'
rabbitmq['port'] = '5672'
rabbitmq['use_tls'] = false

repo['repo_host_url'] = 'https://downloads.morpheusdata.com'

ui['http_client_connect_timeout'] = 10000 # in seconds
ui['http_client_connect_timeout'] = 600000 # in seconds
ui['kerberos_config'] = nil
ui['kerberos_login_config'] = nil
ui['log_dir'] = '/var/log/morpheus/morpheus-ui'
ui['max_memory_mb'] = nil
ui['memory_alloc_arena_max'] = 2
ui['memory_map_max'] = 65536
ui['memory_map_threshold'] = 131072
ui['memory_top_pad'] = 131072
ui['memory_trim_threshold'] = 131072
ui['vm_images_cdn_url'] = 'https://morpheus-images.morpheusdata.com'
```
1.4.2 Offline Installations and Upgrades

For customers that have an appliance behind a firewall/proxy that does not allow downloads from our Amazon download site, you can add the supplemental package to add the needed packages the standard Morpheus installer would have downloaded.

**Offline Installation Requirements**

- NTP should be correctly configured and the server is able to connect to the NTP server in the ntp.conf file
- The OS package repositories should be configured to use local LAN repository servers or the server should be able to receive packages from the configured repositories
- The standard Morpheus and supplemental packages must be downloaded from another system and transferred to the Morpheus Appliance server
- The supplemental package is additive, the full installer is also required

**Note:** The supplemental package is linked 1-to-1 to the appliance release. For example the supplemental package for 4.2.1-1 should be used with the appliance package 4.2.1-1

**Offline Install**

**Ubuntu/Debian**

1. Download both the regular Morpheus Appliance package and the Supplemental packages on to the appliance server:

   ```
   wget http://example_url/morpheus-appliance_version_amd64.deb
   wget http://example_url/morpheus-appliance-supplemental_version_all.deb
   ```

2. Install the both the Appliance package AND the Supplemental package.

   ```
   sudo dpkg -i morpheus-appliance_version_amd64.deb
   sudo dpkg -i morpheus-appliance-supplemental_version_all.deb
   ```

3. Set the Morpheus UI appliance url (if needed, hostname will be automatically set).

   ```
   # edit appliance_url to resolvable url (if not configured correctly by default)
   sudo vi /etc/morpheus/morpheus.rb
   ```

4. Reconfigure the appliance to install required packages

   ```
   sudo morpheus-ctl reconfigure
   ```

The Chef run should complete successfully. There is a small pause when Chef runs the resource remote_file[package_name] action create while Chef verifies the checksum. After the reconfigure is complete, the morpheus-ui will start and be up in a few minutes.

**Note:** Tail the morpheus log file located at /var/log/morpheus/morpheus-ui/current with the command morpheus-ctl tail morpheus-ui and look for the Morpheus ascii logo to know when the morpheus-ui is up.

1.4. Additional Configuration Options
1. Download both the regular Morpheus Appliance package and the matching Supplemental package on to the Appliance server:

```
wget http://example_url/morpheus-appliance_package_url.noarch.rpm
wget http://example_url/morpheus-appliance_package_supplemental_url.noarch.rpm
```

2. Install the both the Appliance package AND the Supplemental package.

```
sudo rpm -i morpheus-appliance_package_url.noarch.rpm
sudo rpm -i morpheus-appliance_package_supplemental_url.noarch.rpm
```

3. Set the Morpheus UI appliance url (if needed, hostname will be automatically set).

```
#Edit appliance_url to resolvable url (if not configured correctly by default)
sudo vi /etc/morpheus/morpheus.rb
```

4. Reconfigure the appliance to install required packages

```
sudo morpheus-ctl reconfigure
```

The Chef run should complete successfully. There is a small pause when Chef runs the resource remote_file[package_name] action create while Chef verifies the checksum. After the reconfigure is complete, the morpheus-ui will start and be up in a few minutes.

**Note:** Tail the morpheus-ui log file with morpheus-ctl tail morpheus-ui and look for the Morpheus ascii logo to know when the morpheus-ui is up.

### 1.4.3 Proxies

**Overview**

In many situations, companies deploy virtual machines in proxy restricted environments for things such as PCI Compliance, or just general security. As a result of this Morpheus provides out of the box support for proxy connectivity. Proxy authentication support is also provided with both Basic Authentication capabilities as well as NTLM for Windows Proxy environments. Morpheus is even able to configure virtual machines it provisions to utilize these proxies by setting up the operating systems proxy settings directly (restricted to cloud-init based Linux platforms for now, but can also be done on windows based platforms in a different manner).

To get started with Proxies, it may first be important to configure the Morpheus appliance itself to have access to proxy communication for downloading service catalog images. To configure this, visit the Administration > Settings page where a section labeled “Proxy Settings” is located. Fill in the relevant connection info needed to utilize the proxy. It may also be advised to ensure that the Linux environment’s http_proxy, https_proxy, and no_proxy are set appropriately.
Defining Proxies

Proxies can be used in a few different contexts and optionally scoped to specific networks with which one may be provisioning into or on a cloud integration as a whole. To configure a Proxy for use by the provisioning engines within Morpheus we must go to Infrastructure > Networks > Proxies. Here we can create records representing connection information for various proxies. This includes the host ip address, proxy port, and any credentials (if necessary) needed to utilize the proxy. Now that these proxies are defined we can use them in various contexts.

Cloud Communication

When morpheus needs to connect to various cloud APIs to issue provisioning commands or to sync in existing environments, we need to ensure that those api endpoints are accessible by the appliance. In some cases the appliance may be behind a proxy when it comes to public cloud access like Azure and AWS. To configure the cloud integration to utilize a proxy, when adding or editing a cloud there is a setting called “API Proxy” under “Advanced Options”. This is where the proxy of choice can be selected to instruct the Provisioning engine how to communicate with the public cloud. Simply adjust this setting and the cloud should start being able to receive/issue instructions.

Provisioning with Proxies

Proxy configurations can vary from operating system to operating system and in some cases it is necessary for these to be configured in the blueprints as a prerequisite. In other cases it can also be configured automatically. Mostly with the use of cloud-init (which all of our out of the box service catalog utilizes on all clouds). When editing/creating a cloud there is a setting for “Provisioning Proxy” in “Provisioning Options”. If this proxy is set, Morpheus will automatically apply these proxy settings to the guest operating system.

Overriding proxy settings can also be done on the Network record. Networks (or subnets) can be configured in Infrastructure > Networks or on the Networks tab of the relevant Cloud detail page. Here, a proxy can also be assigned as well as additional options like the No Proxy rules for proxy exceptions.

Docker

When provisioning Docker based hosts within a Proxy environment it is up to the user to configure the docker host proxy configuration manually. There are workflows that can be configured via the Automation engine to make this automatic when creating docker based hosts. Please see documentation on Docker and proxies for specific information.

Proxy setups can vary widely from company to company, and it may be advised to contact support for help configuring morpheus to work in the proxy environment.

1.4.4 SSL Certificates

By default Morpheus generates a Self-Signed SSL Certificate. The Self-Signed SSL Certificate can be replaced with a Trusted CA Signed SSL Certificate.
Trusted CA Signed SSL Certificate Implementation

1. If you don’t already have your certificate, run an OpenSSL command to generate an SSL certificate request (.csr) and private key (.key). If you need help formatting the command, DigiCert provides a helpful tool.

2. Submit your certificate request (.csr) and await approval of the request and return of the certificate (.crt)

3. Copy the private key and certificate to /etc/morpheus/ssl/your_fqdn_name.key and /etc/morpheus/ssl/your_fqdn_name.crt respectively

   • Extracting Certificates in PFX Format
     
     ```
     # Extract the private key
     openssl pkcs12 -in example.pfx -nocerts -nodes -out priv.key
     
     # Extract the public key
     openssl pkcs12 -in example.pfx -clcerts -nokeys -out pub.crt
     
     # Extract the CA cert chain
     openssl pkcs12 -in example.pfx -cacerts -nokeys -chain -out ca.crt
     ```

   • Extracting Certificates in PEM Format
     
     ```
     # Extract the private key
     openssl x509 -outform der -in your-cert.pem -out your-cert.key
     
     # Extract the public key
     openssl x509 -outform der -in your-cert.pem -out your-cert.key
     ```

4. Edit the configuration file /etc/morpheus/morpheus.rb and add the following entries:

   ```ruby
   nginx['ssl_certificate'] = 'path to the certificate file'
   nginx['ssl_server_key'] = 'path to the server key file'
   ```

   **Note:** Both files should be owned by root and only readable by root, also if the server certificate is signed by an intermediate then you should include the signing chain inside the certificate file. The key file needs to be decrypted for Morpheus to install it properly.

5. Next simply reconfigure the appliance and restart nginx:

   ```bash
   sudo morpheus-ctl reconfigure
   sudo morpheus-ctl restart nginx
   ```
Self-Signed SSL Certificate Regeneration

When Morpheus is deployed it generates a 10 year Self-Signed SSL Certificate. Below details the process to regenerate the Certificate and Key files.

Regenerate both the Certificate and Key

1. Delete the certificate and key files in /etc/morpheus/ssl/.
2. Run Reconfigure `morpheus-ctl reconfigure`.
3. Restart NGINX `morpheus-ctl restart nginx`.

Regenerate only the Certificate

1. Delete the certificate file in /etc/morpheus/ssl/.
2. Run Reconfigure `morpheus-ctl reconfigure`.
3. Restart NGINX `morpheus-ctl restart nginx`.

1.4.5 Import Trusted Certificates

**Important:** The following applies to upgrades after modifying the java keystore.

Steps to import trusted certificates to Morpheus after an upgrade.

1. Obtain the full SSL certificate chain in PEM format.
2. Copy them to each appliance and place them in the `/etc/morpheus/ssl/trusted_certs` directory.
3. Run `morpheus-ctl reconfigure` on each appliance, note you don’t need to stop Morpheus before you run this.
4. Run the following command as root:
   ```bash
   export PATH=/opt/morpheus/sbin:/opt/morpheus/sbin:/opt/morpheus/embedded/sbin:/opt/morpheus/embedded/bin:$PATH
   ```
5. Run the following command for each certificate in the chain, adjusting the file and alias name as needed. Answer yes for the root certificate when asked if you want to trust it.
   ```bash
   /opt/morpheus/embedded/java/jre/bin/keytool -import -keystore /opt/morpheus/embedded/java/jre/lib/security/cacerts -trustcacerts -file /etc/morpheus/ssl/trusted_certs/root_ca.pem -alias some_alias -storepass changeit
   ```
6. Verify by running:
   ```bash
   openssl s_client -connect host:port -showcerts -tls1_2
   ```
7. You should get an output similar to:
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Server public key is 2048 bit
Secure Renegotiation IS supported
No ALPN negotiated
SSL-Session:
  Protocol : TLSv1.2
  Cipher : ECDHE-RSA-AES256-GCM-SHA384
  Session-ID:
    →5D9E820E4FF2A73A9977BA663E6029AA5415FEE85F49D8B1E541F5997C8E1FB2
  Session-ID-ctx:
  Master-Key:
    →29EEC2E7750C659AECB9942902D9A87B824E571522812B718420FC08F8D2ACE68CB16EC812A7D90B12A86D19706
  Key-Arg : None
  PSK identity: None
  PSK identity hint: None
  SRP username: None
  Start Time: 1547219217
  Timeout : 7200 (sec)
  Verify return code: 0 (ok) #<----------------

8. If the certificates are installed correctly you should see Verify return code: 0 (ok). If they were not installed correctly then you will see a return similar to: Verify return code: 21 (unable to verify the first certificate)

9. Repeat for all App Nodes

1.4.6 Data Encryption

By default, Morpheus encrypts sensitive data in the Database using AES encryption mode with GCM. Passwords and other strings in Morpheus Appliance configuration files such as morpheus-secrets.json and morpheus.rb are in plain text as they are only accessible by root.

Passwords and other strings in Morpheus Appliance configuration files can be set to an encrypted string using the Morpheus crypto utility to generate ENC strings and then using ENC(string) as the value in the configuration file.

Additionally a custom Encryption Key Suffix can be set in the morpheus.rb configuration file. This suffix will be combined with a system string to generate a SHA-256 hash, which is used to generate the AES encryption key.

Generate ENC Strings for morpheus-secrets.json

System generated passwords are set in /etc/morpheus/morpheus-secrets.json. These entries can be updated to ENC strings with the following steps:

1. On the Morpheus appliance, run morpheus-ctl get-crypto-string migrate which will output ENC() strings for the passwords in morpheus-secrets.json

2. Update the desired password strings in the morpheus-secrets.json config file with the matching ENC() string.

3. Save morpheus-secrets.json

4. Run morpheus-ctl reconfigure
Generate ENC Strings for custom morpheus.rb entries

ENC() strings can be generated for sensitive data set in morpheus.rb, such as the password to an external service.

To generate ENC(0) strings for morpheus.rb entries:

1. On the Morpheus appliance, run `morpheus-ctl get-crypto-string string $clear_text 'suffix'` which will output strings for the passwords in morpheus-secrets.json
   - Replace `$clear_text` with the string to be encrypted
   - If a suffix is defined in morpheus.rb (as described in the next section), replace `$suffix` with your suffix.

   **Note:** It is advisable to disable bash history logging by running `unset HISTFILE` before running the `morpheus-ctl get-crypto-string` command and then `set HISTFILE=$HOME/.bash_history` to reenable.

2. Update the desired password strings in the `morpheus.rb` config file with the matching string output, using `ENC($output)` format
   - Example: `mysql['morpheus_password'] = 'ENC($ZI5DnaO0quhxKe$kDFD+U2ZeJUyYiNC$F1+czPNy0g==)'`

3. Save `morpheus.rb`
4. Run `morpheus-ctl reconfigure`

**Encrypted Key Suffix**

A custom Encryption Key Suffix can be set in the morpheus.rb configuration file. This suffix will be combined with a system string to generate a SHA-256 Hash, which is used in the generation of the system AES encryption key.

**Danger:** Setting a custom Encryption Key Suffix affects all data encrypted by Morpheus, including database and cypher data. Encryption Key Suffix is required in the event data needs to be migrated or recovered. Once the Encryption Key Suffix is set, data cannot be recovered without it. Store any Encryption Key Suffix externally where it can be referenced for future scenarios.

**Important:** The Encryption Key Suffix cannot be changed or removed after being set. Changing or removing an existing Encryption Key Suffix will prevent data access. If an existing suffix is altered in the morpheus.rb file, it must restore to its original value.

1. Add `app['encrypted_key_suffix'] = '$suffix'` to `/etc/morpheus/morpheus.rb`, replacing `$suffix` with your suffix.
   **Danger:** Once an Encryption Key Suffix is set and applied via reconfigure, it cannot be altered or removed and data cannot be migrated or recovered without it.

2. Run `morpheus-ctl reconfigure`
   - Reconfigure will generate a new encryption key using the suffix and set (ENC) values for the service password in application.yml

1.4. Additional Configuration Options
1.5 Initial Appliance Setup

1.5.1 Appliance Setup

After installation, log into the appliance at the URL presented upon completion. An initial setup wizard walks through the first account and user creations.

1. Enter Master Account name
   - Typically, the Master Account name is your Company name.

2. Create Master User
   - First Name
   - Last Name
   - Username
   - Email Address
   - Password * Must be at least 8 characters long and contain one each of the following: Uppercase letter, lowercase letter, Number, Special Character

3. Enter Appliance Name & Appliance URL
   - The Appliance Name is used for white labeling and as a reference for multi-appliance installations.
   - The Appliance URL is the URL all provisioned instances will report back to. Example: https://example.morpheusdata.com. The Appliance URL can be changed later, and also set to a different URL per cloud integration.

4. Optionally Enable or Disable Backups, Monitoring, or Logs from this screen.

   Note: You may adjust these settings from the Administration section.

   Note: The Master Account name is the top-level admin account.

   Note: The Master User is the system super user and will have full access privileges.

Upon completing of the initial appliance setup, you will be taken to the Administration > Settings page, where you will add your License Key.

1.5.2 Login Methods

Master Tenant
   - Enter username (or email address) and password

Subtenant
To login, subtenants can either use the master tenant URL with subtenant\username formatting:

Example: I have a username subuser that belongs to a tenant with the subdomain subaccount. When logging in from the main login url, I would now need to enter in: subaccount\subuser
Or use the tenant specific URL which can be found and configured under Administration > Tenants > Select Tenant > Identity Sources.

Important: In 3.4.0+ Subtenant users will no longer be able to login from the main login url without specifying their subdomain.

### 1.5.3 Configure Cloud-init Global Settings

When using cloud-init, cloudbase-init, VMware Tools customizations, or Nutanix Sysprep, Global Linux User and Windows Administrator credentials can be set using the settings in Administration > Settings > Provisioning. It is recommended to define these settings after installation unless credentials are defined per Virtual Image for Provisioning.

### 1.5.4 Add a License Key

In order to provision anything in Morpheus, a Morpheus License Key must be applied.

If you do not already have a license key, one may be requested from https://www.morpheushub.com or from your Morpheus representative.

In the Administration > Settings section, select the LICENSE tab, paste your License Key and click *UPDATE*
When the license is accepted, your license details will populate in the Current License section.
If you receive an error message and your license is not accepted, please check it was copied in full and then contact your Morpheus representative. You can also verify the License Key and expiration at https://www.morpheushub.com.

1.6 Core Functionality

1.6.1 Morpheus Discovery

Morpheus has the ability to ingest existing environments. Existing running workloads will be inventoried into Morpheus and displayed in the UI. In 5-7 days Morpheus will start making recommendations based off of usage and pricing.

Note: Workloads that are inventoried do not have to be converted to managed.

Once inventoried, Morpheus can provide valuable data for that instance:

- Morpheus will know about networks
- Start aggregating cost on public clouds
- Start tracking usage
- Some Clouds offer statistical details (Amazon / VMware)
- Power Status
Right away inventorying existing environments will provide you with immediate insight to that environment. Once an existing workload has been discovered it can be converted to managed. Once converted to managed, Morpheus can deliver more capabilities and features.

**Note:** Workloads do not need the agent installed to be managed

Once a workload is managed:

- Enforce expiration/shutdown policies. This helps reign in environments (sprawl) and reduce cost.
- Can tell what instance type it is
- Can install agent (agent is optional)
- Installing agent provides credentials and allows you to run workflows against it (day 2 operations)

### 1.6.2 Morpheus Agent

**Overview**

The Morpheus Agent is an important and powerful facet of Morpheus as an orchestration tool. Though it is not required, which is one unique capability of our platform versus some of our competitors, it is recommended for use as it brings many benefits. Not only does it provide statistics for the guest operating system and resource utilization, it also brings along with it monitoring and log aggregation capabilities. After an initial brownfield discovery, Users can decide to convert unmanaged VMs to managed.

**Note:** Agent installation is not required to manage an Instance. If you don’t have the Agent installed, we make every effort to aggregate stats. These will vary based on the Cloud and can be more limited or less accurate without utilizing Morpheus Agent.

The Morpheus Agent is very lightweight and secure. It does not open any inbound network ports but rather only opens an outbound connection back to the Morpheus appliance over port 443 (HTTPS or WSS protocol). This allows for a bidirectional command bus where instructions can be sent to orchestrate a workload without needing access to things like SSH or WinRM. The tool can even be installed at provision time via technologies like Cloud-Init, such that the Morpheus appliance itself doesn’t even need direct network access to the VLAN under which the workload resides. By doing this we address many of the network security concerns that come with the use of an agent while demonstrating its security and analytics benefits. We can even use this statistical data at the guest OS level rather than the hypervisor level to provide extremely precise right-sizing recommendations.

**Morpheus Agent Key Features**

**Key Enhanced Statistics and Benefits**
### Morpheus Documentation

<table>
<thead>
<tr>
<th>Category</th>
<th>Statistic</th>
<th>With Agent</th>
<th>Without Agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory</td>
<td>Max Memory</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Memory</td>
<td>Used Memory</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Memory</td>
<td>Cache Memory</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Storage</td>
<td>Max Storage</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Storage</td>
<td>Used Memory</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Processing</td>
<td>System CPU %</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Processing</td>
<td>User CPU %</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>IOPS</td>
<td>Total IOPS</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>IOPS</td>
<td>IOPS Read</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>IOPS</td>
<td>IOPS Write</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Networking</td>
<td>Net TX Rate</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Networking</td>
<td>Net RX Rate</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Other</td>
<td>Agent Command Bus</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Other</td>
<td>Log Aggregation</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Other</td>
<td>Health &amp; Monitoring</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Additional benefits:**

- Installation is optional for provisioned and managed VMs
- The Linux agent can be shrunk and should be less than 0.2% peak
- Provides a command bus such that Morpheus doesn’t need credentials to access a box
- Can still manage workflows if credentials are changed
- SSH agent can be disabled and still get access to the box
- Agent can be installed over Cloud-init, Windows unattend.xml, VMware Tools, SSH, WinRM, Cloudbase-Init, or manually
- Makes a single, persistent connection over HTTPS websocket and runs as a service
- Buffers and compresses logs, then sends them in chunks to minimize packets
- Supports syslog forwarding
- Accepts commands, executes commands, writes files, and manipulates firewalls
- Significantly enhances Guidance recommendations through enhanced statistics

**Note:** The Morpheus Agent is required for managed Docker, Kubernetes, SCVMM, Hyper-V, KVM, and ESXi Hosts (for ESXi-only Cloud, not vCenter Clouds).

### Morpheus Agent OS Support

<table>
<thead>
<tr>
<th>Name</th>
<th>Bit Count</th>
<th>Category</th>
<th>Code</th>
<th>OS Family</th>
<th>OS Version</th>
<th>Platform</th>
<th>Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>amazon linux 2 64-bit</td>
<td>64</td>
<td>amazonlinux</td>
<td>amazonlinux.2.64</td>
<td>centos</td>
<td>2</td>
<td>linux</td>
<td>amazon</td>
</tr>
<tr>
<td>CentOS</td>
<td>64</td>
<td>centos</td>
<td>cent</td>
<td>rhel</td>
<td>all</td>
<td>linux</td>
<td>cent</td>
</tr>
<tr>
<td>CentOS 6</td>
<td>64</td>
<td>centos</td>
<td>cent.6</td>
<td>rhel</td>
<td>6</td>
<td>linux</td>
<td>cent</td>
</tr>
<tr>
<td>CentOS 6 64-bit</td>
<td>64</td>
<td>centos</td>
<td>cent.6.64</td>
<td>rhel</td>
<td>6</td>
<td>linux</td>
<td>cent</td>
</tr>
<tr>
<td>centOS 64-bit</td>
<td>64</td>
<td>centos</td>
<td>cent.64</td>
<td>rhel</td>
<td>all</td>
<td>linux</td>
<td>cent</td>
</tr>
<tr>
<td>CentOS 7</td>
<td>64</td>
<td>centos</td>
<td>cent.7</td>
<td>rhel</td>
<td>7</td>
<td>linux</td>
<td>cent</td>
</tr>
</tbody>
</table>
Table 5 – continued from previous page

<table>
<thead>
<tr>
<th>Name</th>
<th>Bit Count</th>
<th>Category</th>
<th>Code</th>
<th>OS Family</th>
<th>OS Version</th>
<th>Platform</th>
<th>Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>centOS 7 64-bit</td>
<td>64</td>
<td>centos</td>
<td>cent.7.64</td>
<td>rhel</td>
<td>7</td>
<td>linux</td>
<td>centos</td>
</tr>
<tr>
<td>centOS 8 64-bit</td>
<td>64</td>
<td>centos</td>
<td>cent.8.64</td>
<td>rhel</td>
<td>8</td>
<td>linux</td>
<td>centos</td>
</tr>
<tr>
<td>debian</td>
<td>32</td>
<td>debian</td>
<td>debian</td>
<td>debian</td>
<td>all</td>
<td>linux</td>
<td>debian</td>
</tr>
<tr>
<td>debian 6</td>
<td>32</td>
<td>debian</td>
<td>debian.6</td>
<td>debian</td>
<td>6</td>
<td>linux</td>
<td>debian</td>
</tr>
<tr>
<td>debian 6 64-bit</td>
<td>64</td>
<td>debian</td>
<td>debian.6.64</td>
<td>debian</td>
<td>6</td>
<td>linux</td>
<td>debian</td>
</tr>
<tr>
<td>debian 64-bit</td>
<td>64</td>
<td>debian</td>
<td>debian.64</td>
<td>debian</td>
<td>all</td>
<td>linux</td>
<td>debian</td>
</tr>
<tr>
<td>debian 7</td>
<td>32</td>
<td>debian</td>
<td>debian.7</td>
<td>debian</td>
<td>7</td>
<td>linux</td>
<td>debian</td>
</tr>
<tr>
<td>debian 7 64-bit</td>
<td>64</td>
<td>debian</td>
<td>debian.7.64</td>
<td>debian</td>
<td>7</td>
<td>linux</td>
<td>debian</td>
</tr>
<tr>
<td>debian 8</td>
<td>32</td>
<td>debian</td>
<td>debian.8</td>
<td>debian</td>
<td>8</td>
<td>linux</td>
<td>debian</td>
</tr>
<tr>
<td>debian 8 64-bit</td>
<td>64</td>
<td>debian</td>
<td>debian.8.64</td>
<td>debian</td>
<td>8</td>
<td>linux</td>
<td>debian</td>
</tr>
<tr>
<td>debian 9.4 64-bit</td>
<td>64</td>
<td>debian</td>
<td>debian.9.4.64</td>
<td>debian</td>
<td>9</td>
<td>linux</td>
<td>debian</td>
</tr>
<tr>
<td>esxi 4</td>
<td>64</td>
<td>esxi</td>
<td>esxi.4</td>
<td>NULL</td>
<td>4</td>
<td>esxi</td>
<td>vmware</td>
</tr>
<tr>
<td>esxi 5</td>
<td>64</td>
<td>esxi</td>
<td>esxi.5</td>
<td>NULL</td>
<td>5</td>
<td>esxi</td>
<td>vmware</td>
</tr>
<tr>
<td>esxi 6</td>
<td>64</td>
<td>esxi</td>
<td>esxi.6</td>
<td>NULL</td>
<td>6</td>
<td>esxi</td>
<td>vmware</td>
</tr>
<tr>
<td>fedora</td>
<td>32</td>
<td>fedora</td>
<td>fedora.64</td>
<td>NULL</td>
<td>all</td>
<td>linux</td>
<td>fedora</td>
</tr>
<tr>
<td>fedora 64-bit</td>
<td>64</td>
<td>fedora</td>
<td>fedora.64</td>
<td>NULL</td>
<td>all</td>
<td>linux</td>
<td>fedora</td>
</tr>
<tr>
<td>linux</td>
<td>64</td>
<td>linux</td>
<td>linux</td>
<td>NULL</td>
<td>all</td>
<td>linux</td>
<td>linux</td>
</tr>
<tr>
<td>linux 32-bit</td>
<td>32</td>
<td>linux</td>
<td>linux.32</td>
<td>NULL</td>
<td>all</td>
<td>linux</td>
<td>linux</td>
</tr>
<tr>
<td>linux 64-bit</td>
<td>64</td>
<td>linux</td>
<td>linux.64</td>
<td>NULL</td>
<td>all</td>
<td>linux</td>
<td>linux</td>
</tr>
<tr>
<td>mac os</td>
<td>64</td>
<td>mac</td>
<td>mac</td>
<td>NULL</td>
<td>all</td>
<td>osx</td>
<td>apple</td>
</tr>
<tr>
<td>opensuse</td>
<td>32</td>
<td>opensuse</td>
<td>opensuse.32</td>
<td>suse</td>
<td>all</td>
<td>linux</td>
<td>opensuse</td>
</tr>
<tr>
<td>opensuse 15 64-bit</td>
<td>64</td>
<td>opensuse</td>
<td>opensuse.15.64</td>
<td>suse</td>
<td>15</td>
<td>linux</td>
<td>opensuse</td>
</tr>
<tr>
<td>opensuse 64-bit</td>
<td>64</td>
<td>opensuse</td>
<td>opensuse.64</td>
<td>suse</td>
<td>all</td>
<td>linux</td>
<td>opensuse</td>
</tr>
<tr>
<td>oracle enterprise</td>
<td>32</td>
<td>oracle</td>
<td>oracle.32</td>
<td>NULL</td>
<td>all</td>
<td>linux</td>
<td>oracle</td>
</tr>
<tr>
<td>oracle enterprise 64-bit</td>
<td>64</td>
<td>oracle</td>
<td>oracle.64</td>
<td>NULL</td>
<td>all</td>
<td>linux</td>
<td>oracle</td>
</tr>
<tr>
<td>oracle linux 64-bit</td>
<td>64</td>
<td>oracle</td>
<td>oracle.linux.64</td>
<td>NULL</td>
<td>all</td>
<td>linux</td>
<td>oracle</td>
</tr>
<tr>
<td>oracle vm server</td>
<td>64</td>
<td>oracle</td>
<td>ovs</td>
<td>NULL</td>
<td>all</td>
<td>linux</td>
<td>oracle</td>
</tr>
<tr>
<td>other 32-bit</td>
<td>32</td>
<td>other</td>
<td>other.32</td>
<td>NULL</td>
<td>all</td>
<td>other</td>
<td>other</td>
</tr>
<tr>
<td>other 64-bit</td>
<td>64</td>
<td>other</td>
<td>other.64</td>
<td>NULL</td>
<td>all</td>
<td>other</td>
<td>other</td>
</tr>
<tr>
<td>redhat</td>
<td>64</td>
<td>redhat</td>
<td>redhat</td>
<td>rhel</td>
<td>all</td>
<td>linux</td>
<td>redhat</td>
</tr>
<tr>
<td>redhat 6</td>
<td>64</td>
<td>redhat</td>
<td>redhat.6</td>
<td>rhel</td>
<td>6</td>
<td>linux</td>
<td>redhat</td>
</tr>
<tr>
<td>redhat 6 64-bit</td>
<td>64</td>
<td>redhat</td>
<td>redhat.6.64</td>
<td>rhel</td>
<td>6</td>
<td>linux</td>
<td>redhat</td>
</tr>
<tr>
<td>redhat 64-bit</td>
<td>64</td>
<td>redhat</td>
<td>redhat.64</td>
<td>rhel</td>
<td>all</td>
<td>linux</td>
<td>redhat</td>
</tr>
<tr>
<td>redhat 7</td>
<td>64</td>
<td>redhat</td>
<td>redhat.7</td>
<td>rhel</td>
<td>7</td>
<td>linux</td>
<td>redhat</td>
</tr>
<tr>
<td>redhat 7 64-bit</td>
<td>64</td>
<td>redhat</td>
<td>redhat.7.64</td>
<td>rhel</td>
<td>7</td>
<td>linux</td>
<td>redhat</td>
</tr>
<tr>
<td>redhat 8 64-bit</td>
<td>64</td>
<td>redhat</td>
<td>redhat.8.64</td>
<td>rhel</td>
<td>8</td>
<td>linux</td>
<td>redhat</td>
</tr>
<tr>
<td>solaris</td>
<td>32</td>
<td>solaris</td>
<td>solaris.32</td>
<td>NULL</td>
<td>all</td>
<td>solaris</td>
<td>solaris</td>
</tr>
<tr>
<td>solaris 64-bit</td>
<td>64</td>
<td>solaris</td>
<td>solaris.64</td>
<td>NULL</td>
<td>all</td>
<td>solaris</td>
<td>solaris</td>
</tr>
<tr>
<td>suse enterprise</td>
<td>32</td>
<td>suse</td>
<td>suse</td>
<td>suse</td>
<td>all</td>
<td>linux</td>
<td>suse</td>
</tr>
<tr>
<td>suse enterprise 11</td>
<td>32</td>
<td>suse</td>
<td>suse.11</td>
<td>suse</td>
<td>11</td>
<td>linux</td>
<td>suse</td>
</tr>
<tr>
<td>suse enterprise 11 64-bit</td>
<td>64</td>
<td>suse</td>
<td>suse.11.64</td>
<td>suse</td>
<td>11</td>
<td>linux</td>
<td>suse</td>
</tr>
<tr>
<td>suse enterprise 12</td>
<td>32</td>
<td>suse</td>
<td>suse.12</td>
<td>suse</td>
<td>12</td>
<td>linux</td>
<td>suse</td>
</tr>
<tr>
<td>suse enterprise 12 64-bit</td>
<td>64</td>
<td>suse</td>
<td>suse.12.64</td>
<td>suse</td>
<td>12</td>
<td>linux</td>
<td>suse</td>
</tr>
<tr>
<td>suse enterprise 15 64-bit</td>
<td>64</td>
<td>suse</td>
<td>suse.12.64</td>
<td>suse</td>
<td>12</td>
<td>linux</td>
<td>suse</td>
</tr>
<tr>
<td>suse enterprise 64-bit</td>
<td>64</td>
<td>suse</td>
<td>suse.64</td>
<td>suse</td>
<td>all</td>
<td>linux</td>
<td>suse</td>
</tr>
<tr>
<td>ubuntu</td>
<td>32</td>
<td>ubuntu</td>
<td>ubuntu</td>
<td>debian</td>
<td>all</td>
<td>linux</td>
<td>ubuntu</td>
</tr>
<tr>
<td>ubuntu 12</td>
<td>32</td>
<td>ubuntu</td>
<td>ubuntu.12</td>
<td>debian</td>
<td>12.04</td>
<td>linux</td>
<td>ubuntu</td>
</tr>
<tr>
<td>ubuntu 12 64-bit</td>
<td>64</td>
<td>ubuntu</td>
<td>ubuntu.12.04</td>
<td>debian</td>
<td>12.04</td>
<td>linux</td>
<td>ubuntu</td>
</tr>
<tr>
<td>ubuntu 13</td>
<td>32</td>
<td>ubuntu</td>
<td>ubuntu.13.10</td>
<td>debian</td>
<td>13.1</td>
<td>linux</td>
<td>ubuntu</td>
</tr>
</tbody>
</table>

1.6. Core Functionality

---

---
Table 5 – continued from previous page

<table>
<thead>
<tr>
<th>Name</th>
<th>Bit Count</th>
<th>Category</th>
<th>Code</th>
<th>OS Family</th>
<th>OS Version</th>
<th>Platform</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>ubuntu 13 64-bit</td>
<td>64</td>
<td>ubuntu</td>
<td>ubuntu.13.10.64</td>
<td>debian</td>
<td>13.1</td>
<td>linux</td>
<td>canonical</td>
</tr>
<tr>
<td>ubuntu 14</td>
<td>32</td>
<td>ubuntu</td>
<td>ubuntu.14.04</td>
<td>debian</td>
<td>14.04</td>
<td>linux</td>
<td>canonical</td>
</tr>
<tr>
<td>ubuntu 14 64-bit</td>
<td>64</td>
<td>ubuntu</td>
<td>ubuntu.14.04.64</td>
<td>debian</td>
<td>14.04</td>
<td>linux</td>
<td>canonical</td>
</tr>
<tr>
<td>ubuntu 15</td>
<td>32</td>
<td>ubuntu</td>
<td>ubuntu.15.10</td>
<td>debian</td>
<td>15.1</td>
<td>linux</td>
<td>canonical</td>
</tr>
<tr>
<td>ubuntu 15 64-bit</td>
<td>64</td>
<td>ubuntu</td>
<td>ubuntu.15.10.64</td>
<td>debian</td>
<td>15.1</td>
<td>linux</td>
<td>canonical</td>
</tr>
<tr>
<td>ubuntu 16</td>
<td>32</td>
<td>ubuntu</td>
<td>ubuntu.16.04</td>
<td>debian</td>
<td>16.04</td>
<td>linux</td>
<td>canonical</td>
</tr>
<tr>
<td>ubuntu 16 64-bit</td>
<td>64</td>
<td>ubuntu</td>
<td>ubuntu.16.04.64</td>
<td>debian</td>
<td>16.04</td>
<td>linux</td>
<td>canonical</td>
</tr>
<tr>
<td>ubuntu 18.04</td>
<td>32</td>
<td>ubuntu</td>
<td>ubuntu.18.04</td>
<td>debian</td>
<td>18.04</td>
<td>linux</td>
<td>canonical</td>
</tr>
<tr>
<td>ubuntu 18.04 64-bit</td>
<td>64</td>
<td>ubuntu</td>
<td>ubuntu.18.04.64</td>
<td>debian</td>
<td>18.04</td>
<td>linux</td>
<td>canonical</td>
</tr>
<tr>
<td>ubuntu 20.04</td>
<td>32</td>
<td>ubuntu</td>
<td>ubuntu.20.04</td>
<td>debian</td>
<td>20.04</td>
<td>linux</td>
<td>canonical</td>
</tr>
<tr>
<td>ubuntu 20.04 64-bit</td>
<td>64</td>
<td>ubuntu</td>
<td>ubuntu.20.04.64</td>
<td>debian</td>
<td>20.04</td>
<td>linux</td>
<td>canonical</td>
</tr>
<tr>
<td>ubuntu 64-bit</td>
<td>64</td>
<td>ubuntu</td>
<td>ubuntu.64</td>
<td>debian</td>
<td>all</td>
<td>linux</td>
<td>canonical</td>
</tr>
<tr>
<td>unknown</td>
<td>64</td>
<td>other</td>
<td>unknown</td>
<td>NULL</td>
<td>all</td>
<td>unknown</td>
<td>unknown</td>
</tr>
<tr>
<td>windows</td>
<td>64</td>
<td>windows</td>
<td>windows</td>
<td>windows</td>
<td>all</td>
<td>windows</td>
<td>microsoft</td>
</tr>
<tr>
<td>windows 10</td>
<td>32</td>
<td>windows</td>
<td>windows.10</td>
<td>windows</td>
<td>10</td>
<td>windows</td>
<td>microsoft</td>
</tr>
<tr>
<td>windows 10 64-bit</td>
<td>64</td>
<td>windows</td>
<td>windows.10.64</td>
<td>windows</td>
<td>10</td>
<td>windows</td>
<td>microsoft</td>
</tr>
<tr>
<td>windows 7</td>
<td>32</td>
<td>windows</td>
<td>windows.7</td>
<td>windows</td>
<td>7</td>
<td>windows</td>
<td>microsoft</td>
</tr>
<tr>
<td>windows 7 64-bit</td>
<td>64</td>
<td>windows</td>
<td>windows.7.64</td>
<td>windows</td>
<td>7</td>
<td>windows</td>
<td>microsoft</td>
</tr>
<tr>
<td>windows 8</td>
<td>32</td>
<td>windows</td>
<td>windows.8</td>
<td>windows</td>
<td>8</td>
<td>windows</td>
<td>microsoft</td>
</tr>
<tr>
<td>windows 8 64-bit</td>
<td>64</td>
<td>windows</td>
<td>windows.8.64</td>
<td>windows</td>
<td>8</td>
<td>windows</td>
<td>microsoft</td>
</tr>
<tr>
<td>windows server 2003</td>
<td>64</td>
<td>windows</td>
<td>windows.server.2003</td>
<td>windows</td>
<td>2003</td>
<td>windows</td>
<td>microsoft</td>
</tr>
<tr>
<td>windows server 2008</td>
<td>64</td>
<td>windows</td>
<td>windows.server.2008</td>
<td>windows</td>
<td>2008</td>
<td>windows</td>
<td>microsoft</td>
</tr>
<tr>
<td>windows server 2008 R2</td>
<td>64</td>
<td>windows</td>
<td>windows.server.2008.r2</td>
<td>windows</td>
<td>2008</td>
<td>windows</td>
<td>microsoft</td>
</tr>
<tr>
<td>windows server 2012</td>
<td>64</td>
<td>windows</td>
<td>windows.server.2012</td>
<td>windows</td>
<td>2012</td>
<td>windows</td>
<td>microsoft</td>
</tr>
<tr>
<td>windows server 2016</td>
<td>64</td>
<td>windows</td>
<td>windows.server.2016</td>
<td>windows</td>
<td>2016</td>
<td>windows</td>
<td>microsoft</td>
</tr>
<tr>
<td>windows server 2019</td>
<td>64</td>
<td>windows</td>
<td>windows.server.2019</td>
<td>windows</td>
<td>2019</td>
<td>windows</td>
<td>microsoft</td>
</tr>
<tr>
<td>xen server 6.1</td>
<td>64</td>
<td>xen</td>
<td>xenserver.6.1</td>
<td>xen</td>
<td>6.1</td>
<td>linux</td>
<td>xen</td>
</tr>
<tr>
<td>xen server 6.2</td>
<td>64</td>
<td>xen</td>
<td>xenserver.6.2</td>
<td>xen</td>
<td>6.2</td>
<td>linux</td>
<td>xen</td>
</tr>
<tr>
<td>xen server 6.5</td>
<td>64</td>
<td>xen</td>
<td>xenserver.6.5</td>
<td>xen</td>
<td>6.5</td>
<td>linux</td>
<td>xen</td>
</tr>
<tr>
<td>xen server 7.0</td>
<td>64</td>
<td>xen</td>
<td>xenserver.7.0</td>
<td>xen</td>
<td>7</td>
<td>linux</td>
<td>xen</td>
</tr>
</tbody>
</table>

**Note:** Other Operating System types may be supported but are not tested.

**Agent Installation**

There are many methods to install the Morpheus Agent on supported targets. All Agent installation methods are executing a script on the target that calls back to the Morpheus appliance over port 443.

**Important:** All Agent installation methods require the Target (VM or Host) to resolve and reach the appliance URL over port 443. In addition to the main Appliance URL (in Administration > Settings), additional Appliance URLs can be set per cloud in the Advanced Options section of the Create/Edit Cloud modal. When this field is populated, it will override the main Appliance URL for anything provisioned into that Cloud.
Basic Installation Steps

1. An Agent installation method is used to get the install script onto the target VM or Host
2. The Agent installation script is executed on the target VM or Host, installing the Agent and all dependencies
3. The Agent is started and makes a websocket connection to the configured Appliance URL over port 443 using the target VM or Host API key

It is important to note these are three separate steps with varying requirements. The first requires a path to get the script on the target. The second requires successful execution of the Agent installation script. The third requires a successful websocket connection. Requirements for the successful execution of each step are covered in the sections below.

Tip: The Morpheus UI current log, located at /var/log/morpheus/morpheus-ui/current, is very helpful when troubleshooting Agent installations.

Agent Install Modes

Agent Installation Method is determined by:

- The AGENT INSTALL MODE setting on target Cloud: - SSH / WinRM / Guest Execution - Cloud Init / Unattend (when available)
- Platform / OS type on Virtual Image or target (VM or Host)
- Virtual Image configuration
- RPC Mode setting (VMware Clouds only)

Agent Installation Methods

The Morpheus Agent can be installed with a variety of automated methods. It is important to note these methods simply get the Agent install script to the target. Successful execution of the Agent install script is not directly related to the Agent install method.

**SSH** Morpheus makes an SSH connection to the VM or Host, CURLs, and executes the Agent install script:

```
curl -k -s "https://${applianceUrl}/api/server-script/agentInstall?
apiKey=${apiKey}" | bash
```

**WinRM** Morpheus makes a WinRM connection to the VM or Host and executes the Agent install script

**VMware Tools** Morpheus executes agentInstall.sh or agentInstall.ps1 via VMware Tools Guest Execution

**Cloud-Init** Morpheus executes agentInstall.sh via cloud-init runcmd

**Cloudbase-Init** Morpheus adds WindowsAgentCloudInitInstallScript to CloudbaseInitUserData

**Windows Unattend** Morpheus adds getWindowsAgentDownloadScript to unattend.xml (RunSynchronousCommand)

**Manual** User executes agentInstall.sh or agentInstall.ps1 manually on the VM or Host. These scripts can be obtained on the VM or Host detail page via Actions > Download Agent Script
SSH

**Process**

Morpheus makes an SSH connection to the VM or Host, CURLs, and executes the Agent install script:

```
curl -k -s "https://${applianceUrl}/api/server-script/agentInstall?apiKey=${apiKey}" | bash
```

**Requirements**

- Port 22 is open for Linux images, and SSH is enabled
- Credentials have been entered on the image if using a custom or synced image. Credentials can be entered on images in the Library > Virtual Images section

WinRM

**Process**

Morpheus makes a WinRM connection to the VM or Host and executes the Agent install script

**Requirements**

- Port 5985 must be open and WinRM enabled for Windows images
- Credentials have been entered on the image if using a custom or synced image. Credentials can be entered on images in the Library > Virtual Images section
- Administrator User (SID 500) is required for Windows Agent install

VMware Tools

**Process**

Morpheus executes agentInstall.sh or agentInstall.ps1 via VMware Tools Guest Execution

**Requirements**

- VMware Tools is installed on the template(s)
- Credentials have been entered on the Image if using an uploaded or synced image when Cloud-init, Guest Customizations, or Sysprep for Windows are not used. Credentials can be entered on Images in the Library > Virtual Images section
- Administrator User (SID 500) is required for Windows Agent install.
Cloud-Init

Process

Morpheus executes agentInstall.sh via Cloud-Init runcmd

Requirements

- Cloud-Init is installed on Virtual Image
- “IS CLOUD INIT ENABLED?” is checked (true) on the Morpheus Virtual Image record
- Cloud-Init User is configured in the Administration > Settings > Provisioning section

Cloudbase-init

Process

Morpheus adds WindowsAgentCloudInitInstallScript to CloudbaseInitUserData

Requirements

- Cloudbase-Init is installed on the Virtual Image
- “IS CLOUD INIT ENABLED?” is checked (true) on the Morpheus Virtual Image record
- Windows Administrator password defined in the Administration > Settings > Provisioning section

Windows Unattend

Process

Morpheus adds getWindowsAgentDownloadScript to unattend.xml (RunSynchronousCommand)

Requirements

VMware

- Windows Administrator password defined in the Administration > Settings > Provisioning section OR Administrator User (SID 500) and valid Windows password are defined on the Morpheus Virtual Image record
- “FORCE GUEST CUSTOMIZATION?” is checked (true) on the Morpheus Virtual Image record when using DHCP
- “IS CLOUD INIT ENABLED?” is unchecked (false) on the Morpheus Virtual Image record

Nutainx/SCVMM/Openstack

- Windows Administrator password defined in the Administration > Settings > Provisioning section OR Administrator User (SID 500) and valid Windows password are defined on the Morpheus Virtual Image record

1.6. Core Functionality
• “ENABLED SYSPREP?” is checked (true) on the Morpheus Virtual Image record
• “IS CLOUD INIT ENABLED?” is unchecked (false) on the Morpheus Virtual Image record

Manual

Process

• From the VM or Host record page (/infrastructure/servers/${id}) run ACTIONS > Download Agent Script
• This is will generate an Agent install script based off the target OS and platform, Appliance URL, and API key
• Manually execute the downloaded script on the Target VM or Host
## Agent Install Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Agent Installation Method</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Requirement</strong></td>
<td>SSH</td>
</tr>
<tr>
<td>Target (vm/host) to resolve and reach Appliance URL over 443</td>
<td>YES</td>
</tr>
<tr>
<td>Target (vm/host) to resolve and reach Appliance URL over 80</td>
<td>Ubuntu 14.04 Only</td>
</tr>
<tr>
<td>Websockets enabled when using load balancer</td>
<td>YES</td>
</tr>
<tr>
<td>Access to Target VM/Host on port 22</td>
<td>YES</td>
</tr>
<tr>
<td>Access to Target VM/Host on port 5985</td>
<td>NO</td>
</tr>
<tr>
<td>Vmware Tools installed and flagged on Virtual Image</td>
<td>NO</td>
</tr>
<tr>
<td>Syspreped Image and Sysprep Enabled flagged on Virtual Image (Nutanix, Openstack, SCVMM)</td>
<td>NO</td>
</tr>
<tr>
<td>Force Guest Customizations flagged on Virtual Image</td>
<td>NO</td>
</tr>
<tr>
<td>Cloud-Init installed and flagged on Virtual Image</td>
<td>NO</td>
</tr>
<tr>
<td>Global Cloud-Init user populated in Administration &gt; Settings &gt; Provisioning</td>
<td>NO</td>
</tr>
<tr>
<td>Windows Administrator Password populated in Administration &gt; Settings &gt; Provisioning</td>
<td>NO</td>
</tr>
<tr>
<td>Access to configured YUM or APT repos</td>
<td>NO</td>
</tr>
<tr>
<td>.net &gt;=4.5.2 (Windows, Morpheus &gt;= 4.1.2)</td>
<td>N/A</td>
</tr>
<tr>
<td>User with Sudo Access set on Virtual Image (Greenfield)</td>
<td>YES</td>
</tr>
<tr>
<td>Administrator User (SID 500) set on Virtual Image (Greenfield)</td>
<td>N/A</td>
</tr>
<tr>
<td>User with Sudo Access set on VM/Host Record (Brownfield)</td>
<td>YES</td>
</tr>
</tbody>
</table>
| Administrator User (SID 500) set on VM/Host Record (Brownfield)             | N/A | YES   | YES          | N/A        | N/A         | N/A      | N/A
When provisioning an Instance, there are network and configuration requirements to consider in order to successfully install the Morpheus Agent. Typically, when a VM Instance is still in the provisioning phase long after the VM is up, the Instance is unable to reach Morpheus. Depending on the Agent install mode, it could also mean Morpheus is unable to reach the Instance.

The most common reason an Agent install fails is the provisioned Instance cannot reach the Morpheus Appliance via the Appliance URL set in Administration > Settings over port 443. When an Instance is provisioned from Morpheus, it must be able to reach the Morpheus appliance via the Appliance URL or the Agent will not be installed.

In addition to the main Appliance URL in Administration > Settings, additional Appliance URLs can be set per Cloud in the Advanced Options section of the Cloud configuration modal when creating or editing a Cloud. When this field is populated, it will override the main Appliance URL for anything provisioned into that Cloud.

**Tip:** The Morpheus UI current log, located at /var/log/morpheus/morpheus-ui/current, is very helpful when troubleshooting Agent installations.

**Agent Install Methods**

Morpheus Agent installation supports multiple install methods.

- SSH/WinRM
- VM Tools
- Cloud-Init & Cloudbase-Init
- Windows Unattended
- Manual
For All Agent Install Methods

When an Instance is provisioned and the Agent does not install, verify the following for any Agent install mode:

- The Morpheus Appliance URL (Administration > Settings) is both reachable and resolvable from the provisioned node

**Note:** Be sure to use `https://` even when using an IP address for the appliance.

- Inbound connectivity access to the Morpheus appliance from provisioned VMs and container hosts on port 443 (needed for Agent communication)
- Private (non-Morpheus provided) VM images and templates must have their credentials stored. These can be entered or edited in the Library > Virtual Images section by clicking the Actions dropdown on an image detail page and selecting Edit.

**Note:** Administrator user is required for Windows Agent install.

- The Instance does not have an IP address assigned. For scenarios without a DHCP server, static IP information must be entered by selecting the Network Type: Static in the Advanced Options section during provisioning. IP Pools can also be created in the Infrastructure > Networks > IP Pools section and added to Cloud network sections for IPAM
- DNS is not configured and the node cannot resolve the appliance. If DNS cannot be configured, the IP address of the Morpheus appliance can be used as the main or Cloud appliance

**SSH**

- Port 22 is open for Linux images, and SSH is enabled
- Credentials set on the image if using a custom or synced image. Credentials can be entered on images in the Library > Virtual Images section

**WinRM**

- Port 5985 must be open and WinRM enabled for Windows images
- Credentials have been entered on the image if using a custom or synced image. Credentials can be entered on images in the Library > Virtual Images section

**Note:** Administrator user is required for Windows Agent install.
VMware Tools (vmtools)

- VMware Tools is installed on the template(s)
- Credentials have been entered on the image if using custom or synced image. Credentials can be entered on images in the Library > Virtual Images section
- Sudo privileges required for Linux
- Administrator User required for Windows (SID 500)

Cloud-Init

- Cloud-Init settings configured in Administration > Settings > Provisioning section
- Cloud-Init installed on Virtual Image
- Cloud-Init enabled on Virtual Image config

Cloudbase-Init

- Windows Administrator Password defined in Administration > Settings > Provisioning section
- Cloudbase-Init installed on Virtual Image
- Cloudbase-Init enabled on Virtual Image config
- Cloudbase-Init is only required for OpenStack Cloud types

Note: Unattend Agent Installation and customizations are recommended over Cloudbase-Init

Windows Unattended

- Windows Administrator Password defined in Administration > Settings > Provisioning section
- VMware: Force Guest Customizations set to forced on Virtual Image config when using DHCP (Static Assignment will already force Guest Customizations)
- Nutanix & SCVMM: Virtual Image is sysprepped and shutdown, Sysprep Enabled flagged on Virtual Image config

Manual

Agent Install scripts can be downloaded from Morpheus by selecting Actions > Download Agent Script from an Instance detail page, then run manually on the target host when required for a given managed resource. Please note the script will be unique per managed resource and should not be saved to run as needed on any arbitrary resources in the future.

When installing on Windows, continue with the steps below to complete manual installation:

- Open powershell as an administrator
- Run the `unblock-file` cmdlet against the download agent installation script:
Unblock-File -Path C:\Users\User01\Documents\Downloads\agentInstall.ps1
Get-ExecutionPolicy
Set-ExecutionPolicy -ExecutionPolicy Unrestricted -ScopeCurrentUser

- After running the powershell script, ensure the script downloaded the msi and the Agent service started correctly:
  Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -ScopeCurrentUser

Following setup, verify that the Agent is reporting back to the Morpheus appliance.

**Restarting the Morpheus Agent**

In some situations, it may necessary to restart the Morpheus Agent on the host to re-sync communication from the Agent to the Morpheus appliance.

**Linux**

On the target host, run `sudo morpheus-node-ctl restart morphd` and the Morpheus agent will restart. `morpheus-node-ctl status` will also show the agent status.

**Windows**

The Morpheus Windows Agent service can be restarted in Administrative Tools > Services.

**Tip:** The Morpheus Remote Console is not dependent on Agent communication and can be used to install or restart the Morpheus agent on an Instance.

**Uninstall Morpheus Agent**

**Linux Agents**

You can use the following to uninstall the linux agent (contains commands for both rpm and deb agents)

```bash
sudo rm /etc/apt/sources.list.d/morpheus.list \\
sudo morpheus-node-ctl kill \\
sudo apt-get -y purge morpheus-node \\
sudo apt-get -y purge morpheus-vm-node \\
sudo yum -y remove morpheus-node \\
sudo yum -y remove morpheus-vm-node \\
sudo yum clean all \\
sudo systemctl stop morpheus-node-runsvdir \\
sudo rm -f /etc/systemd/system/morpheus-node-runsvdir.service \\
sudo systemctl daemon-reload \\
sudo rm -rf /var/run/morpheus-node \\
```
### Windows Agents

```bash
$app = Get-WmiObject -Class Win32_Product
$app.Uninstall()
```

### CentOS/RHEL 7 Images

For custom CentOS 7 images we highly recommend setting up Cloud-Init and fixing the network device names. More information for custom CentOS images can be found in the CentOS 7 image guide.

### 1.6.3 Communication Data

The following page contains communication information between the Morpheus appliance, integrated technologies, managed machines, and services.

#### Communication Frequency and Configurability

The following table contains communication information, including frequency and configurability between Morpheus and its supported technology integrations.

<table>
<thead>
<tr>
<th>Source</th>
<th>Push/Pull</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Foundry App Check</td>
<td>Server Pull</td>
<td>Cloud Foundry Applications that exist within Morpheus</td>
</tr>
<tr>
<td>Docker Container Check</td>
<td>Server Pull</td>
<td>Docker containers that exist within Morpheus</td>
</tr>
<tr>
<td>Elastic Search Check</td>
<td>Server Pull</td>
<td>Elastic Search application</td>
</tr>
<tr>
<td>Microsoft SQL Server Check</td>
<td>Server Pull</td>
<td>Microsoft SQL application</td>
</tr>
<tr>
<td>Mongo Check</td>
<td>Server Pull</td>
<td>Mongo DB application</td>
</tr>
<tr>
<td>MySQL Check</td>
<td>Server Pull</td>
<td>MySQL application</td>
</tr>
<tr>
<td>Postgres Check</td>
<td>Server Pull</td>
<td>Postgres application</td>
</tr>
<tr>
<td>Push API Check</td>
<td>Client Push</td>
<td>Morpheus API</td>
</tr>
<tr>
<td>Rabbit MQ Check</td>
<td>Server Pull</td>
<td>Rabbit MQ application</td>
</tr>
<tr>
<td>Redis Check</td>
<td>Server Pull</td>
<td>Redis application</td>
</tr>
<tr>
<td>Risk Check</td>
<td>Server Pull</td>
<td>Risk application</td>
</tr>
<tr>
<td>SNMP Check</td>
<td>Server Pull</td>
<td>SNMP</td>
</tr>
<tr>
<td>Socket Check</td>
<td>Server Pull</td>
<td>Web Socket</td>
</tr>
<tr>
<td>Virtual Machine Check</td>
<td>Server Pull</td>
<td>Virtual Machine that exists within Morpheus</td>
</tr>
<tr>
<td>Web Check</td>
<td>Server Pull (GET) or Server Push (POST)</td>
<td>Web application</td>
</tr>
<tr>
<td>Public Cloud Integration</td>
<td>Server Pull</td>
<td>Alibaba Cloud</td>
</tr>
<tr>
<td>Public Cloud Integration</td>
<td>Server Pull</td>
<td>Amazon AWS</td>
</tr>
<tr>
<td>Public Cloud Integration</td>
<td>Server Pullconstent荪</td>
<td>Amazon AWS GovCloud</td>
</tr>
<tr>
<td>Public Cloud Integration</td>
<td>Server Pull</td>
<td>DigitalOcean</td>
</tr>
</tbody>
</table>

| (continued from previous page)          |                                  |                                                                              |

### Morpheus Documentation

```bash
sudo pkill runsv \
sudo pkill runsvdir \
sudo pkill morphd \
sudo usermod -l morpheus-old morpheus-node \
```
### 1.6. Core Functionality

<table>
<thead>
<tr>
<th>Source</th>
<th>Push/Pull</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Cloud Integration</td>
<td>Server Pull</td>
<td>Google Cloud Platform</td>
</tr>
<tr>
<td>Public Cloud Integration</td>
<td>Server Pull</td>
<td>Huawei Cloud</td>
</tr>
<tr>
<td>Public Cloud Integration</td>
<td>Server Pull</td>
<td>IBM Cloud</td>
</tr>
<tr>
<td>Public Cloud Integration</td>
<td>Server Pull</td>
<td>Microsoft Azure</td>
</tr>
<tr>
<td>Public Cloud Integration</td>
<td>Server Pull</td>
<td>Open Telekom Cloud</td>
</tr>
<tr>
<td>Public Cloud Integration</td>
<td>Server Pull</td>
<td>Oracle Public Cloud</td>
</tr>
<tr>
<td>Public Cloud Integration</td>
<td>Server Pull</td>
<td>UpCloud</td>
</tr>
<tr>
<td>Public Cloud Integration</td>
<td>Server Pull</td>
<td>VMware on AWS</td>
</tr>
<tr>
<td>Private Cloud Integration</td>
<td>Server Pull</td>
<td>Cisco UCS Manager</td>
</tr>
<tr>
<td>Private Cloud Integration</td>
<td>Server Pull</td>
<td>Dell EMC</td>
</tr>
<tr>
<td>Private Cloud Integration</td>
<td>Server Pull</td>
<td>HPE</td>
</tr>
<tr>
<td>Private Cloud Integration</td>
<td>Server Pull</td>
<td>HPE OneView</td>
</tr>
<tr>
<td>Private Cloud Integration</td>
<td>Server Pull</td>
<td>KVM</td>
</tr>
<tr>
<td>Private Cloud Integration</td>
<td>Server Pull</td>
<td>MacStadium</td>
</tr>
<tr>
<td>Private Cloud Integration</td>
<td>Server Pull</td>
<td>Microsoft Azure Stack</td>
</tr>
<tr>
<td>Private Cloud Integration</td>
<td>Server Pull</td>
<td>Microsoft Hyper-V</td>
</tr>
<tr>
<td>Private Cloud Integration</td>
<td>Server Pull</td>
<td>Nutanix SCVMM</td>
</tr>
<tr>
<td>Private Cloud Integration</td>
<td>Server Pull</td>
<td>Openstack</td>
</tr>
<tr>
<td>Private Cloud Integration</td>
<td>Server Pull</td>
<td>Oracle VM</td>
</tr>
<tr>
<td>Private Cloud Integration</td>
<td>Server Pull</td>
<td>Pivotal Cloud Foundry</td>
</tr>
<tr>
<td>Private Cloud Integration</td>
<td>Server Pull</td>
<td>Supermicro</td>
</tr>
<tr>
<td>Private Cloud Integration</td>
<td>Server Pull</td>
<td>Vmware vCloud Director</td>
</tr>
<tr>
<td>Private Cloud Integration</td>
<td>Server Pull</td>
<td>Vmware ESXi</td>
</tr>
<tr>
<td>Private Cloud Integration</td>
<td>Server Pull</td>
<td>VMware Fusion</td>
</tr>
<tr>
<td>Private Cloud Integration</td>
<td>Server Pull</td>
<td>VMware vCenter</td>
</tr>
<tr>
<td>Private Cloud Integration</td>
<td>Server Pull</td>
<td>Xen Server</td>
</tr>
<tr>
<td>Automation Integration</td>
<td></td>
<td>Ansible</td>
</tr>
<tr>
<td>Automation Integration</td>
<td></td>
<td>Ansible Tower</td>
</tr>
<tr>
<td>Automation Integration</td>
<td></td>
<td>Chef</td>
</tr>
<tr>
<td>Automation Integration</td>
<td></td>
<td>Puppet</td>
</tr>
<tr>
<td>Automation Integration</td>
<td></td>
<td>Salt</td>
</tr>
<tr>
<td>Automation Integration</td>
<td></td>
<td>Terraform</td>
</tr>
<tr>
<td>Automation Integration</td>
<td></td>
<td>vRealize Orchestrator</td>
</tr>
<tr>
<td>Backup Integration</td>
<td></td>
<td>Commvault</td>
</tr>
<tr>
<td>Backup Integration</td>
<td></td>
<td>Veeam</td>
</tr>
<tr>
<td>Backup Integration</td>
<td></td>
<td>Rubrik</td>
</tr>
<tr>
<td>Backup Integration</td>
<td></td>
<td>Zerto</td>
</tr>
<tr>
<td>Backup Integration</td>
<td></td>
<td>Avamar</td>
</tr>
<tr>
<td>Build Integration</td>
<td></td>
<td>Jenkins</td>
</tr>
<tr>
<td>Container Integration</td>
<td></td>
<td>Docker</td>
</tr>
<tr>
<td>Container Integration</td>
<td></td>
<td>Docker Registry</td>
</tr>
<tr>
<td>Container Integration</td>
<td></td>
<td>Kubernetes</td>
</tr>
<tr>
<td>Deployment Integration</td>
<td></td>
<td>Git/Github</td>
</tr>
<tr>
<td>DNS Integration</td>
<td></td>
<td>AWS Route53</td>
</tr>
<tr>
<td>DNS Integration</td>
<td></td>
<td>Microsoft DNS</td>
</tr>
<tr>
<td>DNS Integration</td>
<td></td>
<td>PowerDNS</td>
</tr>
<tr>
<td>Identity Management Integration</td>
<td>Server Pull</td>
<td>Microsoft AD</td>
</tr>
<tr>
<td>Identity Management Integration</td>
<td>Server Pull</td>
<td>OneLogin</td>
</tr>
<tr>
<td>Source</td>
<td>Push/Pull</td>
<td>Destination</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Identity Management Integration</td>
<td>Server Pull</td>
<td>Okta</td>
</tr>
<tr>
<td>Identity Management Integration</td>
<td>Server Pull</td>
<td>Jump Cloud</td>
</tr>
<tr>
<td>Identity Management Integration</td>
<td>Server Pull</td>
<td>LDAP</td>
</tr>
<tr>
<td>Identity Management Integration</td>
<td>Server Pull</td>
<td>SAML</td>
</tr>
<tr>
<td>IPAM Integration</td>
<td>Server Pull</td>
<td>Infoblox</td>
</tr>
<tr>
<td>IPAM Integration</td>
<td>Server Pull</td>
<td>phpIPAM</td>
</tr>
<tr>
<td>IPAM Integration</td>
<td>Server Pull</td>
<td>Bluecat</td>
</tr>
<tr>
<td>IPAM Integration</td>
<td>Server Pull</td>
<td>SolarWinds</td>
</tr>
<tr>
<td>ITSM Integration</td>
<td>Server Pull</td>
<td>ServiceNow</td>
</tr>
<tr>
<td>ITSM Integration</td>
<td>Server Push</td>
<td>ServiceNow</td>
</tr>
<tr>
<td>ITSM Integration</td>
<td>Server Pull</td>
<td>Cherwell</td>
</tr>
<tr>
<td>ITSM Integration</td>
<td>Server Pull</td>
<td>Remedy</td>
</tr>
<tr>
<td>Key &amp; Certificate Integration</td>
<td>Server Pull</td>
<td>Venafi</td>
</tr>
<tr>
<td>Load Balancer Integration</td>
<td>Server Pull</td>
<td>AzureLB</td>
</tr>
<tr>
<td>Load Balancer Integration</td>
<td>Server Pull</td>
<td>F5 BigIP</td>
</tr>
<tr>
<td>Load Balancer Integration</td>
<td>Server Pull</td>
<td>Citrix NetScaler</td>
</tr>
<tr>
<td>Logging Integration</td>
<td></td>
<td>Syslog</td>
</tr>
<tr>
<td>Monitoring Integration</td>
<td>Server Pull</td>
<td>ServiceNow</td>
</tr>
<tr>
<td>Monitoring Integration</td>
<td></td>
<td>AppDynamics</td>
</tr>
<tr>
<td>Monitoring Integration</td>
<td></td>
<td>NewRelic</td>
</tr>
<tr>
<td>Network Integration</td>
<td>Server Pull</td>
<td>NSX-T</td>
</tr>
<tr>
<td>Network Integration</td>
<td>Server Pull</td>
<td>NSX-V</td>
</tr>
<tr>
<td>Network Integration</td>
<td>Server Pull</td>
<td>Cisco ACI</td>
</tr>
<tr>
<td>Network Integration</td>
<td>Server Pull</td>
<td>Unisys Stealth</td>
</tr>
<tr>
<td>Storage Integration</td>
<td>Server Pull</td>
<td>3Par</td>
</tr>
<tr>
<td>Storage Integration</td>
<td>Server Pull</td>
<td>Azure Storage</td>
</tr>
<tr>
<td>Storage Integration</td>
<td>Server Pull</td>
<td>Dell ECS</td>
</tr>
<tr>
<td>Storage Integration</td>
<td>Server Pull</td>
<td>Isilon</td>
</tr>
<tr>
<td>Morpheus Agent</td>
<td>Agent Pull</td>
<td>Application Tier</td>
</tr>
</tbody>
</table>

## Ports and Protocols

The following table contains communication port and protocol data between Morpheus appliance tiers, managed machines, and services. All communication to and from Morpheus goes thru the application tier with exception of inter-cluster communications for each of the Morpheus tiers when using a distributed architecture.

Ports used to communicate with integrated technologies are those defined for the integration’s API. They are not represented in this table as many of these are configurable and may be different in each customer environment. Additionally, ports used to complete Morpheus checks are customizable and may vary for each check configured. They are also not represented in this table.

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Port</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Application Tier</td>
<td>443</td>
<td>TCP</td>
<td>User Access</td>
</tr>
<tr>
<td>Morpheus Servers</td>
<td>DNS Servers</td>
<td>53</td>
<td>TCP</td>
<td>Domain Name Resolution</td>
</tr>
<tr>
<td>Morpheus Servers</td>
<td>Time Source</td>
<td>123</td>
<td>TCP</td>
<td>Time Resolution</td>
</tr>
<tr>
<td>Morpheus Servers</td>
<td>Web or Offline Installer</td>
<td>80, 443</td>
<td>TCP</td>
<td>Download repos and Morpheus updates</td>
</tr>
<tr>
<td>Managed Machine</td>
<td>Application Tier</td>
<td>443</td>
<td>TCP</td>
<td>Morpheus Agent Communication</td>
</tr>
<tr>
<td>Managed Machine</td>
<td>Application Tier</td>
<td>80, 443</td>
<td>TCP</td>
<td>Agent Installation. (Requires persistent...)</td>
</tr>
<tr>
<td>Source</td>
<td>Destination</td>
<td>Port</td>
<td>Protocol</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------------------------</td>
<td>---------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Managed Machine</td>
<td>Application Tier</td>
<td>N/A</td>
<td>N/A</td>
<td>Agent Installation Cloud-init (Linux)</td>
</tr>
<tr>
<td>Managed Machine</td>
<td>Application Tier</td>
<td>N/A</td>
<td>N/A</td>
<td>Agent Installation Cloudbase-init (Windows)</td>
</tr>
<tr>
<td>Managed Machine</td>
<td>Application Tier</td>
<td>N/A</td>
<td>N/A</td>
<td>Agent Installation VMtools</td>
</tr>
<tr>
<td>Managed Machine</td>
<td>Docker Image Repo</td>
<td>443</td>
<td>TCP</td>
<td>Static IP Assignment &amp; IP Pools</td>
</tr>
<tr>
<td>Managed Machine</td>
<td>Application Tier</td>
<td>69</td>
<td>TCP/UDP</td>
<td>PXE Boot (Forwarded to internal PXE port 6969)</td>
</tr>
<tr>
<td>Application Tier</td>
<td>Managed Machine</td>
<td>5985</td>
<td>TCP</td>
<td>Agent Installation WinRM (Windows)</td>
</tr>
<tr>
<td>Application Tier</td>
<td>Managed Machine</td>
<td>22</td>
<td>TCP</td>
<td>Agent Installation SS (Linux)</td>
</tr>
<tr>
<td>Application Tier</td>
<td>Managed Machine</td>
<td>22, 3389, 443</td>
<td>TCP</td>
<td>Remote Console (SSH, RDP, HTML)</td>
</tr>
<tr>
<td>Application Tier</td>
<td>AWS S3</td>
<td>443</td>
<td>TCP</td>
<td>Morpheus Catalog Image Download</td>
</tr>
<tr>
<td>Application Tier</td>
<td>Hypervisor</td>
<td>443</td>
<td>TCP</td>
<td>Hypervisor hostname resolvable</td>
</tr>
<tr>
<td>Application Tier</td>
<td>Non- Transactional Database Tier</td>
<td>443</td>
<td>TCP</td>
<td>Applicable if using Amazon ES</td>
</tr>
<tr>
<td>Application Tier</td>
<td>Docker CE Repo</td>
<td>443</td>
<td>TCP</td>
<td>Applicable only when integrated</td>
</tr>
<tr>
<td>Application Tier</td>
<td>Rubygems</td>
<td>443</td>
<td>TCP</td>
<td></td>
</tr>
<tr>
<td>Application Tier</td>
<td>Morpheus Hub</td>
<td>443</td>
<td>TCP</td>
<td>(Optional) Telemetry data (Disabled only via license feature)</td>
</tr>
<tr>
<td>Application Tier</td>
<td>Mail Server</td>
<td>25 or 465</td>
<td>SMTP</td>
<td>Send email from Morpheus</td>
</tr>
<tr>
<td>Application Tier</td>
<td>postmarkapp</td>
<td>2525</td>
<td>TCP</td>
<td>Send email from Morpheus (standard SMTP)</td>
</tr>
<tr>
<td>Application Tier</td>
<td>Messaging Tier</td>
<td>5672</td>
<td>TCP</td>
<td>AMQP non-TLS connections</td>
</tr>
<tr>
<td>Application Tier</td>
<td>Messaging Tier</td>
<td>5671</td>
<td>TCP</td>
<td>AMQP TLS enabled connections</td>
</tr>
<tr>
<td>Application Tier</td>
<td>Messaging Tier</td>
<td>61613</td>
<td>TCP</td>
<td>STOMP Plugin connections (R)</td>
</tr>
<tr>
<td>Application Tier</td>
<td>Messaging Tier</td>
<td>61614</td>
<td>TCP</td>
<td>STOMP Plugin TLS enabled connections</td>
</tr>
<tr>
<td>Messaging Tier</td>
<td>Messaging Tier</td>
<td>25672</td>
<td>TCP</td>
<td>Inter-node and CLI tool communication</td>
</tr>
<tr>
<td>Administrator Web Browser</td>
<td>RabbitMQ Server Management</td>
<td>15672</td>
<td>TCP</td>
<td>Management plugin</td>
</tr>
<tr>
<td>Administrator Web Browser</td>
<td>RabbitMQ Server Management</td>
<td>15671</td>
<td>TCP</td>
<td>Management plugin SSL</td>
</tr>
<tr>
<td>Messaging Tier Cluster Node</td>
<td>Messaging Tier Cluster Node</td>
<td>4369</td>
<td>TCP</td>
<td>erlang (epmd) peer discovery server</td>
</tr>
<tr>
<td>Application Tier</td>
<td>Non-Transactional Database Tier</td>
<td>9200</td>
<td>TCP</td>
<td>Elasticsearch requests (Used in all cases except when utilizing AWS ES)</td>
</tr>
<tr>
<td>Non-Transactional Database Tier</td>
<td>Non-Transactional Database Tier</td>
<td>9300</td>
<td>TCP</td>
<td>Elasticsearch Cluster</td>
</tr>
<tr>
<td>Transactional Database Tier</td>
<td>Transactional Database Tier</td>
<td>4567</td>
<td>TCP/UDP</td>
<td>Write-set replication traffic (own)</td>
</tr>
<tr>
<td>Transactional Database Tier</td>
<td>Transactional Database Tier</td>
<td>4568</td>
<td>TCP</td>
<td>Incremental State Transfer (IST)</td>
</tr>
<tr>
<td>Application Tier</td>
<td>Transactional Database Tier</td>
<td>3306</td>
<td>TCP</td>
<td>MySQL client connections</td>
</tr>
<tr>
<td>Backup Solution</td>
<td>Transactional Database Tier</td>
<td>4444</td>
<td>TCP</td>
<td>State Snapshot Transfer (SST)</td>
</tr>
<tr>
<td>Application Tier</td>
<td>Integrated Technology</td>
<td>Varies</td>
<td>TCP</td>
<td>Integrations (Uses the port of the protocol)</td>
</tr>
</tbody>
</table>

### 1.6.4 VMware Support Statement

The **morphdatI** will support customers who run Morpheus products on supported operating systems, irrespective of whether they are running in VMware environments or not. **morphdatI** supports operating systems, not specific hardware configurations. Accordingly, VMware operates as a hardware abstraction layer.

VMware supports a set of certified operating systems and hardware. The customer and VMware will be responsible for any interactions or issues that arise at the hardware or operating system layer as a result of their use of VMware.

**morphdatI** will not require clients to recreate and troubleshoot every issue in a non-VMware environment; however, **morphdatI** does reserve the right to request our customers to diagnose certain issues in a native certified operating system environment, operating without the virtual environment. **morphdatI** will only make this request when there is reason to believe that the virtual environment is a contributing factor to the issue.

Any time spent on investigation of problems that may, in the sole opinion of **morphdatI** be related to VMware, will be handled in the following fashion:

1. **morphdatI** will provide standard support to all Morpheus products.
2. If a problem is encountered while Morpheus is/are running in a VMware environment, the client may be required to recreate the problem on a non-VMware server unit, at which time |morphdat| will provide regular support.

3. The client can authorize |morphdat| to investigate the VMware-related items at normal time and materials rates. If such investigation shows that the problem is VMware related, the client may contract |morphdat| to provide a software change to resolve the issue if such a resolution is possible.

4. Regardless of the problem type or source, if the problem is determined to be a non VMware-related issue, time spent on investigation and resolution will be covered as part of regular maintenance and support will be provided as usual.
2.1 Dashboard

The Dashboard is a single pane of glass showing quick, easy to read performance and configuration information about the Morpheus Environment.

**Status** There are four gauges across the top of the dashboard page showing quick system stats for Instances, Monitoring Status, Log Errors, and Backups. Each gauge also serves as a quick link for each section.

**My Instances** The My Instances section shows quick information about 5 favorite instances like Type, IP and Port. Click View All to be taken directly to the instances page.

**Monitoring** The Monitoring section displays an overall health, availability statistics, as well as response time and any open incidents requiring action.

**Recent Activity** Recent Activity is displayed on the right side of the dashboard page. Items like instance provisioning and deletion, backups, and alerts are displayed here.

**Logs** All Morpheus logs are application aware. Log information from hypervisors, servers, and applications are pushed up into the Morpheus controller node and made searchable and actionable. Choose a timeframe from the Logs pane to view statistics or click List to view all log information.

**Backups** The backup pane at the bottom of the page shows statistics about Morpheus backups. Information about success and failure rates and the number of backups run versus scheduled is available here. Click on the List button to be taken directly to the backups page where you can view and configure backups.

2.2 Reports

2.2.1 Overview

Morpheus offers 28 different report types which are designed to slice up costing and usage across Clouds, Tenants, and more. Reports can be run on-demand as needed or can be scheduled to run on certain intervals to be viewed at a later time. The list of available report types can be viewed at Operations > Reports.
2.2.2 Report Types

ACCOUNT INVENTORY

- Tenant Inventory Summary

CLOUD USAGE

- Cloud Usage
- Cloud Usage App Summary
- Cloud Usage Instance Type Summary
- Tenant Usage

CLOUD COST

- Amazon Reservation Coverage
- Amazon Reservation Utilization
- Amazon Savings Inventory Summary
• Amazon Savings Plan Coverage
• Amazon Savings Plan Utilization
• Application Cost
• Cloud Cost
• Group Cost
• Instance Cost
• Invoice Details
• Tenant Cost
• Time Series Cost

INFRASECURE INVENTORY
• Cloud Inventory Summary
• Container Host Inventory Summary
• Group Inventory Summary
• Guidance
• Hypervisor Inventory Summary
• Migration Planning
• Tenant Resource Allocation

PROVISIONING INVENTORY
• Instance Inventory Summary
• Software Inventory
• Software Inventory By Server
• Tag Compliance
• Virtual Machine Inventory Summary
• Workload Summary

By clicking into a report type, users can see any previous runs and active report schedules. New on-demand runs and new schedules of the selected report type can be created, edited, or deleted from here. The next few sections go into creating, editing, scheduling, viewing, and deleting reports in greater detail.

2.2.3 Create Reports

To create a new report, navigate to the report type list page (Operations > Reports). Click RUN NOW to the right of the specific report type to bring up the wizard to run that particular report. The required and optional fields to run the selected report type will appear, for example, the configuration panel for the Instance Cost report is shown below:
In this case, we can choose to scope the report by start and end dates, Groups, Clouds, Tenants, and can specific include or omit Instances based on tags. Once the report is run, it will be visible in the list of Instance Cost reports and all reports until deleted.

### 2.2.4 Schedule Reports

In addition to running on-demand reports, Morpheus also allows reports to be scheduled. This allows you to save report configuration and have access to refreshed information on the schedule you need.

The process of scheduling a report is nearly identical to running on on-demand. From the report type list page (Operations > Reports) click **SCHEDULE** to the right of the report type you wish to schedule. The required and optional fields to schedule the selected report type will appear, for example, the configuration panel for the Instance Cost report is shown below:
In this case, we can choose to scope the report by start and end dates, Groups, Clouds, Tenants, and can specific include or omit Instances based on tags. Additionally, we select the time schedule on which this report should automatically run.

**Note:** Morpheus includes three schedules by default: Date and Time (run once at the specified time), Daily at Midnight, and Weekly on Sunday at Midnight. Any other listed scheduling periods are user-configured execution schedules (Library > Automation > Execute Scheduling). Create a new execution schedule if none of the existing schedules work for your reporting needs.

### 2.2.5 Viewing Results

A list of all report runs is viewable on the Results tab of the report types list page (Operations > Reports). To view the report itself, click on the hyperlinked report filters. Only reports that are ready for viewing will have an active hyperlink on their filters. In addition to report filters, the run date, report type, creating user, and run status are shown. Click on any of these headers to filter the report list by that column in either ascending or descending order. Any report can be deleted by clicking on the trash can icon at the end of its row.
2.2.6 Viewing Schedules

A list of all scheduled report runs can be viewed in the Scheduled tab of the report types list page (Operations > Reports). The friendly name of the report schedule is displayed along with the report type, last run time, next run time, and success status of the previous run. Schedules can be edited or deleted by clicking on the pencil or trash can icon, respectively. We can also view the most recent run of a given schedule (if it was successful) by clicking on the hyperlinked “last run” value.

2.3 Analytics

2.3.1 Overview

The Morpheus Analytics engine gives administrators the tools to break down costs and usage, then filter the results by relevant delineations including Groups, Clouds, Tenants or even tag values. Analytics dashboards can be organized into three primary categories based on their measurement intentions: costing, utilization, and workloads. Each dashboard type is discussed in further detail below.
2.3.2 Costing: Cloud Costing

The Cloud Costing dashboard breaks down total costs by cloud type, cloud region, and individual cloud. This includes reporting the total number of clouds that meet your filters, the month-to-date running total, the projected monthly spend, among other useful metrics.

**Filters**

Filter the Clouds pulled into the dashboard by one or more of the following fields:

- Cloud (all matched by search)
- Group
• Cloud (selected from dropdown)
• Tenant
• Tag (Key)
• Value (tag value)

Data Displayed
The following aggregate totals are compiled for all Clouds that meet set filters:

• CLOUDS: The total number of Clouds that meet set filters
• MONTH TO DATE: The total spend in the current month for all Clouds meeting dashboard filters
• PROJECTED: The projected total spend for the current month for all Clouds meeting dashboard filters
• CLOUD TYPES: The number of distinct cloud types that meet the dashboard filters, such as Amazon AWS, Microsoft Azure, VMware, or any other Morpheus-supported Cloud types
• REGIONS: The total number of regions represented by Clouds meeting the dashboard filters

In addition to the totals described above, graphs visualize the percentage of these totals accounted for by specific Clouds, Cloud types, and Cloud regions.

Cloud List
Each Cloud that meets set filters is listed at the bottom of the dashboard, the following data points are revealed for each individual Cloud:

• TYPE: The Cloud type, such as Amazon AWS, Microsoft Azure, VMware, or any other Morpheus-supported Cloud type
• NAME: The name given to the Cloud in Morpheus at the time of integration
• LOCATION: The Cloud location (if available)
• REGION: The Cloud region (if available)
• MONTH TO DATE: The current month-to-date spend for the individual Cloud listed
• PROJECTED TOTAL: The projected total spend for the current month for the individual Cloud listed
2.3.3 Costing: Group Costing

The Group Costing dashboard aggregates cost totals for all Groups that meet filters set on the dashboard. This allows administrators to sort Groups by their total costs and anticipate monthly total costs by Group.

**Filters**

Filter the Groups pulled into the dashboard by one or more of the following fields:

- Group (all matched by search)
- Group (selected from dropdown)
- Cloud
- Tenant
Data Displayed

The following aggregate totals are compiled for all Groups that meet set filters:

- **GROUPS**: The total number of Groups that meet set filters
- **MONTH TO DATE**: The total spend in the current month for all Groups meeting dashboard filters
- **PROJECTED**: The projected total spend for the current month for all Groups meeting dashboard filters

Group List

Each Group that meets set filters is listed at the bottom of the dashboard, the following data points are revealed for each individual Group:

- **NAME**: The name given to the Group in Morpheus at the time of creation
- **LOCATION**: The Group location (if available)
- **DATA CENTER**: The Group datacenter (if available)
- **MONTH TO DATE**: The current month-to-date spend for the individual Group listed
- **PROJECTED TOTAL**: The projected total spend for the current month for the individual Group listed
2.3.4 Costing: Tenant Costing

The Tenant Costing dashboard aggregates costing totals across all Tenants that meet the filters set on the dashboard. This information helps administrators track the current spend of each Tenant for the current monthly period. It also helps identify the costliest Tenants and to anticipate month-end costs for each individual Tenant.

Filters

Filter the Tenants pulled into the dashboard by one or more of the following fields:

- Tenant (all matched by search)
• Cloud
• Tenant (selected from dropdown)

Data Displayed

The following aggregate totals are compiled for all Tenants that meet set filters:

• TENANTS: The total number of Tenants that meet set filters
• MONTH TO DATE: The total spend in the current month for all Tenants meeting dashboard filters
• PROJECTED: The projected total spend for the current month for all Tenants meeting dashboard filters
• LAST MONTH: The total spend in the prior month for all Tenants meeting dashboard filters

Tenant List

Each Tenant that meets set filters is listed at the bottom of the dashboard, the following data points are revealed for each individual Tenant:

• NAME: The name given to the Tenant in Morpheus at the time of creation
• DESCRIPTION: The Tenant description (if available)
• MONTH TO DATE: The current month-to-date spend for the individual Tenant listed
• PROJECTED TOTAL: The projected total spend for the current month for the individual Tenant listed
2.3.5 Costing: User Costing

The User Costing dashboard allows administrators to analyze costs for a group of Users that meet specific filters. Once the group is selected, total costs by User for the current month and projected totals are displayed. Administrators can identify their costliest Users and anticipate the total cost by User for budgeting purposes.

**Filters**

Filter the Groups pulled into the dashboard by one or more of the following fields:
• User (all matched by search)
• Group
• Cloud
• Period (Current month, last three months, last six months, or last 12 months)
• Tenant

Data Displayed

The following aggregate totals are compiled for all Users that meet set filters:

• **USERS**: The total number of Users that meet set filters
• **MONTH TO DATE**: The total spend in the current month for all Users meeting dashboard filters
• **PROJECTED**: The projected total spend for the current month for all Users meeting dashboard filters

User List

Each User that meets set filters is listed at the bottom of the dashboard, the following data points are revealed for each individual User:

• **USERNAME**: The username given to the User in Morpheus at the time of creation
• **MONTH TO DATE**: The current month-to-date spend for the individual User listed
• **PROJECTED TOTAL**: The projected total spend for the current month for the individual User listed
2.3.6 Costing: Workload Costing

The Workload Costing dashboard allows administrators to look at all or a subset of Morpheus-managed workloads to analyze their cost impact. Filters can be set to isolate a specific group of workloads and cost breakdowns are shown. Graphs are generated to reveal cost breakdowns of individual workloads or certain groups of workloads.

Filters

Filter the workloads pulled into the dashboard by one or more of the following fields:

- Workload name (all matched by search)
- Group
- Cloud
- Tenant
• Tag (Key). This is a required field and the top key in the list will be pre-selected by default
• Value (tag value)

**Data Displayed**

The following aggregate totals are compiled for all workloads that meet set filters:

- **WORKLOADS**: The total number of workloads that meet set filters
- **MONTH TO DATE**: The total spend in the current month for all workloads meeting dashboard filters
- **PROJECTED**: The projected total spend for the current month for all workloads meeting dashboard filters
- **TYPES**: The total number of workload types represented among workloads meeting set filters
- **SIZES**: The total number of unique workload sizes represented among workloads meeting set filters

### 2.3.7 Costing: Budget Analysis

**BUDGET COST ANALYSIS**

![Budget Analysis Dashboard](image)

- **1 BUDGETS**
- **$14 MONTH TO DATE**
- **$0 BUDGETS TO DATE**
- **$273 COST TO DATE**
- **$273 TO BUDGET**

![Budget vs Actual Chart](image)

<table>
<thead>
<tr>
<th></th>
<th>JANUARY</th>
<th>FEBRUARY</th>
<th>MARCH</th>
<th>APRIL</th>
<th>MAY</th>
<th>JUNE</th>
<th>JULY</th>
<th>AUGUST</th>
<th>SEPTEMBER</th>
<th>OCTOBER</th>
<th>NOVEMBER</th>
<th>DECEMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Budget</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
</tr>
<tr>
<td>Actual</td>
<td>$45</td>
<td>$42</td>
<td>$42</td>
<td>$45</td>
<td>$45</td>
<td>$53</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Tenant, Cloud, Group, or User) and budgets of the same scope are viewed together in this dashboard. A scope filter must be set in order for data to be populated into the dashboard. Once a scope is selected, the search bar can be utilized to return only budgets within the selected scope whose “Name” meets the search terms.

Filters

Filter the budgets pulled into the dashboard by one or more of the following fields:

- Budget name (all matched by search)
- Scope (This is a required field, data is not populated into the dashboard until a scope is specified)

Data Displayed

The following aggregate totals are compiled for all budgets that meet set filters:

- **BUDGETS**: The total number of budgets that meet set filters
- **MONTH TO DATE**: The total spend in the current month against the selected budgets
- **BUDGETS TO DATE**: The total amount budgeted to date among budgets selected by the dashboard filters (from the start of the year to the end of the current interval)
- **TO BUDGET**: The difference between the COST TO DATE and BUDGETS TO DATE value, should be close to $0 if the costs are appropriately tracking against the budgeted amounts

Budget List

Each budget with its own graph and breakdown is displayed going down the page. The format of the information presented depends on the interval that the specific budget is configured for.
2.3.8 Costing: Tag Costing

The Tag Analysis dashboard creates groups of workloads based on the presence of specific tags and meeting other filters. This workload group can be analyzed for total cost and projected costs.

Filters

Filter the workloads pulled into the dashboard by one or more of the following fields:

- Tag key (all matched by search)
- Metric (apply to see the top tag values by workload count, price, memory, storage, or CPU cores)
• Group
• Cloud
• Tenant
• Tag (Key)

Data Displayed
The following aggregate totals (by tag) are compiled for workloads that meet set filters:

• **TAGS**: The total number of unique tag keys for workloads meeting dashboard filters
• **MONTH TO DATE**: The total spend in the current month for selected workloads
• **PROJECTED**: The total projected current-month spend for selected workloads

**Tags List**
A list of each tag (key) represented on selected workloads is displayed in a list below the dashboard graphs. We also see the total number of workloads associated with the tag, the total memory, total storage, total CPU cores, and total price. If we click the “MORE” link at the end of each row, we can see a list of all tag values associated with the key.
The Utilization vs Cost dashboard is designed to reveal workloads which are underutilized (expensive and seldom-used) and which are very cost-efficient (inexpensive and frequently-used). Administrators can filter the workloads considered by the dashboard through the use of filters and potentially identify areas of cost savings by decommissioning seldom-used machines.

**Filters**

Filter the workloads pulled into the dashboard by one or more of the following fields:
• Workload name (all matching search terms)
• Time period (Current, one-day average, one-week average, one-month average, three-month average, six-month average, or one-year average)
• Type (virtual machines, hosts, or bare metal)
• Tenant
• Tag (Key)
• Value (Tag value)

Data Displayed

The following aggregate totals are compiled for workloads that meet set filters:

• COUNT: The total number of workloads that meet dashboard filters
• CLOUD COUNT: The total number of Clouds represented by the selected workloads
• MONTH TO DATE: The total spend in the current month for selected workloads
• PROJECTED: The total projected current-month spend for selected workloads
• AVERAGE UTILIZATION: The computed average utilization figure for all workloads selected by dashboard filters

Utilization List

In addition to the totals and graph displayed, two workload lists are given showing the least utilized workloads by cost (lowest utilization per cost dollar) and the least utilized workloads overall (lowest utilization overall). These workloads are listed with links to the Instance or server detail pages, along with other details related to price and resource utilization.
2.3.10 Workloads: Instance Type Usage

The Instance Type Usage dashboard organizes workloads meeting dashboard filters by their Instance type. In addition to counts, administrators can view resource consumption and cost figures by Instance type groupings as well.

Filters

Filter the workloads pulled into the dashboard by one or more of the following fields:

- Instance type name (all matching search terms, Morpheus-default Instance types are not included when using the search filter)
- Metric (apply to see the top Instance types by workload count, price, memory, storage, or CPU cores)
- Group
• Cloud
• Tenant
• Tag (Key)
• Value (Tag value)

Data Displayed

The following aggregate totals are compiled for workloads that meet set filters:

• **TYPES:** The total number of Instance types represented among workloads meeting the dashboard filters
• **INSTANCES:** The total number of Instances represented in the data
• **MONTH TO DATE:** The total spend in the current month for selected workloads
• **PROJECTED:** The total projected current-month spend for selected workloads
• **MEMORY:** The total memory allotted to selected workloads
• **STORAGE:** The total storage allotted to selected workloads

Instance Type Usage List

Each Instance type represented in the dashboard is listed below the graph. For each Instance type shown, we see the number of Groups the Instance type is represented in, the number of Clouds the Instance type has been provisioned into, and the total amount of memory allotted to workloads of each Instance type.
2.3.11 Workloads: Instance Usage

The Instance Usage dashboard shows Instance counts, resource utilization, and cost breakdowns by Cloud. Administrators can set filters to limit the workloads that are considered for dashboard analysis and then see the results given by Cloud groupings.

Filters

Filter the workloads pulled into the dashboard by one or more of the following fields:

- Instance name (all matching search terms)
- Metric (apply to see the top Clouds by workload count, price, memory, storage, or CPU cores)
- Group
• Cloud
• Tenant
• Tag (Key)
• Value (Tag value)

Data Displayed

The following aggregate totals are compiled for workloads that meet set filters:

• CLOUDS: The total number of Clouds represented among workloads meeting the dashboard filters
• INSTANCES: The total number of Instances represented in the data
• MONTH TO DATE: The total spend in the current month for selected workloads
• PROJECTED: The total projected current-month spend for selected workloads
• MEMORY: The total memory allotted to selected workloads
• STORAGE: The total storage allotted to selected workloads

Instance Usage List

All Clouds represented in the dashboard are listed here. For each Cloud, we see the total Instance count, total memory allotted, total storage allotted, total CPU cores, and the total price.
2.3.12 Workloads: Blueprint Usage

The Blueprint Usage dashboard lists all provisioned Apps that meet filters set on the dashboard. Once the desired group of Apps is filtered into the dashboard, administrators will see the total provisioned from each Blueprint, total number of Instances created from the Apps, and costing details.

Filters

Filter the Apps pulled into the dashboard by one or more of the following fields:

- App name (all matching search terms)
- Metric (apply to see the top Clouds by workload count, price, memory, storage, or CPU cores)
- Group
- Cloud
- Tenant
- Tag (Key)
- Value (Tag value)
Data Displayed

The following aggregate totals are compiled for Apps that meet set filters:

- **TYPES**: The total number of App types represented among Apps meeting the dashboard filters
- **APPS**: The total number of Apps represented in the dashboard
- **INSTANCES**: The total number of Instances contained in all Apps meeting dashboard filters
- **MONTH TO DATE**: The total month-to-date spend for all Apps shown in the dashboard
- **MEMORY**: The total memory allotted to selected Apps
- **STORAGE**: The total storage allotted to selected Apps

Blueprint Usage List

All Blueprints which have a currently-existing App provisioned from them and selected in the dashboard filters are listed here. The name and type of the Blueprint is listed along with the total number of Instances across all provisionings, total Groups, total Clouds, and the total count of all Apps from that Blueprint.

### 2.3.13 Workloads: Apps Usage

<table>
<thead>
<tr>
<th>APPS USAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>$0</th>
<th>5.8GB</th>
<th>22GB</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLOUDS</td>
<td>APPS</td>
<td>INSTANCES</td>
<td>TOTAL COST</td>
<td>MEMORY</td>
<td>STORAGE</td>
</tr>
</tbody>
</table>

**APP USAGE BY CLOUD**

VMware Demo Cluster: 2

Instance Usage

<table>
<thead>
<tr>
<th>CLOUD</th>
<th>COUNT</th>
<th>MEMORY</th>
<th>STORAGE</th>
<th>CPU</th>
<th>PRICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Demo Cluster</td>
<td>2</td>
<td>5.9GB</td>
<td>22.0GB</td>
<td>1</td>
<td>$0.07</td>
</tr>
</tbody>
</table>

The Apps Usage dashboard lists all provisioned Apps that meet a set of filters and organizes them by Cloud. Totals for cost and resource usage of all relevant Apps can be viewed with a per-Cloud breakdown.
Filters
Filter the Apps pulled into the dashboard by one or more of the following fields:

- App name (all matching search terms)
- Metric (apply to see the top Clouds by workload count, price, memory, storage, or CPU cores)
- Group
- Cloud
- Tenant
- Tag (Key)
- Value (Tag value)

Data Displayed
The following aggregate totals are compiled for Apps that meet set filters:

- **CLOUDS**: The total number of Clouds represented among Apps meeting the dashboard filters
- **APPS**: The total number of Apps represented in the dashboard
- **INSTANCES**: The total number of Instances contained in all Apps meeting dashboard filters
- **TOTAL COST**: The total cost of all selected Apps
- **MEMORY**: The total memory allotted to selected Apps
- **STORAGE**: The total storage allotted to selected Apps

Instance Usage List
All Clouds with a currently-provisioned App which is selected in the dashboard filters are listed here. The name of the Cloud is listed along with its App count, the total memory, total storage, total CPU cores and price of the Apps provisioned in that Cloud are also listed.

2.4 Guidance

2.4.1 Overview
The **Operations > Guidance** section shows recommendations for resource and cost optimization. By analyzing the CPU, RAM, and Storage activity of Instances and Hosts, Morpheus can recommend actions for sizing and power state. Guidance is customizable to show recommendations based on 30, 60, or 90 day periods, this dropdown toggle is visible on the Guidance list page (Operations > Guidance). Guidance thresholds are also customizable, they can be edited in **AdmSetGui**.

Configuration
Guidance is configured per Cloud and is turned off by default.

To turn on Morpheus Guidance for a Cloud:

1. Navigate to **Infrastructure > Clouds**
2. Click **EDIT**
3. Expand the **Advanced Options** section in the Edit Cloud modal
4. In the **Guidance** dropdown, select Manual
5. Click **SAVE CHANGES**

Guidance recommendations will begin to appear in the guidance section when generated.

Once Guidance has been turned on for a Cloud, Morpheus will determine if a guidance recommendation should be made once every 30 minutes. In the event that no recommendations can be made, no entry will be added to the list of suggested guidances. As the guidance list continues to grow, sorting and filtering may become necessary to focus on the recommendations that are relevant to the user at the time.

It’s important to note that acting on recommendations is entirely manual at this time. In many cases, Morpheus provides one-click action to take the recommended steps but Guidance recommendations cannot be taken automatically. This is a feature that is being explored for a future update but has not been tagged for any specific release version at this time. In addition, it’s recommended that Morpheus Agent be installed to maximize the benefits of Guidance. While Guidance will still work without installing the Agent, the greatly-enhanced statistics provided by the Agent will significantly improve Guidance recommendations.

To see more detail on a Guidance recommendation in your list, click on the (i) button at the far right side of each list row. This will open a detail modal that gives additional information on the Guidance entry. In some cases, such as with sizing and shutdown recommendations, the user can simply click the “EXECUTE” button to take the recommended action as shown below.

Other types of Guidance recommendations, such as reserve compute recommendations, must be taken in the cloud and Morpheus does not offer the execute button.
Note: The IGNORE button will remove the recommendation from the UI. Subsequent recommendations of the same type will NOT display for the same object (VM, Cloud etc) again unless the original recommendation is resolved.

Recommendations

To view and act on Guidance recommendations, navigate to Operations > Guidance.

The Guidance list contains the following details:

Severity Icon Indicates the severity of the recommended action.
Type Recommended action Type
Metric Guidance Metric used for recommended action.
Action Recommended Action for the Instance or Host, such as “Reduce Host memory” or “Shutdown Instance”
RESOURCE The Instance or Host targeted
SAVINGS Shows projected Monthly Costs savings if recommended action is taken.
DATE Date and Time stamp the recommended action was generated.
Information Link Click to view details on the recommendation.

Note: Guidance Actions are not automatically triggered at this time.
Filters

Search  Search for Guidance recommendations
Type  Filter by Sizing or Shutdown Guidance Types.
Severity  Filter by Guidance Severity of All, Info, Warning, or Critical.
Metric  Filter by All, Memory, CPU, or Power Guidance Metrics.

2.5 Wiki

The Morpheus Wiki is a tenant-wide, RBAC-controlled, auditable Wiki that allows easy UI, API and CLI access to information, notes, configurations or any other data needed to be referenced or shared with others. Wiki pages can be created directly from the Wiki tab of the detail page for various resource types, including Clouds, Groups, Servers, Instances, Clusters, and Self-Service Persona Catalog Items. Wiki pages created this way are automatically categorized under the appropriate resource type. Additional Wiki pages and custom categories can be created when viewing the whole Wiki at Operations > Wiki. Here you will also see the complete Wiki, including pages created on various object detail pages which are categorized appropriately.

2.5.1 Highlights

• Main Wiki section is at Operations > Wiki
• Wiki tabs are on Clouds, Groups, Instances, Hosts, VMs, Bare Metal, and Clusters detail pages
• Additional Wiki Pages and Categories can be created from Operations > Wiki
• When a Wiki tab is populated, a Page is automatically added and accessible at Operations > Wiki
• One Wiki is created per Tenant. There is no multi-tenant access to Wikis
• The Wiki is accessible from the UI, CLI and API.
• Wiki access is RBAC-controlled via the Operations: Wiki permission in User and Tenant Roles (None, Read and Full)
• Page updates are stamped with the “Last Updated By” user and the time the edit was made
• Wiki pages can be searched from /operations/wiki or navigated from /operations/wiki-page/page-index
• All wiki pages are encrypted using AES 256-bit encryption
• Wiki pages use Flexmark for Markdown. Annotate your Wiki pages with headers, text styling, code blocks, hyperlinks, and more as needed
• Create a new page with title “Home” to replace the default Wiki landing page that ships with Morpheus

Note:  The Wiki replaces Notes. Notes are automatically migrated to corresponding Wiki pages when upgrading Morpheus to 4.0.0+.

The Wiki service ties into assets throughout the environment. Create pages for Instances, hosts, groups, clouds, and even clusters directly on their detail pages. Or, just create general notes pages in the centralized Wiki section in Markdown format.

Creating your first page is as simple as clicking the Create Page button. Write down some content, give the page a title, and click SAVE. The wiki will also keep track of who last edited a page and when. The beauty of this wiki is that
its clean and easy to write down notes related to various parts of your application deployment or infrastructure without going to an external tool.

All wiki pages are encrypted using AES-256 bit encryption. Though we don’t advise storing passwords in a wiki document (services like Cypher are for that), role-based access control also can properly restrict access to content related to Instances or hosts the user may not have access to.

To get started, simply create a page with the title Home. When that page is created, it will become the new default page for the Wiki and visible by all the users that have access to this section.

### 2.6 Costing

#### 2.6.1 Budgets

Budgets provide insight into spending across their designated scope, allowing users to create and plan a budget targeted to their account, clouds, tenants, users, or groups.

**Creating A Budget**

1. Navigate to **Operations > Costing > Budgets**
2. Start a new budget by clicking **+ ADD**
   1. **Name**
   2. **Description**
   3. **Scope**: Here you can choose which construct this budget is tied to (Account, Tenant, Cloud, Group, or User)
   4. **Period**: Currently “Year” is the only option
   5. **Year**: Select a year to set budgets for future years. Alternatively, select “custom” to create a multi-year budget or input a custom fiscal year if required by your organization
   6. **Interval**: Choose Month, Quarter, Year then fill in the budgeted amount for that interval
3. Click **SAVE CHANGES**
Multi-year Budgets

Some organizations may need to create multi-year budgets or may need to set a fiscal year period. By default, annual budgets are tied to a calendar year (January - December) but Morpheus offers the flexibility of setting a fiscal year period when needed. When selecting a value from the YEAR dropdown in the add/edit budget modal, select “Custom” rather than one of the discreet years from the list. After selecting Custom, START DATE and END DATE fields allow the user to input any desired fiscal year period. Users can enter a period of up to three years using the start and end date bookends. The entered period must be one, two or three full years, partial years are not permitted.

In the example below, I’ve created a three-year budget:
Cloud Budgets

If you scope a budget to a Cloud, visit the Cloud summary tab in Infrastructure > Clouds > Select Cloud to see a cost-to-budget breakdown for that Cloud.
To view the budget summary, click into the budget to see a breakdown of budgeted amounts against actual costs for the selected interval period. Budgets can be edited or deleted by clicking the pencil or trash can icons, respectively, for each budget.
Budget Analytics

In Operations > Analytics > Budget Analysis select scope (Account, Tenant, Cloud, Group, User) to view the budget analysis. If a budget exists for the selected scope, a cost breakdown against budgeted amounts will be shown.
Morpheus offers highly-granular costing data through invoices. Invoice views are highly customizable, allowing for nearly unlimited combinations of output columns and filtering. Invoices are based on monthly periods and allow you to slice costs in a highly granular way, as well as predict final monthly costs before the end of the period. As with other Morpheus UI pages that support advanced table customization, these views can be saved to provide easy access to costing views specific to varying business needs. By default, the invoice list page will show the last three months’ invoices across all clouds and invoice types but the list can be modified to target differing time periods or resource groupings. Read on in this section to discover the meaning of various invoice types and how this tool can be used to create targeted costing views.

Invoices for Public vs On-Prem Clouds

Morpheus supports live cost syncing for many public clouds, including all of the most commonly-used public clouds like Amazon AWS, Microsoft Azure, and Google Cloud Platform. For these clouds, costing sync is enabled through the COSTING field on the Add/Edit Cloud modal (Infrastructure > Clouds > selected Cloud > EDIT button). When live costs are synced from public clouds, invoices will be generated for this activity including month-to-date costs, projected monthly totals, historical cost data, and a lot more which is discussed in the following sections. Additionally, Morpheus has implemented a costing service for on-prem clouds to closely mirror the live costing experience through a public cloud. As with public clouds, this costing service is enabled for on-prem clouds through the COSTING field on the Add/Edit Cloud modal (Infrastructure > Clouds > selected Cloud > EDIT button). Change the setting to “Sync Costing” and save the changes to the cloud integration. From this point, costs will be aggregated into

2.6.2 Invoices

Morpheus offers highly-granular costing data through invoices. Invoice views are highly customizable, allowing for nearly unlimited combinations of output columns and filtering. Invoices are based on monthly periods and allow you to slice costs in a highly granular way, as well as predict final monthly costs before the end of the period. As with other Morpheus UI pages that support advanced table customization, these views can be saved to provide easy access to costing views specific to varying business needs. By default, the invoice list page will show the last three months’ invoices across all clouds and invoice types but the list can be modified to target differing time periods or resource groupings. Read on in this section to discover the meaning of various invoice types and how this tool can be used to create targeted costing views.

Invoices for Public vs On-Prem Clouds

Morpheus supports live cost syncing for many public clouds, including all of the most commonly-used public clouds like Amazon AWS, Microsoft Azure, and Google Cloud Platform. For these clouds, costing sync is enabled through the COSTING field on the Add/Edit Cloud modal (Infrastructure > Clouds > selected Cloud > EDIT button). When live costs are synced from public clouds, invoices will be generated for this activity including month-to-date costs, projected monthly totals, historical cost data, and a lot more which is discussed in the following sections. Additionally, Morpheus has implemented a costing service for on-prem clouds to closely mirror the live costing experience through a public cloud. As with public clouds, this costing service is enabled for on-prem clouds through the COSTING field on the Add/Edit Cloud modal (Infrastructure > Clouds > selected Cloud > EDIT button). Change the setting to “Sync Costing” and save the changes to the cloud integration. From this point, costs will be aggregated into
invoices for on-prem clouds in the same way as public clouds including complete line item listings, current costs for the month, month-end projections, and much more as discussed in the next sections.

**Invoice List Page**

The invoices list page shows high-level aggregate data on a group of invoices and allows you to locate a specific invoice for a deeper look. By default, invoices from the last three months across all clouds and types are shown here. Depending on settings, this page can automatically refresh itself so the list of displayed invoices and the aggregate information on them is up to date.

**Aggregated Invoice Data**

The following aggregate totals are displayed for all invoices picked up by set filters:

- **Periods**: The total number of months in the period determined by your start and end date filters. If no start and end dates are set, a three month period will be shown. If a one-month period is selected, the name of that month (ex. Aug 2020) is shown

- **Total Invoices**: The total number of invoices captured by current filters

- **MTD Cost**: The combined month-to-date cost for all invoices captured by current filters

- **Total Cost**: The expected total month-end cost for all invoices captured by current filters
Creating Views

Invoice list views are highly-customizable allowing for virtually limitless combinations of output columns and filtering. A common set of output columns is provided in a default view but users can add and remove columns from a large list of data points and even save multiple views for easy access to different data sets. Any of your stored views can be set as the default to be displayed each time the invoices list page is active.

To create a new invoices view:

1. Click the gear icon
2. Click on one or more columns from the “Columns” list to add or remove an output field
3. Click “+ add view”
4. Provide a name and a description value for your new view
5. If desired, mark the box to set the new view as your default view so it appears automatically each time the invoices list page is accessed
6. Click SAVE

Available Output Columns

When creating an invoices view, there are many output columns available to select. Consult the list below for more details on each of the available columns:

Available Output Columns: Expand for Complete List

- **Invoice ID**: The unique ID in Morpheus for the invoice
- **Type**: The invoice type; Cloud, Container, Group, Server, Instance, Resource, User, or Volume
- **Ref ID**: An ID for the reference object tied to the invoice (server, instance, cloud, etc.). Reference IDs are reused across invoice types so invoices referring to identical Ref IDs may not necessarily refer to the same reference object
- **Reference**: The name of the reference object (server, cloud, user, group, etc.) tied to the invoice
• **Cloud ID:** The internal ID for a Cloud integration in Morpheus. This field will be blank unless the invoice references a Cloud

• **Cloud:** The name for a Cloud integration in Morpheus. This field will be blank unless the invoice references a Cloud

• **Instance ID:** The internal ID for an Instance in Morpheus. This field will be blank unless the invoice references an Instance

• **Instance:** The name for an Instance in Morpheus. This field will be blank unless the invoice references an Instance

• **Server ID:** The internal ID for a server in Morpheus. This field will be blank unless the invoice references a server

• **Server:** The name for a server in Morpheus. This field will be blank unless the invoice references a server

• **Cluster ID:** The internal ID for a cluster in Morpheus. This field will be blank unless the invoice references a cluster

• **Cluster:** The name for a cluster in Morpheus. This field will be blank unless the invoice references a cluster

• **Plan ID:** The internal ID for a service plan in Morpheus. This field will be populated only for invoices that reference an object which would be associated with a service plan (server, Instance, container, etc.).

• **Plan:** The name for a service plan in Morpheus. This field will be populated only for invoices that reference an object which would be associated with a service plan (server, Instance, container, etc.).

• **Group ID:** The internal ID for a Group in Morpheus. This field will be blank unless the invoice references a Group

• **Group:** The name for a Group in Morpheus. This field will be blank unless the invoice references a Group

• **User ID:** The internal ID for a User in Morpheus. This field will be blank unless the invoice references a User.

• **User:** The name for a User in Morpheus. This field will be blank unless the invoice references a User.

• **Tenant ID:** The internal ID for the Morpheus Tenant which owns the reference object

• **Tenant:** The name of the Morpheus Tenant which owns the reference object

• **Period:** The monthly period during which the invoice was generated

• **Interval:** The length of the invoice billing period, currently all invoices are generated at a one-month interval

• **Start Date:** The start date and time for the invoice period, typically the first of the month at midnight

• **End Date:** The end date and time for the invoice period, typically the last day of the month at midnight

• **Ref Start:** The date and time the reference object is created or the start of the invoicing period if the reference object existed prior to the start of the invoicing period

• **Ref End:** The date and time the reference object is decommissioned or the end of the invoicing period if the reference object still existed at the end of the period

• **Compute Cost:** The actual compute costs for the invoice (from public cloud costing API when available or from an on-prem cloud with “Sync Costing” enabled)

• **Storage Cost:** The actual storage costs for the invoice (from public cloud costing API when available or from an on-prem cloud with “Sync Costing” enabled)

• **Network Cost:** The actual network costs for the invoice (from public cloud costing API when available or from an on-prem cloud with “Sync Costing” enabled)

• **Extra Cost:** The actual additional costs for the invoice (from public cloud costing API when available or from an on-prem cloud with “Sync Costing” enabled)
• **MTD Cost**: The actual month-to-date costs for the invoice (from public cloud costing API when available or from an on-prem cloud with “Sync Costing” enabled)

• **Total Cost**: The actual total costs for the invoice (from public cloud costing API when available or from an on-prem cloud with “Sync Costing” enabled)

• **Metered Compute Cost**: Compute costs determined by Morpheus usage and pricing data (when live pricing data is not available, such as with an on-prem cloud without “Sync Costing” enabled)

• **Metered Storage Cost**: Storage costs determined by Morpheus usage and pricing data (when live pricing data is not available, such as with an on-prem cloud without “Sync Costing” enabled)

• **Metered Network Cost**: Network costs determined by Morpheus usage and pricing data (when live pricing data is not available, such as with an on-prem cloud without “Sync Costing” enabled)

• **Metered Extra Cost**: Additional costs determined by Morpheus usage and pricing data (when live pricing data is not available, such as with an on-prem cloud without “Sync Costing” enabled)

• **Metered MTD Cost**: Month-to-date costs determined by Morpheus usage and pricing data (when live pricing data is not available, such as with an on-prem cloud without “Sync Costing” enabled)

• **Metered Total Cost**: Total costs determined by Morpheus usage and pricing data (when live pricing data is not available, such as with an on-prem cloud without “Sync Costing” enabled)

• **Compute Price**: The actual compute price (cost plus markup) for the invoice (from public cloud costing API when available or from an on-prem cloud with “Sync Costing” enabled)

• **Storage Price**: The actual storage price (cost plus markup) for the invoice (from public cloud costing API when available or from an on-prem cloud with “Sync Costing” enabled)

• **Network Price**: The actual network price (cost plus markup) for the invoice (from public cloud costing API when available or from an on-prem cloud with “Sync Costing” enabled)

• **Extra Price**: The actual additional price (cost plus markup) for the invoice (from public cloud costing API when available or from an on-prem cloud with “Sync Costing” enabled)

• **MTD Price**: The actual month-to-date price (cost plus markup) for the invoice (from public cloud costing API when available or from an on-prem cloud with “Sync Costing” enabled)

• **Total Price**: The actual total price (cost plus markup) for the invoice (from public cloud costing API when available or from an on-prem cloud with “Sync Costing” enabled)

• **Active**: Indicates whether or not the reference object is currently existing and active

• **Date Created**: The date and time the invoice is created

• **Last Updated**: The date and time the invoice was last updated
Invoice Types

Invoices can reference any of the Morpheus workload element types or resource reference types in the list below. Some invoice types are broader and may account for resource costs calculated in other narrower invoice types. For instance, a container-type invoice returns costs for a single node of an Instance while an Instance-type invoice for the same period may be including costs for that same single node. The invoices list view can be filtered to show just one type or all types. Complete descriptions of each invoice type are included below:

- **Cloud:** In Morpheus, a Cloud is any connection into a public cloud, private cloud, hybrid cloud, or bare metal server
- **Container:** A single node of a service, in other words, a single node of a Morpheus Instance. This could be a virtual machine or Docker container which is part of a Morpheus-managed Instance
- **Group:** In Morpheus, Groups define which resources a user has access to through their role. Clouds are added to Groups and users access Clouds to which their roles give access
- **Server:** A server refers to any individual host, virtual machine, or bare metal server that is inventoried or managed by Morpheus. This can include servers which are parts of Morpheus-managed Instances or inventoried servers from integrated Clouds
- **Instance:** A set of containers or virtual machines which correlate to a single horizontally-scalable entity. This could be a single VM or it could be many VMs operating as a service
- **Resource:** Resource-type invoices are generated when Morpheus cannot determine that the referenced costs belong to any of the other resource reference types in this list
- **User:** User-type invoices aggregate the costs of resources owned by a specific Morpheus user during the invoicing period
- **Volume:** When possible, costs will be tied to known volumes and a volume-type invoice is generated as a result

Invoice Detail Page

Summary

The summary tab of the invoice detail page displays a great deal of reference information about the resource identified by the invoice. This will vary depending on the type of resource. In addition, total and projected costs are displayed along with cost breakdowns for compute, storage, network, and other categories. Month-to-date totals and final month projections are given.
The history tab displays the costs and prices for the associated resource over time. This tab is especially valuable for resources that have existed through at least a few invoicing periods to show changes over time. In addition, cost breakdowns for compute, storage, network, and other categories are shown for each invoicing period. These costs can be displayed visually through graphs.
Morpheus Documentation

For supported resource types, Morpheus includes a tab to display all costing line items. This provides the user with a complete list of line items that make up the costing totals on the invoice.

### Line Items

For supported resource types, Morpheus includes a tab to display all costing line items. This provides the user with a complete list of line items that make up the costing totals on the invoice.
2.6.3 Usage

The Operations > Costing > Usage section shows billing information for Instances and hosts that have pricing configured on their Service Plan.

**Important:** Pricing must be enabled in Administration > Settings > Provisioning and Service Plans configured with price sets in |AdmPla| for pricing to show in the Usage section.

### View Usage

All Instances are listed by default, with the most recent usage information showing first.

Usage details can be filtered by Cloud and date:

- **Cloud** Default view is for all Clouds. Select a Cloud to show Instance and host usage for only one Cloud.
- **Date** Default view shows most current Usage. Select the Date filter to scope to a different date range.

### API & CLI

Usage information can also be extracted via the Morpheus API and CLI, including the ability to extract usage per Tenant.

**Note:** Appropriate Role permissions for Operations: Usage are required to view the Usage section.
2.7 Approvals

Morpheus and Service Now Approvals

2.7.1 Overview

Policies can be created for Groups and Clouds to require approvals for actions with the built-in Morpheus approvals engine, or via a ServiceNow integration. Approvals can be configured for Provisioning and Lifecycle extensions.

2.7.2 Configuring Approvals

Configuring Morpheus for Approvals

To configure Morpheus for approvals:

1. Configure Roles for Approval access

2. Optionally configure a ServiceNow Integration for ServiceNow approvals.
   - Please note ServiceNow integration is not required for Internal Approvals.

3. Create approvals policies for:
   - Internal Approvals
   - SNOW Approvals

Configure Roles

Configure User Role access settings in Administration > Roles > (Role) > Operations: Approvals.

- All Users with a Role applied containing Operations: Approvals set to Full will have approval authority, and be able to Approve, Deny or Cancel approval requests.
- All Users with a Role applied that has Operations: Approvals set to Read will be able to view Approval requests and history, but will not be able to Approve, Deny or Cancel approval requests.
- All Users with a Role applied that has Operations: Approvals set to None will not have access to the Operations: Approvals section, and such will not be able to see or act on approval requests.
- Regardless of Role settings, any instance or app provisioned by any user to a group or cloud with an active Approval policy applied will require approval before the instance or app will provision.

ServiceNow Approvals

Configure ServiceNow integration for SNOW Approvals

1. Navigate to Admin > Integrations

2. Select + NEW INTEGRATION

3. Select ServiceNow from the Type dropdown in the Integration modal and enter:
   - Name Name of the integration in Morpheus
   - Enabled Leave checked to enable the integration.
   - Host URL of the ServiceNow host (ex: https://ven0000.service-now.com)
• **User** A User in ServiceNow that is able to access the REST interface and create/update/delete incidents, requests, requested items, item options, catalog items, workflows, etc.

• **Password** Password for User above

4. Save Changes

Morpheus then configures the integration with ServiceNow, syncs ServiceNow workflows which are available when creating approvals policies. (This process can take up to 5 minutes depending on the size of the workflow table in ServiceNow.)

### Create Approval Policies

- Policies applied to a Group are created in Infrastructure > Groups > (group) > Policies tab.
- Policies applied to a Cloud are created in Infrastructure > Clouds > (cloud) > Policies tab.

**To create an Approval policy:**

1. Navigate to the Policies tab in the Group or Cloud to which the policy will apply.
2. Select + ADD POLICY to open the New Policy wizard
3. Select Provision Approval from the Type dropdown
4. Add an optional description
5. **Leave Enabled selected for this Policy to be active once saved.**
   - Enabled can be deselected to disable to policy.
6. In the config section, select either Internal Approvals or ServiceNow Approvals:
   - **Internal Approvals** Approval requests will be managed within Morpheus via the Operations: Approvals section.
   - **ServiceNow Approvals** Approval requests will be managed with ServiceNow (SNOW). Please note a ServiceNow integration (Admin: Integrations) must be configured prior to SNOW Approval policy generation.
     - For ServiceNow Approvals, select the appropriate ServiceNow workflow for this policy. Please note the workflows presented are created in ServiceNow and synced with Morpheus.
7. Add the Morpheus Accounts to which this policy will apply, or leave the Accounts field blank to apply to all accounts.
8. Save

Upon saving, a new policy is created in the Group or Cloud Policies tab.

**Note:** SNOW Approvals will take a few moments to save as the policy is generated.
2.7.3 Managing Approval Requests

Once Instance approval policies are added to a Group or Cloud, any Instance or App provisioned into that Group or Cloud will create an approval request entry in the Operations > Approvals section.

**Note:** User Role permission Operations: Approvals > FULL is required to manage Approvals.

- To Approve, Deny, or Cancel an internal approval request, select the request and use the Actions dropdown.
- To Cancel a ServiceNow Approval request, select the request and use the Actions dropdown. ServiceNow approvals are managed in ServiceNow.

**Note:** Instances requiring provisioning approval will have a PENDING status until approved.

Each Approval Request will have:

- Name: A name for the approval in Morpheus
- Monthly Price (Est.): The estimated monthly price of the Instance to be provisioned
- Request Type: What is being requested, such as Instance approval
- External Name: For ServiceNow integrations, the name of the approval in the ServiceNow console
- Type: Internal or ServiceNow
- Status
- Date Created
- Requested By: The Morpheus user making the request

**Actions dropdown (for internal approval requests)**

- Approve
- Deny
- Cancel

**Actions dropdown (for ServiceNow requests)**

- Cancel

**Note:** The Approvals list view can be sorted by NAME, REQUEST TYPE, EXTERNAL NAME, DATE CREATED, and REQUESTED BY

**Internal approval requests**

To Approve, Deny or Cancel an Internal approval request:

1. Navigate to Operations > Approvals
2. Select the Name of the Approval request
3. Select Actions on the far right of the request
4. Select Approve, Deny, or Cancel from the Actions dropdown
5. Select OK on the confirmation modal
• When an Internal request is approved, the related instance will begin to provision immediately and the request will show approved.
• When an Internal request is denied, the related instances status will change to Denied and the request will show Rejected in the Approvals section.
• When an Internal request is canceled, the related related instances status will change to Cancelled and the request will be canceled.

ServiceNow Approval requests

ServiceNow approval request are managed in ServiceNow. The process of approving or rejecting requests is determined by the ServiceNow Workflow selected when configuring the SNOW Approval policy. These Workflows are configured in ServiceNow.

Important: Morpheus syncs with ServiceNow every 5 minutes. Once an Approval Request is Approved or Rejected in Service Now, it will take up to 5 minutes for the instance to respond accordingly, and the status for the approval request in the Approvals section in Morpheus to update.

2.8 Activity

The Activity section displays a recent activity report for Auditing. Morpheus defines an activity as any major action performed on an instance or server, such as, but not limited to adding a server, deleting a server, provisioning an instance, deleting an instance, creating a backup, etc… This view can be searched and filtered by type, user, and date range.

2.8.1 Activity

There are four types of activities that are displayed in the Activity Reports:

• Backup
• Provisioning
• Alert
• Permissions

To View a Recent Activity report:

1. Select the Operations link in the navigation bar.
2. Select Activity in the sub navigation bar.

Recent activity is displayed in order from recent to oldest. This view can be searched and filtered by type, user, and date range.

Review

To review the item the activity occurred on, click the name of the activity and it will go to a new page and display that item.
Note: Deleted activities are displayed as an alert and do not contain a link to the event item. If the activity is not a deletion event we provide a link on the activity name to go to the item the activity occurred on. Delete activity alerts are shown for Instances, servers, Clouds, Groups, and Monitoring Checks.

To Filter:

1. Click the filter drop down of type of filter you want to apply.
2. Select the appropriate filter.

2.8.2 Alarms

The ALARMS section shows Operation notifications from Cloud and other Service Integrations. Cloud and other Service Integration Alarms are not generated by Morpheus but synced and displayed for visibility in Morpheus.

2.8.3 History

The HISTORY section shows Process History from Instances and Apps processes. This is an aggregate view of the History tab in Instance and App details pages.

Processes can be expanded to view all process steps and process history detail including output and errors.

Access to HISTORY is given by the Operations:Activity Role permission.

The Logs displayed in Administration - Health - Morpheus Logs are from /var/log/morpheus/morpheus-ui/current. These logs show all ui activity and are useful for troubleshooting and auditing.

Note: Stack traces in Administration - Health - Morpheus Logs are filtered for Morpheus services. Complete stack traces can be found in /var/log/morpheus/morpheus-ui/current.
There are several capabilities in the Morpheus provisioning engine. Things ranging from application / service deployments via containers, virtual machines, and even bare metal. Deployment management and app template construction are also core aspects of the provisioning engine. Take advantage of custom tasks and workflows within any environment by building tasks and workflows from those tasks. There is a lot of information to cover with regards to provisioning but Morpheus makes it intuitive and smooth.

3.1 Requirements

Provisioning Instances and Apps typically involves many steps beyond starting a workload. Morpheus is centered around automating everything desired for your application to be fully operational, including networking, storage, hostnames, domains, dns, licenses, scripts/automation, scaling, load balancers, security, accessibility, governance, auditing, monitoring, backups, costs, sizing and on and on. Point being there is a lot that goes on when spinning up an instance or app, and to make the magic happen a few requirements need to be met.

Important: By default, Agent Installation is enabled when provisioning unless deselected on the Virtual Images or SKIP AGENT INSTALL is selected when provisioning.

3.1.1 VM Provision Steps

While an infinite number of steps can happen when provisioning an Instance or App using VM(s) in Morpheus, the basic order is:

- Look for Virtual Image

  Morpheus will check if the Virtual Image set on the Node Type or selected during provisioning is already available in the source Cloud. If not and it is an Uploaded/Local Image, Morpheus will attempt to upload the Image to the target Cloud.

- Upload Image

  For Uploaded/Local Images that do not exist in the target cloud, Morpheus will need to upload the Image. Ensure the Virtual Image is valid for the target Cloud, the Image meets the target cloud upload requirements, and Morpheus has network access and permissions to upload the image.

Note: When uploading an image to a VMware Cloud, the Virtual Image is copied directly to the target ESXi host, NOT through the vCenter server. Ensure the Morpheus Appliance(s) can resolve target ESXi hostnames and connect on port 443 for successful vmdk/ova uploads.
Clone Image

Once the Image is confirmed available in the target cloud, Morpheus will clone the Image to the target Datastore.

**Note:** The target host must have access to the target Datastore of the Image

- Reconfigure Image
  Once cloned, Morpheus will resize the Image based off provisioning parameters

- Cloud-init (if enabled)
  **Attached cloud-init iso** When using cloud-init, Morpheus will attach a tiny metadata iso to the new VM. Network, Machine, User and any other cloud-init metadata will be sourced from this iso.
  **VM Tools** Morpheus will run Guest Customizations via VMware VM Tools, including network config when assigning static IP’s.

- Wait for Power On status and Network info
  Morpheus will wait to hear back from the target cloud/hypervisor that the VM has successfully started and has an IP address.

**Note:** If VM TOOLS INSTALLED? is NOT checked on the source Virtual Image configuration, Morpheus will skip waiting for network.

- Finalize
  By default this will include Agent Installation and any post-provision scripts or workflows or integration automation steps.

  **Important:** If the VM is stuck in finalize for longs periods of time, this typically means the Agent cannot be installed or has not been heard back from. This will result in a ! warning Instance status upon provisioning completion.

  If agent installation is not possible or desired, uncheck “Install Agent” on the source Virtual Image configuration or select “Skip Agent Install” during provisioning to speed up provisioning completion.

### 3.1.2 Virtual Images

While containers are the future, the most common provisioning method involves Virtual Machines, and the most important part of Provisioning a VM is the Virtual Image. When provisioning a VM, Morpheus will need to do a few things depending on the location of the Virtual Image and if agent install, console access, and script execution is desired.

**Synced Images need to be properly configured** Morpheus gathers as much metadata for synced images as possible, but depending on the cloud, os, image configuration, agent install settings, by default the synced Virtual Images may not be ready to provision until configured. The Virtual Image is already at the target Cloud, but datastore selection, credentials, cloud-init settings, and networks and security settings on the Virtual Image can cause provisioning issues.

**Local/Uploaded Virtual Images** Images uploaded to Morpheus are configured during the Add Virtual Image process, however Morpheus in most scenarios will still need to copy the Virtual Image to the target Hypervisor/Cloud upon the first provision to the target Cloud. In addition to the requirements for provisioning a synced Virtual
Image, copying an uploaded Virtual Image to the target Cloud is required and network and image configurations can cause upload failures, resulting in provisioning issues.

**Marketplace Images**  
AWS and Azure marketplace Images can be provisioned using the generic Amazon or Azure Instance Types, or added as Virtual Images as scoped to Node Types for custom Instance Types. Marketplace items provisioned/added to Morpheus still fall upon the requirements of the target Cloud, such as matching the region with the Image and licensing.

**Synced Images**

When a Cloud is added to Morpheus, all available Images/Templates records from that Cloud will be synced in regardless of Inventory settings on the Cloud. These Image records will be available in the Virtual Images section and can be provisioned by using the target clouds generic Instance Type, ie VMware, Amazon, Azure, Openstack etc Instance Types, or by creating custom Instance Types and selecting the Image on a Node Type.

**Note:**  
Synced Virtual Images are just meta-data records in Morpheus pointing to the Image in the target Cloud. The actual Image files are not copied/imported to Morpheus.

Before provisioning a synced Virtual Images, ensure the image is configured properly:

**Name**  
Name of the Virtual Image in Morpheus. This can be changed from the name of the Image, but editing will not change the name of the actual Image.

**Operating System**  
 Specifies the Platform and OS of the image. All Windows images will need to have Operating System specified on the Virtual Image, as Morpheus will assign Linux as the Platform for all Images without Operating System specified.

**Minimum Memory**  
The Minimum Memory setting will filter available Service Plans options during provisioning. Service Plans that do not meet the Minimum Memory value set on the Virtual Image will not be provided as Service Plan choices.

**Cloud Init Enabled?**  
On by default, uncheck for any Image that does not have Cloud-Init or Cloudbase-Init installed.

---

**Important:** Provisioning a Virtual Image that has **Cloud Init Enabled?** checked on the Virtual Record in Morpheus but does not have cloud-init installed will result in immediate provisioning failure.

---

**Install Agent**  
On by default, uncheck to skip Agent install. Note this will result in the loss of utilization statistics, logs, script execution, and monitoring. (Some utilization stats are collected for agent-less hosts and vm’s from VMware and AWS clouds).

**Username**  
Existing Username on the Image. This is required for authentication, unless Morpheus is able to add user data, Cloud-Init, Cloudbase-Init or Guest Customizations. If Cloud-Init, Cloudbase-Init Guest Customizations or Nutanix Sysprep are used, credentials are defined in Administration > Settings > Provisioning and User Settings. If credentials are defined on the Image and Cloud-Init is enabled, Morpheus will add that user during provisioning, so ensure that user does not already exist in the image (aka root). For Windows Guest Customizations, Morpheus will set the Administrator password to what is defined on the image if Administrator user is defined. Do not define any other user than Administrator for Windows Images unless using Cloudbase-init. Morpheus recommends running Guest Customizations for all Windows Images, which is required when joining Domains as the SID will change.

**Password**  
Password for the Existing User on the image if Username is populated.

**Storage Provider**  
Location where the Virtual Image will be stored. Default Virtual Image Storage location is /var/opt/morpheus/morpheus-ui/VMs. Additional Storage Providers can be configured in Infrastructure > Storage.
Cloud-Init User Data  Accepts what would go in runcmd and can assume bash syntax. Example use: Script to configure satellite registration at provision time.

Permissions

Set Tenant permissions in a multi-tenant Morpheus environment. No impact on single-tenant environments.

Visibility

Private  Image is only available in the specified Tenants below.
Public  Image is available to all Tenants.

Tenant  If Visibility is set to Private, specify Tenants the Image will be available for.

Auto Join Domain?  Enable to have Instances provisioned with this image auto-join configured domains (Windows only, domain controller must be configured in Infrastructure > Network and the configured domain set on the provisioned to Cloud or Network).

VirtIO Drivers Loaded?  Enable if VirtIO Drivers are installed on the image for provisioning to KVM based Hypervisors.

VM Tools Installed?  On by default, uncheck if VMware Tools (including OpenVMTools) are not installed on the Virtual Image. Morpheus will skip network wait during provisioning when deselected.

Force Guest Customization?  VMware only, forces guest customizations to run during provisioning, typically when provisioning to a DHCP network where guest customizations would not run by default. This is required for host/computer name definitions. domain joining, licenses and user definitions when using DHCP.

Trial Version  Enable to automatically re-arm the expiration on Windows Trial Images during provisioning.

Enabled Sysprep?  Applicable to Nutanix Only. Enable if the Windows Image has been sysprepped. If enabled, Morpheus will inject Unattend.xml through the Nutanix API (v3+ only)

Important:  Provisioning a Virtual Image that has Cloud Init Enabled?  checked on the Virtual Record in Morpheus but does not have cloud-init installed will result in immediate provisioning failure.

Important:  For Linux images without cloud-Init, an existing username and password must be defined on the Virtual Image record for Agent Install, Domain joining, licensing, script execution and other automation, and SSH or RDP Console access.

Local Virtual Images

A Local Virtual Image means it has been uploaded to Morpheus. To provision, Morpheus will need to upload the Image to the target Cloud upon first provision.

- Ensure the Virtual Image is valid for the target Cloud, the Image meets the target cloud upload requirements, and Morpheus has network access and permissions to upload the image.

Note:  When uploading an image to a VMware Cloud, the Virtual Image is copied directly to the target ESXi host, NOT through the vCenter server. Ensure the Morpheus Appliance(s) can resolve target ESXi hostnames and connect on port 443 for successful vmdk/ova uploads.

Once a Local Virtual Image has been uploaded to a Cloud, subsequent provisions will use the Image local to the cloud instead of uploading again as long as the copied image is still available in the source Cloud.
3.1.3 Agent Install

When provisioning an instance, there are some network and configuration requirements to successfully install the morpheus agent. Typically when a vm instance is still in the provisioning phase long after the vm is up, the instance is unable to reach Morpheus, or depending on agent install mode, Morpheus is unable to reach the instance.

The most common reason an agent install fails is the provisioned instance cannot reach the Morpheus Appliance via the appliance_url set in Administration > Settings over both 443 and 80. When an instance is provisioned from Morpheus, it must be able to reach the Morpheus appliance via the appliance_url or the Agent will not be installed.

In addition to the main appliance_url in Administration > Settings, additional appliance_urls can be set per cloud in the Advanced options of the cloud configuration pane when creating or editing a cloud. When this field is populated, it will override the main appliance url for anything provisioned into that cloud.

**Tip:** The Morpheus UI current log, located at /var/log/morpheus/morpheus-ui/current, is very helpful when troubleshooting agent installations.

**Agent Install Modes**

There are 3 Agent install modes:

- ssh/winrm
- VMware Tools
- cloud-init

**For All Agent Install modes**

When an instance is provisioned and the agent does not install, verify the following for any agent install mode:

- The Morpheus appliance_url (Administration > Settings) is both reachable and resolvable from the provisioned node.
- The appliance_url begins with to **https://**, not **http://**.

**Note:** Be sure to use **https://** even when using an IP address for the appliance.
Morpheus Documentation

- Inbound connectivity access to the Morpheus Appliance from provisioned VM’s and container hosts on port 443 (needed for agent communication)
- Private (non-morpheus provided) vm images/templates must have their credentials entered. These can be entered/edited in the Library > Virtual Images section but clicking the Actions dropdown of an image and selecting Edit.

**Note:** Administrator user is required for Windows agent install.

- The instance does not have an IP address assigned. For scenarios without a DHCP server, static IP information must be entered by selecting the Network Type: Static in the Advanced section during provisioning. IP Pools can also be created in the Infrastructure > Networks > IP Pools section and added to clouds network sections for IPAM.
- DNS is not configured and the node cannot resolve the appliance. If DNS cannot be configured, the IP address of the Morpheus appliance can be used as the main or cloud appliance.

**SSH/Winrm**

**Linux Agent**

- Port 22 is open for Linux images, and SSH is enabled
- Credentials have been entered on the image if using custom or synced image. Credentials can be entered on images in the Library > Virtual Images section.

**Windows Agent**

- Port 5985 must be open and WinRM enabled for Windows images.
- Credentials have been entered on the image if using custom or synced image. Credentials can be entered on images in the Library > Virtual Images section.

**Note:** Administrator user is required for Windows agent install.

**VMware tools (vmtools) rpc mode**

- VMware tools is installed on the template(s)
- Credentials have been entered on the Image if using uploaded or synced image when Cloud-init or Guest Customizations or Sysprep for Windows are not used. Credentials can be entered on Images in the Library > Virtual Images section.
Cloud-Init agent install mode

- Cloud-Init is configured in Administration > Settings > Provisioning section
- Provisioned image/blueprint has Cloud-Init (linux) or Cloudbase-Init (windows) installed

3.2 Provisioning Concepts

Morpheus is a powerful infrastructure agnostic Cloud Application Management Platform. As a result of this there are some differing concepts compared to other CMP platforms in the space. It is here that it is important to notice the qualification difference between Morpheus and other platforms.

Morpheus refers to itself as a CAMP (Cloud Application Management Platform) as opposed to a (Cloud Management Platform). While that may seem minor, it actually is a big deal. Many CMP based applications start at the IaaS layer and work up to the application layer (often needing additional PaaS) architectures to fill out the model. Morpheus was designed from a middle-ground perspective. As such some concepts are a bit different. This provides a more complete platform that allows for greater capabilities out of the box as will be seen when these concepts are covered.

3.2.1 Instances

Morpheus starts with provisioning Instances. In some platforms an Instance is representative of a singular object like a “Virtual Machine” in Amazon. In Morpheus, this concept was rethought. An Instance is more of a representation of a Resource or Service. This service may involve several virtual machines or even several docker containers.

For example, in the morpheus Instance wizard Mongo is an option and contains several “Instance Configurations”. One of these configurations is a full Mongo cluster consisting of either seven virtual machines or seven docker containers. Rather than representing these directly as seven individual “instances”, Morpheus groups them together into a singular instance of a service that contains multiple containers or virtual machines. This even allows for instance actions that can be performed to expand capacity on an instance (either horizontally or vertically). In the past, a database server may have been representative of a singular server, but this model has drastically changed in a big data world. This same concept also can apply to something like a simple Apache web server where there are 10 copies of a web server horizontally scaled out to handle traffic.

When viewing an instance detail page, one is able to look at details/statistics specific to a virtual machine or container. Morpheus simply helps simplify the management model for tracking these services.

3.2.2 Containers / Nodes / Virtual Machines

In relation to Instances, an instance can have many nodes. A node is a generic representation of a container or a virtual machine. In most cases, Morpheus will represent a node as a Container or Virtual Machine depending on the provisioning engine used for the instance. Node is just a generic naming representation when referring to these types of items. The public developer API, however, often refers to both virtual machines and docker containers as Containers. The UI was since updated to better delineate this concept for easier understanding but in essence the name is valid for both concepts of containerized environments as well as Virtual Machines. In fact, one can even think of a Docker Host as a Hypervisor (which we do).
3.2.3 Hosts / Servers

This concept is mostly tailored to users of morpheus responsible for managing and maintaining the underlying infrastructure integrations. A Host typically refers to a Docker Host in which a container in an instance is running, or a hypervisor virtual machines can be provisioned onto. A Server is the underlying general representation of a physical or virtual server. It could be a Host representation, a Virtual Machine, or even a Bare Metal delineation.

When a user provisions a vm based instance, a corresponding server record is created to represent the link to the actual resource via the underlying provisioning engine. This may seem a bit odd but provides an aspect of Morpheus that is quite powerful. This singular concept is what allows Morpheus to ingest “Brownfield” environments. We do not need to start clean. Morpheus can be integrated into existing environments and manage existing virtual machines. The way Morpheus does this is by periodically syncing existing vms from the added cloud integrations. A server record will be created and periodically updated (5 minutes typically) with realtime information and changes. This, in essence, provides CMDB based capabilities as well. When a server is discovered, the user (given the appropriate access) can convert the virtual machine to a managed instance. When this is done a corresponding Instance is made in the provisioning section of Morpheus and the Morpheus Agent can also optionally be installed to provide more refined guest operating system level statistics and logging.

3.2.4 Apps

On top of all the previous concepts, Morpheus provides an Apps layer. An App is a collection of Instances linked together via application tiers. Tiers allow the user to define segregated sections of connectivity between the various elements / instances within an application. Once these instances are all linked together in an application concept, this may affect Instance environments and provide service discovery capabilities for them to cross connect. There are several service discovery aspects within morpheus as well as integrations with services.

3.2.5 Blueprints

A blueprint is typically referred to as an Application Blueprint. It allows a user to define an application structure for easy reproducibility and deployment into various environments. They can be used to mix and match various instance types to provision an application dependent on multiple layers of services.

3.3 Catalog

The Catalog presents a simplified self-service view where users can select and deploy Instances, Blueprints or Workflows with pre-defined configuration in just a few clicks and without presenting an overwhelming list of options. Selections are presented as tiles and users can add items to a cart as if shopping on an eCommerce website. For users who tend to provision regularly from a small selection of Instance Types and configurations, the catalog is an easier option compared with the much more detailed and option-rich Instance provisioning wizard.

3.3.1 Configuring Catalog Item Access

Within the Catalog, users are presented with selections based on their User Role. Additionally, Catalog Item access can be set on the Tenant Role to restrict certain items from all users in the Tenant. By default, User Roles have no access to any catalog items. Thus, administrators will need to enable access to some Catalog Items in order for users to make use of this view.

Configuring Global Access:

- **Full**: Gives access to all Catalog Items
- **Custom**: Gives access to individually-selected items from the list below
• **None:** No access is given to any Catalog Items

**Tip:** When giving Custom access, be sure to set access on some of the individual catalog items to Full in order to reveal those items to the Role group.

### 3.3.2 Catalog

The catalog shows the complete list of pre-defined catalog items available to the user for provisioning. Catalog items are not created here, however. For more on creating catalog items, see the Catalog Items tab in the Morpheus Library section (Library > Blueprints > Catalog Items).

![Morpheus Catalog](image)

### 3.3.3 Placing Orders

From the Catalog page, select the tile for your chosen item to see any custom options that may need to be set prior to provisioning.
Once the item is in the cart, make any additional selections to complete the order. Once finished, proceed to the cart by clicking on the cart icon at the top of the application window. Click “Review Order”. When reviewing your order, each selected item is listed along with its estimated cost. The total estimated cost for the entire order is also computed.

Once **PLACE ORDER** is clicked, the provisioning process will begin and the user is redirected back to the catalog page. Any new orders can be viewed in Inventory and additional details can be accessed through the Inventory item detail page.
3.3.4 Inventory

The Inventory Page reveals the complete list of items which have been ordered by the user and provisioned. Users will only see their own items in this section.

3.3.5 Inventory Detail

Access the detail page for an item in your inventory by clicking the View Details link. The page displayed will look very similar to an Instance or App detail page in the Standard Persona. Highly detailed information on the health of the Instance or App are shown here. We can also take actions against Instances such as running Tasks or Workflows, reconfiguring the Instance, controlling the power state, and more.
3.4 Instances

Instances is a great starting point for taking advantage of self service features and spinning up both VM’s and containers. In Morpheus it may be advisable to cover the definition of a few terms used within the application so as to reduce confusion.

**Instance** A set of containers or virtual machines that can correlate to a single horizontally scalable entity or a service suite like a database. (It is important to note that an instance can contain one or more containers/vms depending on the instance type and configuration).

**Container** Typically a docker container provisioned via a Morpheus Docker host.

**Virtual Machine** A virtualized compute server provisioned onto various hypervisor hosts.

The top of the main Instances page shows overall statistics for the listed Instances, including count, status, and resource utilization. You can search for instances by name, or filter by group, instance type, or category.

**Note:** Instances listed are determined by group access and role permissions.

The Instance list contains important information about each instance, including the instance name, environment tag, instance type icon, ip and port info, instance version, the number of virtual machines or containers in the instance, the group the instance is in, and the cloud or clouds the instance is in.
3.4.1 Creating Instances

The instance catalog is the one stop shop for selecting items to be provisioned and pieced together. It contains not only basic container and vm options but also tailored services for SQL databases, NoSQL databases, cache stores, message busses, web servers, and even full fledged apps. The list contains a lot of items to choose from and they are represented to the user based on what provisioning engines are enabled and integrated in the Morpheus environment.

To get started, simply click the + Add button in the upper right of the Provisioning > Instances section. A modal will display allowing the catalog to be searched. Once an item is selected it is just a matter of following the steps through the wizard.

**Tip:** The instance catalog can be customized via role based access control thereby restricting access to non sanctioned catalog items, as well as added to via the Library section. It is completely customizable.

The next step will ask for a Group and Cloud to be selected. The Group is an abstract representation that can contain multiple cloud integrations. These cloud integrations can also be in multiple groups and is also useful for using role based access control to restrict provisioning access and set retainment policies. If the environment is new and these do not yet exist, it may be advisable to refer to the main section on Getting Started by setting up some cloud integrations and infrastructure first. The wizard continues by allowing us to choose a name for the instance as well as an environment.

**Note:** Currently the Environment option is mostly useful for presenting the user with informative metadata around the instance when coming back to it later.

Moving on, it is now time to configure the Instance. Depending on the option that was chosen and the Instance Configuration that is chosen fields will change. This can include cloud specific fields (i.e. Datastore for VMware or Network). There will also be options like initial username. Some of these fields are optional and will be represented as such.

Configuration options provided in this screen are very powerful. An example is Mysql where a Master/Slave or Master/Master layout can be selected. These configurations will automatically deploy two MySQL VMs or containers and link them together to provide replication. These types of configurations exist for a wide range of instance types and are optimized for high performance and scale. It is even possible to provision entire sharded Mongo clusters.

One last step before the instance can be provisioned is the Automation step. This wizard step may or may not appear depending on the capabilities of the instance type or previous configurations in the account. It is here one can easily select a post provisioning workflow to run (see more on Tasks and Workflows), assign a load balancer, or even configure the backup job that gets created.

Now that the steps are completed for provisioning the selected instance type, simply review your selections and complete. The instance will automatically show up in the instances list and its provisioning state will be represented. Depending on what was provisioned this step can range from seconds to minutes (typically a container configuration will be rather quick if the instance type has previously been provisioned before).
3.4.2 Instance Details

The instance detail page is where you can view and fully manage an instance. To get to an instance detail page, navigate to provisioning, instances, and click on an instance. Please note instance details and actions differ between instance types and user permissions.

There are several sections within an Instance page that provide useful capabilities to the user.

**Summary**  Stats and status information

**Deploy**  Track deployment history for instance types that support deployments or manually kick off a deployment (only visible for instance types that support deployments)

**Settings**  Some instance types support custom configuration settings (i.e. mysql presents the my.ini)

**Network**  Useful for configuring security groups and access to the instance.

**Monitoring**  Quick summary of the monitoring system and all checks that were configured to test the state of the instance

**Backups**  Quick backup dashboard. Useful for viewing historical backups as well as kicking off new ones.

**Logs**  View all aggregated logs from the containers or VM’s representing the instance.

**Environment**  View the environment variables presented to the instances or exported by the instances via Apps (more on this in the Apps section). Even see Imported environment variables that may be referenced by the running instance.

**Scale**  For instances that support load balancing and auto scaling. Easily configure auto scaling thresholds and load balancer settings that pertain to a particular instance. When creating a scale schedule for already-provisioned Instances, a timezone selection is not shown because Morpheus automatically detects the timezone configuration of the web browser.

**Console**  Access the instance or container via a client-less Console supporting SSH, RDP, VNC, and even hypervisor level remote consoles.

3.4.3 Managing Instances

Instance actions allow you to perform numerous management tasks on instances. The actions available depend on the instance type, hypervisor, roles permissions, and instance state.

**Edit**  Edit the Name, Description, Environment, Group, Metadata, Tags, and Owner for the Instance.

**Delete**  Deletes the Instance.

**Important:**  Deleting an Instance will delete the actual VM’s or Containers and cannot be undone, unless a Delayed Removal policy has been applied prior to the Deletion. To delete Instances without deleting associated VM’s, delete the Instances VM record(s) from the Infrastructure section with “Remove Infrastructure” deselected and select “Remove Associated Instances” in the VM delete modal options. This will delete the records in Morpheus but leave the infrastructure in place.

**Tip:**  You can change the owner of an instance easily by selecting the edit button and entering a new owner in the corresponding field.
**Actions**

Available options in the Actions dropdown can include:

**Suspend** Puts the VM in a suspended state without shutting down the OS.

**Stop/Start/Rerstart Service** Stops, Starts or Restarts the service associated with the Instance Type.

**Stop/Start/Rerstart Server** Stops, Starts or Restarts the Virtual Machine.

**Import as Image** Clones and exports VM in its current state to target Storage provider and adds Virtual Image Record with metadata matching the source Instance’s configuration.

**Clone to Image** Clones and converts VM in its current state to image in the source Cloud and adds Virtual Image Record with metadata matching the source Instance’s configuration.

**Lock/Unlock Instance** A locked instance cannot be deleted until it is unlocked.

**Reconfigure** The Reconfigure action allows service plan, disk, cpu, ram, networks and storage controller changes. Available options depend on the instance type and service plan configuration. Some resize actions require an instance restart.

**Clone** Creates a new Instance from the Instance at its current state.

**Backup** Immediately executes a backup of the Instance. Only available for Instances with backups enabled.

**Run Workflow** Presents workflow options and then immediately runs selected Workflow on the Instance. Workflows can be created in the Library > Automation section.

**Run Script** Presents Script options and immediately executes selected Script on the Instance. Scripts can be created in the Library section.

**Apply Template** Presents Template options and immediately applies selected Template to the Instance. Templates can be created in the Library section.

**Add Node** Adds an additional node to the configuration. Additional options and configurations are required in the add node wizard depending on instance configuration and type.

**Eject Disk** Ejects attached disk/iso.

**Add Slave** Adds a database slave in the Instance.

**Change Master** Changes the database Master node in an Instance.

**Clone to Template (VMware)** Creates a new VMware Template from the Instance with corresponding Morpheus Virtual Image record.

**Tip:** Scrolling down in the Actions dropdown may be necessary to see all options.

**Performing Instance Actions**

1. Select the Provisioning link in the navigation bar.
2. Click the Instance from the list of instances you wish to perform an action on.
3. Click the Actions drop down button and select an Action.
Notes

Every Instance has a Wiki section for adding useful information about the Instance. Wiki can be added by selecting the Wiki tab button on the bottom of Instance Detail pages. Instances with associated VMware VM’s will bi-directionally sync Morpheus Instance Wiki content and VMware VM Notes. See the Wiki Section for more details.

Tip: Markdown Syntax is supported in Wikis.

3.5 Apps

Apps allow instances having general relationships to be grouped in a clean and organized manner. App functionality enables full control of which instances belong in an app as well setting Firewall and Access Control List (ACL) rules. Use Apps to structure all necessary components into a single place. Add checks and groups for web servers, database nodes, etc.

Apps can be created from Blueprints, which are made in Library > Blueprints > App Blueprints or from Existing Apps.

3.5.1 Creating Apps from Blueprints

1. Click +ADD on the right side of the main Apps section in Provisioning.
2. Select an existing App Blueprint and click NEXT.

**Note:** App Blueprints must be created in Library > Blueprints > App Blueprints to appear as options when provisioning an App.

3. Enter a Name for the App and select a Group. Default Cloud and Env can also be selected.
4. Click NEXT. Blueprint configurations matching the Group, Cloud and Environment selections will auto-populate the configurations of the Instances in the App. If no Blueprint Configuration matched the Group, Cloud or Env selections, the Instances will have default configurations.
5. Configure your Instances. Depending on the Blueprint Configurations settings, instances may already be fully configured. Fields that are locked in a Blueprint cannot be edited when creating an App.

**Note:** Once an Instance is fully configured, a green checkmark will appear next to the Instance. Instances that have required fields that need populated will have a red X and must be completed. If your Blueprint is already fully configured you can simply select complete!

6. Select COMPLETE and the App will be created and the Instances will begin provisioning.
### 3.5.2 Creating Apps from Existing Instances

1. Click +ADD on the right side of the main Apps section in Provisioning.
2. Select **APP FROM EXISTING INSTANCES** from the Blueprints list and click NEXT.
3. Enter a Name for the App and select a Group. Default Cloud and Env can also be selected.

   **Note:** Only instances within the selected Group and Cloud will be available to be added to the App.

4. In the STRUCTURE section, select + to add a Tier

---

3.5. **Apps**
5. Select or enter a Tier Name.
6. Select the Tier to set Boot Order, rename, or once multiple Tiers are added, connect the Tier to other Tiers.
7. In the STRUCTURE section, select + in a Tier to add an Instance
8. Select the Instance Type of the Existing Instance to be added to the App.
9. In the STRUCTURE section, select the Instance.
10. In the CONFIGURATION section, select the Cloud the Existing Instance is in. Existing INSTANCES that match the Group, Cloud and Instance Types set will populate.
11. Select the desired Instance from the INSTANCES list. Selected instance will show in the SELECTED INSTANCE section.

**Note:** Only one existing Instance can be added per Instance. To add multiple Existing Instances, repeat the step above including adding an Instance for each Existing Instance to be added to the App.

12. Once all Existing Instances have been selected, click **COMPLETE**.
13. A new App will be created out of the Existing Instances.
3.5.3 Exporting Configuration JSON

To export an App Blueprint as JSON:

1. Navigate to Provisioning > Apps
2. Select an App from the list to view the App detail page
3. Click the Actions button and select Export
4. The App export file will be downloaded to your computer as `{app_name}.json`

3.5.4 Provisioning Apps via API

Apps can also be provisioned via Morpheus API and CLI. Links to documentation sites for Morpheus API and CLI are in the main side navigation bar.

3.6 Jobs

Jobs are for scheduled execution of Automation Tasks and Workflows. Jobs can be set to execute on a schedule, at one specific point in time, and/or execute manually (on-demand). Jobs are linked to existing Tasks or Workflows, and allow for custom configuration options. Jobs can be associated with Instances, Servers, or have no association, such as a job for an SSH task.

Jobs allow for scheduled execution of nearly anything as Tasks Types include Bash, Powershell, HTTP/API, Ansible, Chef, Puppet, Groovy, Python, jRuby, Javascript, and library scripts and templates, which can be configured for resource, remote, or local execution targets. If you need something to execute on a schedule, Morpheus Jobs can deliver.

Jobs are configured in the JOBS tab, and the JOB EXECUTIONS tab contains Job execution history with result output.

3.6.1 Jobs

Required Role Permissions Click to Expand/Hide

Provisioning: Jobs

- **None**: Cannot access Provisioning > Jobs > Jobs tab
- **Read**: Can access Provisioning > Jobs > Jobs tab but cannot create, edit, or delete Jobs
- **Full**: Full permissions to create, view, edit, and delete Jobs

Provisioning: Job Executions

- **None**: Cannot access Provisioning > Jobs > Job Executions tab
- **Read**: Can access and view Provisioning > Jobs > Job Executions tab including job execution history, status, and Job output
Creating Jobs

**Note:** Jobs require existing Tasks or Workflows. See the appropriate section of Morpheus docs for more on creating Tasks and Workflows.

To create a new job:

1. Navigate to Provisioning > Jobs
2. Select + ADD
3. Enter the following
   - **NAME:** Name of the Job in Morpheus
   - **JOB TYPE:** A Task Job will execute a selected Task, a Workflow Job will execute a selected Workflow
   - **ENABLED:** When checked, the Job will run as scheduled
4. Select NEXT
5. Configure the Job

**Task Jobs**

**TASK:** Select target Task. If relevant to the Task, Input fields will be presented

**SCHEDULE:**
- Manual: Job is not scheduled but can be executed from Provisioning > Jobs and selecting Actions > Execute
- Date And Time: Job will be executed at one specific point in time and not again (unless rescheduled or executed manually)
- Schedule: Select a configured Execution Schedule. Execution Schedules are created in Library > Automation > Execute Scheduling

**Note:** Morpheus provides two default execution schedules, Daily at Midnight and Weekly on Sunday at Midnight. Any additional schedules were created by a User. Additional schedules can be added in Library > Automation > Execute Scheduling

**CONTEXT TYPE:** Server or Instance

**CONTEXT SERVER/INSTANCE:** Select the Server or Instance you wish to target with the Job

**RUN NOW:** When checked, the Job will execute on save regardless of SCHEDULE setting.

**Workflow Jobs**

**WORKFLOW:** Select target Workflow. If relevant to the Workflow, Input fields will be presented

**SCHEDULE:**
- Manual: Job is not scheduled but can be executed from Provisioning > Jobs and selecting Actions > Execute
- Date And Time: Job will be executed at one specific point in time and not again (unless rescheduled or executed manually)
- Schedule: Select a configured Execution Schedule. Execution Schedules are created in Library > Automation > Execute Scheduling
Note: Morpheus provides two default execution schedules, Daily at Midnight and Weekly on Sunday at Midnight. Additional schedules were created by a User. Additional schedules can be added in Library > Automation > Execute Scheduling.

CONTEXT TYPE: Server or Instance

CONTEXT SERVER/INSTANCE: Select the Server or Instance you wish to target with the Job

RUN NOW: When checked, the Job will execute on save regardless of SCHEDULE setting.

6. Select NEXT

7. Select COMPLETE

Creating and Running Security Scan Jobs

Security Scan Jobs allow users to create and schedule SCAP program (Security Content Automation Program) scans for groups of managed systems. These Jobs can call in existing SCAP packages and checklists, which are used to scan the targeted systems on-demand or on a scheduled basis. Historical data for these scans is saved in the Job Execution list and in the software section of server detail pages. Detailed scan reports can also be viewed for each system as needed once the scan is complete. See the SCAP documentation on the NIST website for information on developing your own scanning procedures.

Note: Creating and editing Security Scan Jobs requires the “Security: Scanning” Role permission set to Full. Viewing Security Scan Jobs and seeing the results for scanned servers requires at least a Read-level permission.

Add a new Security Scan Job

Note: New security scan packages are added in Morpheus Library rather than here in the Jobs section. Ensure you have uploaded the desired security package in Library > Templates > Security Packages before proceeding with new security Job creation.

1. Navigate to Provisioning > Jobs > Jobs Tab

2. Click +ADD

3. Set the Job type to “Security Scan Job” and provide a friendly name for the Job

4. Click NEXT
5. Select a security package, see the previous section to add a new one
6. Enter your Scan Checklist (XML document) and Security Profile (XCCDF document), more information on these can be found in the SCAP documentation linked above
7. Set a schedule or leave as Manual to only run this scan on-demand (new execution schedules can be created in Library > Automation if needed)
8. Set the context, can be Instance or Server. Select as many Instances or Servers as needed for this scanning run
9. Click NEXT
10. After final review, click COMPLETE

Running Security Scan Jobs

Once created, Security Scan Jobs will run based on the configured schedule. They can also be run on-demand when needed:

1. Navigate to Provisioning > Jobs > Jobs Tab
2. Click MORE
3. Click “Execute”
Viewing Completed Security Scan Jobs

To view a list of completed Security Scan Jobs (and Jobs of other types):

1. Navigate to Provisioning > Jobs > Job Executions Tab
2. Additional details can be viewed by clicking (i)

To view scan results for specific servers:

1. Navigate to the server detail page (Infrastructure > Hosts > Virtual Machines tab > Selected server)
2. Click on the Software tab part way down the page, then click on the Security subtab
3. High level details on previous scans is viewable here
4. To view the full report, click (i)

Security Drift

In addition to tracking the scan results over time as described in the previous section, Morpheus also provides detail into the change from the most recent scan to the one prior. This information is displayed in the Software tab (and Security subtab) of the detail page for the virtual machine (accessed from the associated Instance detail page or at Infrastructure > Hosts > Virtual Machines). The information surfaced by this view is listed below. If there is no change, you’ll simply see a “No Drift” message.

- **Title**: The criteria for the test that has newly passed or failed
- **Severity**: The severity level for the indicated security requirement
- **Result**: The indicator for whether this test has newly passed or failed
- **New Pass**: The number of tests that have newly passed compared to the prior scan
- **New Fail**: The number of tests that have newly failed compared to the prior scan
- **Status**: An indicator of the change in security posture since the prior scan. A net gain in test failures will yield a negative status indicator while net gains in passed tests (or no change) will yield a positive status indicator
3.6.2 Job Executions

Required Role Permissions **Click to Expand/Hide**

Access and capabilities for the **Job Executions** section is determined by the following role permissions:

**Role: Feature Access: Provisioning: Job Executions**

- None: Cannot access Provisioning: Job Executions section
- Read: Can access Provisioning: Job Executions section

The Job Executions tab contains execution history of completed Jobs, including any process outputs and error messages. Information included in the Job Executions list includes:

- **Execution Status Icon**
- **Job Name - Task Name - Result Error Message**: The title of each execution includes the Job Name, Task or Workflow name (for Task and Workflow job types), and execution result error messages (when applicable) separated by hyphens (-). The title also links to the Job Execution detail page
- **Start Date**: The date and time the Job Execution kicked off. When expanded, the start date and time of each individual Task are also shown
- **Duration**: The time taken for the Job to complete. When expanded, the time to complete each individual Task is also shown
- **User**: The user who executed or scheduled the Job

Additional details and actions are available per execution:

- Select an execution name to go to the Job Execution Detail page
- Select the icon at the end of the row to expand the execution and view additional details, including task process output
- Select the icon to copy process output to local clipboard
- Select the icon at the end of an expanded to to collapse additional execution details
3.7 Executions

Executions contains the execution status and history from Task and Operational Workflow Executions run from Library > Automation > Tasks and Library > Automation > Workflows. Executions for Tasks and Workflows are split out to their own labeled tabs.

Note: Tasks and Workflows executed from a Job or from Instance or Host Actions do not populate in the Executions Section, and can be referenced from the History tab on the target resource. All task and Workflow executions can be referenced in Operations > Activity > History

Execution results in the ui display:

<table>
<thead>
<tr>
<th>NAME</th>
<th>Name of the Task or Workflow Executed</th>
</tr>
</thead>
<tbody>
<tr>
<td>TYPE</td>
<td>Type of execution (Task or Workflow)</td>
</tr>
<tr>
<td>START DATE</td>
<td>Date and time of execution</td>
</tr>
<tr>
<td>ETA/DURATION</td>
<td>Estimate time of completion for executions in progress, or the total execution time for completed executions.</td>
</tr>
<tr>
<td>RESULTS</td>
<td>Result status of execution (Succeeded, Failed, In-Progress or Pending)</td>
</tr>
</tbody>
</table>

Execution Detail (i) Click on the \( i \) to view process output results

Note: Job and automation executions can be expanded to show process details by clicking on the arrow icon immediately to the right of the NAME column.

3.8 Code

Note: In v5.3.2+, provisioning/deployments is moved to provisioning/code.

Provisioning > Code contains the Repositories, Deployments and Code Integrations sections.

Required Role Permissions Click to Expand/Hide

Access and capabilities for the Code section is determined by the following role permissions:

Role: Feature Access: Infrastructure: Groups

- None: Cannot access Provisioning: Code section
- Read or Full: Can access Provisioning: Code section

Role: Feature Access: Provisioning: Code Repositories

- None: Cannot access Provisioning: Code Repositories
- List Files: Can browse repo folder and file names, select branch, refresh Repositories. Cannot access/view file contents.
- Read or Full: Can browse repo folder and file names, select branch, refresh Repositories and access/view file contents.

Role: Feature Access: Provisioning: Code Deployments
• None: Cannot access Provisioning: Code Deployments.
• Read: Can view Code Deployments. Cannot create, delete or edit Code Deployments.
• Full: Can create, delete and edit Code Deployments.

**Role: Feature Access: Provisioning: Code Integrations**
• None: Cannot access Provisioning: Code Integrations.
• Read: Can view Code Integrations. Cannot create, delete or edit Code Integrations.
• Full: Can create, delete and edit Code Integrations

### 3.8.1 Repositories

The *Provisioning → Code → Repositories* section contains the repositories integrated with Morpheus allowing users to browse repository folders and files, view file contents from any branch, trigger a refresh, and create tasks, scripts and templates directly from the repos.

• Browse integrated repositories
• View repo files
• Switch branches
• Trigger repo refreshes
• Filter by Integration, Organization or Text search
• Create Custom Views
• Create Tasks from repo files
• Create Spec Templates from repo files

**Role Permissions**

Access and capabilities for the **Repositories** section is determined by the following role permissions:

**Role: Feature Access: Infrastructure: Groups**
• None: Cannot access Provisioning: Code section
• Read or Full: Can access Provisioning: Code section

**Role: Feature Access: Administration: Users**
• None: Can view repo list but cannot browse repo folder and file names, select branch, refresh repositories or access/view file contents
• Read or Full: Can view repo list, browse repo folder and file names, select branch, refresh repositories. Cannot access/view file contents without Read or Full level permission on **Provisioning: Code Repositories**

**Role: Feature Access: Provisioning: Code Repositories**
• None: Cannot access Provisioning: Code Repositories
• List Files: Can browse repo folder and file names, select branch, refresh Repositories. Cannot access/view file contents
• Read or Full: Can browse repo folder and file names, select branch, refresh Repositories and access/view file contents

Role: Feature Access: **Provisioning:**  Tasks

• None: Cannot create Tasks from repo files in repository browser
• Read or Full: Can create Tasks from repo files in repository browser

Role: Feature Access: **Provisioning:**  Library

• None: Cannot create Spec Templates from files in repository browser
• Read or Full: Can create Spec Templates from files in repository browser

**List Repositories**

1. Select the **Provisioning** link in the navigation bar
2. Select the **Code** link in the sub-navigation bar
3. Users with sufficient permissions will see a list view of all integrated code repositories
4. Use the Search, Integrations or Organizations filter to filter listed repositories

**Tip:** Select the gear icon in the top right of the repos list view to create and save custom list views.

**Refresh Repository**

1. Select the **Provisioning** link in the navigation bar
2. Select the **Code** link in the sub-navigation bar
3. Select name of target repository
4. Select **ACTIONS > Refresh**

**Browse Repositories**

1. Select the **Provisioning** link in the navigation bar
2. Select the **Code** link in the sub-navigation bar
3. Select name of target repository
4. Users with sufficient permissions can browse repo folder and file names, select branches, and refresh repositories. Users can access/view file contents with Read or Full level permission on **Provisioning: Code Repositories**
5. Select target folder icon to drill into the folder
**View Repository File**

1. Select the **Provisioning** link in the navigation bar
2. Select the **Code** link in the sub-navigation bar
3. Select name of target repository
4. Select icon to right of target file name

**Note:** Users can access/view file contents only with Read or Full level permission on **Provisioning: Code Repositories**. File contents displayed is from last repo sync. Refresh repo to ensure current version for recent commits.

**Create Task from Repository File**

1. Select the **Provisioning** link in the navigation bar
2. Select the **Code** link in the sub-navigation bar
3. Select name of target repository
4. Select gear icon to right of compatible target file name
5. Select target task type from available actions
6. Complete the NEW TASK wizard to create a new Task. The TYPE, SOURCE, REPOSITORY and FILE PATH fields will be automatically configured

**Note:** Shell and Powershell Tasks types can be created from the code repo browser in v5.3.4. Ensure file compatibility with target Task type.

**Note:** Users can create tasks from Repositories only with Read or Full level permission on **Library: Tasks**.

**Create Spec Template from Repository File**

1. Select the **Provisioning** link in the navigation bar
2. Select the **Code** link in the sub-navigation bar
3. Select name of target repository
4. Select gear icon to right of target file name
5. Select target spec template type from available actions
6. Complete the NEW SPEC TEMPLATE wizard to create a new Spec Template. The TYPE, SOURCE, REPOSITORY and FILE PATH fields will be automatically configured

**Note:** Terraform spec template types can be created from the code repo browser in v5.3.4. Other spec template types can be created from repo files by changing the TYPE field in the NEW SPEC TEMPLATE wizard.
3.8.2 Deployments

Note: In v5.3.2+, Provisioning → Deployments has been moved to Provisioning → Code → Deployments

The deployments section provides very useful PaaS like capabilities when it comes to deploying applications into the newly provisioned environment. These can be uploaded directly from the UI, pulled from a build server, pulled from a public or private Git repository or even via the API and the various plugins created, such as Jenkins, and Gradle to support continuous build / integration workflows.

A deployment can be considered a set of versions that relate to a particular project or application being deployed. This allows one to keep track of a history of versions and easily reuse these deployment versions across instances that may exist in different environments. An example might be to deploy a version from a deployment to a staging instance and (once approved) also deployed into production.

Role Permissions

Access and capabilities for the Deployments section is determined by the following role permissions:

- **Role: Feature Access: Infrastructure:** Groups
  - None: Cannot access Provisioning: Code section
  - Read or Full: Can access Provisioning: Code section

- **Role: Feature Access: Provisioning:** Code Deployments
  - None: Cannot access Provisioning: Code Deployments.
  - Read: Can view Code Deployments. Cannot create, delete or edit Code Deployments.
  - Full: Can create, delete and edit Code Deployments.

Getting Started

Getting started with deployments is easy. They can vary slightly for the application stack being deployed but the simplest phase of a deployment is adding a version and adding the appropriate files to the deployment archive that are needed for the application to run. This could be a single file like a WAR file for Tomcat, or it could be hundreds of files for stacks like Ruby on Rails.

There are a few ways to create a deployment. The first is to use the Provisioning → Code → Deployments section of the application to create them. Simply add a new deployment and give it a name representing the application that is being deployed. Once a deployment is created select the deployment to view its versions (which will be empty to start). Next, it is time to add a version.

When adding a version there are several options. There are 3 types represented by the UI. These include File, Fetch, and Git respectively. A File deployment allows the user to simply drag their files into the file explorer presented by the dialog. This file explorer can take single files or entire file trees (If files exist in subfolders then only the Chrome browser is supported due to browser limitations at the time of this writing). This is also the common type that is represented when files are uploaded via the CLI, or available build tool integration plugins. Once the files have completed their upload simply save the version for use.
Git

For performing git based deploys Morpheus supports both public and private repositories. To utilize a private git repository the add version dialog will display a public keypair that can be added to the git service for authentication purposes. Currently this keypair is shared across the account and not specifically scoped to the user so it may be advisable to connect this integration to a deployment account in git. From here either a ssh or https git url can be entered along with a git branch or tag name. Once the version is saved, this repository will be copied down into the deployment archive for use.

Fetch

Fetch based deployments are pretty straightforward. Simply enter a url to a file representing the deployment. This can be a single file (in which case it will just be added to the deployment archive singularly) or it can be a zip file (which will automatically be expanded into the archive). HTTP Authentication options can also be entered if the url requires some form of basic authentication scheme for access by the appliance.

Deploying to an Instance

Now that a version has been added to a deployment, it is easy to push that deployment out to any instance provisioned within Morpheus by navigating to the specific Instance that it needs deployed to. On the Instance detail page there is a tab called Deploy. From here simply add a deploy. The dialog will ask firstly from which deployment the deploy is from (or allow you to create a new one on the spot), and secondly which version to deploy (also with the option to add one on the fly). The next step of the wizard will display any configuration options that might be specific to the instance type being deployed to (i.e. CATALINA_OPTS for Tomcat or Java Command for java) as well as the file explorer and deployment type selections for review (or use when creating a new version on the fly). Fill in the required items then simply hit complete. The deploy will now be asynchronously sent off to all of the virtual machines or containers within the instance in a rolling restart and the deployment status will be represented.

Tip: When deploying to an instance, the custom configuration options that were entered during the previous deployment are automatically carried forward allowing one to edit them or leave them as is.

Rolling Backwards and Forwards

Because of the tracked history of deployments kept within Morpheus, the deploy tab of instance detail makes it easy to choose a previously run deployment and jump back to it in the event of a failed deployment. The history will automatically be updated and the configuration, as well as data from the previous deployment state of the instance will be restored.

Offloading Storage

Since a full history of the backup builds are kept in Morpheus, as the appliance grows it becomes necessary to change where these are stored. On a fresh install these are stored on the local appliance in /var/opt/morpheus or wherever the master account may have changed the configuration to point to. It is also possible to adjust the deployment archive store by creating a Storage Provider tied to an S3 compatible object store, Openstack Swift object store, or any other type of mountpoint provided. This option can be adjusted in Administration → Settings → Provisioning once a storage provider is created within the account.
Add Deployment

1. Select the Provisioning link in the navigation bar.
2. Select the Code link in the sub-navigation bar.
3. Select the Deployments tab.
4. Click the + Add button.
5. Enter a Name for the deployment and a description (optional)
6. Click the Save Changes button to save.

Add Version

1. Select the Provisioning link in the navigation bar.
2. Select the Code link in the sub-navigation bar.
3. Select the Deployments tab.
4. Click the Name of the deployment you would like to add a version to.
5. Click the Add Version button.
6. From the Add Version Wizard select the deployment type.
7. Input the Version of the deployment.
8. Depending on the type of deployment selected perform one of the following:
   - **Files** Drag files into the file explorer presented by the dialog. This file explorer can take single files or entire file trees.
   - **Fetch** Enter a url to a file representing the deployment.
   - **Git** The add version dialog will display a public key pair that can be added to the git service for authentication purposes. Either a ssh or https git url can be entered along with a git branch or tag name.
9. Click the Save Changes button to save.

Edit Deployment

1. Select the Provisioning link in the navigation bar.
2. Select the Code link in the sub-navigation bar.
3. Select the Deployments tab.
4. Click the icon on the row of the deployment you wish to edit, or click the Name of the deployment and then the Edit button from the deployment detail page.
5. Modify information as needed
6. Click the Save Changes button to save.
Delete Deployment

1. Select the Provisioning link in the navigation bar.
2. Select the Code link in the sub-navigation bar.
3. Select the Deployments tab.
4. Click the icon on the row of the deployment you wish to delete, or click the Name of the deployment and then the DELETE button.

3.8.3 Code Integrations

The Provisioning → Code → Integrations section is where Code Integrations, such as Git and Github Repository Integrations, and Jenkins Build Service Integrations, can be created and managed.

Role Permissions

Access and capabilities for the Integrations section is determined by the following role permissions:

Role: Feature Access: Infrastructure: Groups
- None: Cannot access Provisioning: Code section
- Read or Full: Can access Provisioning: Code section

Role: Feature Access: Provisioning: Code Integrations
- None: Cannot access Provisioning: Code Integrations.
- Read: Can view Code Integrations. Cannot create, delete or edit Code Integrations.
- Full: Can create, delete and edit Code Integrations
4.1 Automation

The Automation section is composed of Tasks and Workflows. Tasks can be scripts added directly, scripts and blueprints from the Library section, recipes, playbooks, salt states, puppet agent installs, or http (api) calls. These tasks are combined into workflows, which can be selected to run at provision time or executed on existing instances via Actions > Run Workflow.

4.1.1 Tasks

Overview

There are many Task Types available, including scripts added directly, scripts and templates from the Library section, recipes, playbooks, salt states, puppet agent installs, and http (api) calls. Tasks are primarily created for use in Workflows, but a single Task can be executed on an existing instance via Actions > Run Task.

Role Permissions

The User Role Permission ‘Provisioning: Tasks FULL’ is required to create, edit and delete tasks.

Tasks Types that can execute locally against the Morpheus Appliance have an additional Role Permission: Tasks - Script Engines. Script Engine Task Types will be hidden for users without Tasks - Script Engines role permissions.

Common Options

When creating a Task, the required and optional inputs will vary significantly by the Task type. However, there are options which are common to Tasks of all types.
Target Options

When creating a Task, users can select a target to perform the execution. Some Task types allow for any of the three execution targets listed below and some will limit the user to two or just one. The table in the next section lists the available execution targets for each Task type.

- **Resource**: An Morpheus-managed Instance or server is selected to execute the Task
- **Local**: The Task is executed by the Morpheus appliance node
- **Remote**: The user specifies a remote box which will execute the Task

Execute Options

- **Retryable**: When marked, this Task can be configured to be retried in the event of failure
- **Retry Count**: The maximum number of times the Task will be retried when there is a failure
- **Retry Delay**: The length of time (in seconds) Morpheus will wait to retry the Task
- **Allow Custom Config**: When marked, a text area is provided at Task execution time to allow the user to pass extra variables or specify extra configuration
## Task Types

Table 1: Available Task Types

<table>
<thead>
<tr>
<th>Task Type</th>
<th>Task Description</th>
<th>Source Options</th>
<th>Execute Target Options</th>
<th>Configuration Requirements</th>
<th>Role Permissions Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ansible</td>
<td>Runs an Ansible playbook. Ansible Integration required</td>
<td>An-</td>
<td>Local, Re-</td>
<td>Existing Ansible Integration</td>
<td>Provisioning: Tasks</td>
</tr>
<tr>
<td>Tower</td>
<td>Relays Ansible calls to Ansible Tower</td>
<td>Ansible</td>
<td>An-</td>
<td>All, Re-</td>
<td>Existing Ansible Integration</td>
</tr>
<tr>
<td>Chef</td>
<td>Executes Chef bootstrap and run list. Chef Integration required</td>
<td>Chef</td>
<td>Chef Re-</td>
<td>Existing Chef Integration</td>
<td>Provisioning: Tasks</td>
</tr>
<tr>
<td>Email</td>
<td>Send an email from a Workflow</td>
<td>Task</td>
<td>Task Content</td>
<td>SMTP Configured</td>
<td>Provisioning: Tasks</td>
</tr>
<tr>
<td>Groovy script</td>
<td>Executes Groovy Script locally (on Morpheus app node)</td>
<td>Local,</td>
<td>Local</td>
<td>None</td>
<td>Provisioning: Tasks</td>
</tr>
<tr>
<td>Javascript</td>
<td>Executes Javascript locally (on Morpheus app node)</td>
<td>Local,</td>
<td>Local</td>
<td>None</td>
<td>Provisioning: Tasks</td>
</tr>
<tr>
<td>jRuby Script</td>
<td>Executes Ruby script locally (on Morpheus app node)</td>
<td>Local,</td>
<td>Local</td>
<td>None</td>
<td>Provisioning: Tasks</td>
</tr>
<tr>
<td>Library Script</td>
<td>Creates a Task from an existing Library Script</td>
<td>Library</td>
<td>Library Script</td>
<td>Existing Library Script</td>
<td>Provisioning: Tasks</td>
</tr>
<tr>
<td>Library Template</td>
<td>Creates a Task from an existing Library Template</td>
<td>Library</td>
<td>Library Template</td>
<td>Existing Library Templates</td>
<td>Provisioning: Tasks</td>
</tr>
<tr>
<td>PowerShell Script</td>
<td>Execute PowerShell Script on the Target Resource</td>
<td>Local,</td>
<td>Remote, Re-</td>
<td>None</td>
<td>Provisioning: Tasks</td>
</tr>
<tr>
<td>Puppet Agent Install</td>
<td>Executes Puppet Agent bootstrap, writes puppet.conf and triggers agent checkin. Puppet Integration required</td>
<td>Local,</td>
<td>Local</td>
<td>None</td>
<td>Provisioning: Tasks</td>
</tr>
<tr>
<td>Library Script</td>
<td>Creates a Task from an existing Library Script</td>
<td>Library</td>
<td>Library Script</td>
<td>Existing Library Script</td>
<td>Provisioning: Tasks</td>
</tr>
<tr>
<td>Library Template</td>
<td>Creates a Task from an existing Library Template</td>
<td>Library</td>
<td>Library Template</td>
<td>Existing Library Templates</td>
<td>Provisioning: Tasks</td>
</tr>
<tr>
<td>Python Script</td>
<td>Executes Python Script locally</td>
<td>Local,</td>
<td>Local</td>
<td>None</td>
<td>Provisioning: Tasks</td>
</tr>
<tr>
<td>Restart</td>
<td>Restarts target VM/Host/Container</td>
<td>System</td>
<td>Re-</td>
<td>None</td>
<td>Provisioning: Tasks</td>
</tr>
</tbody>
</table>
Task Configuration

- **Ansible Playbook**

  - **NAME**: Name of the Task
  - **CODE**: Unique code name for API, CLI, and variable references
  - **ANSIBLE REPO**: Select existing Ansible Integration
  - **GIT REF**: Specify tag or branch (Option, blank assumes default)
  - **PLAYBOOK**: Name of playbook to execute, both playbook and playbook.yml format supported
  - **TAGS**: Enter comma separated tags to filter executed tasks by (ie --tags)
  - **SKIP TAGS**: Enter comma separated tags to run the playbook without matching tagged tasks (ie --skip-tags)

  **Important**: Using different Git Refs for multiple Ansible Tasks in same Workflow is not supported. Git Refs can vary between Workflows, but Tasks in each Workflow must use the same Git Ref.

- **Chef bootstrap**

  - **NAME**: Name of the Task
  - **CODE**: Unique code name for API, CLI, and variable references
  - **CHEF SERVER**: Select existing Chef integration
  - **ENVIRONMENT**: Populate Chef environment, or leave as _default
  - **RUN LIST**: Enter Run List, eg role[web]
  - **DATA BAG KEY**: Enter data bag key (will be masked upon save)
  - **DATA BAG KEY PATH**: Enter data bag key path, eg /etc/chef/databag_secret
  - **NODE NAME**: Defaults to Instance name, configurable
  - **NODE ATTRIBUTES**: Specify attributes inside the {}  

- **Groovy script**

  - **NAME**: Name of the Task
  - **CODE**: Unique code name for API, CLI, and variable references
  - **RESULT TYPE**: Single Value, Key/Value Pairs, or JSON
  - **CONTENT**: Contents of the Groovy script if not sourcing it from a repository
• Email

**Email**

- **NAME:** Name of the Task
- **CODE:** Unique code name for API, CLI, and variable references
- **SOURCE:** Choose local to draft or paste the email directly into the Task. Choose Repository or URL to bring in a template from a Git repository or another outside source
- **EMAIL ADDRESS:** Email addresses can be entered literally or Morpheus automation variables can be injected, such as `<%=instance.createdByEmail%>`
- **SUBJECT:** The subject line of the email, Morpheus automation variables can be injected into the subject field
- **CONTENT:** The body of the email is HTML. Morpheus automation variables can be injected into the email body when needed
- **SKIP WRAPPED EMAIL TEMPLATE:** The Morpheus-styled email template is ignored and only HTML in the Content field is used

**Tip:** To whitelabel email sent from Tasks, select **SKIP WRAPPED EMAIL TEMPLATE** and use an HTML template with your own CSS styling

• HTTP (API)

**HTTP**

- **NAME:** Name of the Task
- **CODE:** Unique code name for API, CLI, and variable references
- **RESULT TYPE:** Single Value, Key/Value Pairs, or JSON
- **URL:** An HTTP or HTTPS URL as the HTTP Task target
- **HTTP METHOD:** GET (default), POST, PUT, PATCH, HEAD, or DELETE
- **AUTH USER:** Username for username/password authentication
- **PASSWORD:** Password for username/password authentication
- **BODY:** Request Body
- **HTTP HEADERS:** Enter requests headers, examples below:

<table>
<thead>
<tr>
<th>Authorization</th>
<th>Bearer token</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content-Type</td>
<td>application/json</td>
</tr>
</tbody>
</table>

- **IGNORE SSL ERRORS:** Mark when making REST calls to systems without a trusted SSL certificate

• Javascript

**JavaScript**

- **NAME:** Name of the Task
Morpheus Documentation

- **CODE**: Unique code name for API, CLI, and variable references
- **RESULT TYPE**: Single Value, Key/Value Pairs, or JSON
- **SCRIPT**: Javascript contents to execute

• **jRuby Script**

![Ruby]

- **NAME**: Name of the Task
- **CODE**: Unique code name for API, CLI, and variable references
- **RESULT TYPE**: Single Value, Key/Value Pairs, or JSON
- **CONTENT**: Contents of the jRuby script is entered here if it’s not being called in from an outside source

• **Library Script**

![Library Script]

- **NAME**: Name of the Task
- **CODE**: Unique code name for API, CLI, and variable references
- **RESULT TYPE**: Single Value, Key/Value Pairs, or JSON
- **SCRIPT**: Search for an existing script in the typeahead field

• **Library Template**

![Library Template]

- **NAME**: Name of the Task
- **CODE**: Unique code name for API, CLI, and variable references
- **TEMPLATE**: Search for an existing template in the typeahead field

• **Powershell Script**

![Powershell]

- **NAME**: Name of the Task
- **CODE**: Unique code name for API, CLI, and variable references
- **RESULT TYPE**: Single Value, Key/Value Pairs, or JSON
- **ELEVATED SHELL**: Run script with administrator privileges
- **IP ADDRESS**: IP address of the PowerShell Task target
- **PORT**: SSH port for PowerShell Task target (5985 default)
- **USERNAME**: Username for PowerShell Task target
- **PASSWORD**: Password for PowerShell Task target
- **Content**: Enter script to execute if not calling the script in from an outside source
• Puppet Agent Install

  – NAME: Name of the Task
  – CODE: Unique code name for API, CLI, and variable references
  – PUPPET MASTER: Select Puppet Master from an existing Puppet integration
  – PUPPET NODE NAME: Enter Puppet node name. Variables supported eg. `<%= instance.name %>`
  – PUPPET ENVIRONMENT: Enter Puppet environment, eg. `production`

• Python Script

  Important: Beginning with Morpheus version 4.2.1, Python Tasks use virtual environments. For this reason, `virtualenv` must be installed on your appliances in order to work with Python Tasks. See the information below for more detailed steps to install `virtualenv` on your Morpheus appliance node(s).

  – NAME: Name of the Task
  – CODE: Unique code name for API, CLI, and variable references
  – RESULT TYPE: Single Value, Key/Value Pairs, or JSON
  – CONTENT: Python script to execute is entered here if not pulled in from an outside repository
  – COMMAND ARGUMENTS: Optional arguments passed into the Python script. Variables supported eg. `<%= instance.name %>`
  – ADDITIONAL PACKAGES: Additional packages to be installed after `requirements.txt` (if detected). Expected format for additional packages: `'packageName==x.x.x packageName2==x.x.x'`, the version must be specified
  – PYTHON BINARY: Optional binary to override the default Python binary

Python and Morpheus

Enterprise Proxy Considerations

Additional considerations must be made in enterprise proxy environments where Python Tasks are run with additional package download requirements. These additional packages are downloaded using `pip` and may not obey global Morpheus proxy rules. To deal with this, create or edit the pip configuration file at `/etc/pip.conf`. Your configuration should include something like the following:

```
[globals]
proxy = http://some-proxy-ip.com:8087
```

For more information, review the Pip documentation on using proxy servers here.

CentOS 7 / Python 2.7 (RHEL system Python)
With a fresh install of Morpheus on a default build of CentOS 7, Python Tasks will not function due to the missing requirement of `virtualenv`.

If you attempt to run a python task, you will get an error similar to the following:

```
Task Execution Failed on Attempt 1
sudo: /tmp/py-8ae51ebf-749c-4354-b6e4-11ce541afad5/bin/python: command not found
```

In order to run Morpheus Python Tasks in CentOS 7, install `virtualenv`:

```
yum install python-virtualenv
```

If you require `python3`, you can specify the binary to be used while building the virtual environment. In a default install, do the following: `yum install python3`. Then, in your Morpheus Python Task, specify the binary in the PYTHON BINARY field as “/bin/python3”. This will build a virtual environment in /tmp using the python3 binary, which is equivalent to making a virtual environment like so: `virtualenv ~/venv -p /bin/python3`.

If you wish to install additional Python packages into the virtual environment, put them in pip format and space-separated into the ADDITIONAL PACKAGES field on the Python Task. Use the help text below the field to ensure correct formatting.

**CentOS 8 and Python**

In CentOS 8, Python is not installed by default. There is a platform-python but that should not be used for anything in userland. The error message with a default install of CentOS 8 will be similar to this:

```
Task Execution Failed on Attempt 1
sudo: /tmp/py-cffc9a8f-c40d-451d-956e-d6e9185ade33/bin/python: command not found
```

The default virtualenv for CentOS 8 is the python3 variety, for Morpheus to use Python Tasks, do the following: `yum install python3-virtualenv`.

If Python2 is required, do the following: `yum install python2` and specify `/bin/python2` as the PYTHON BINARY in your Morpheus Task.

This will build a virtualenv in /tmp using the python2 binary, which is equivalent to making a virtualenv like so: `virtualenv ~/venv -p /bin/python2`.

If you wish to install additional Python packages into the virtual environment, put them in pip format and space-separated into the ADDITIONAL PACKAGES field on the Python Task. Use the help text below the field to ensure correct formatting.

- **Restart**

  - **NAME**: Name of the Task
  - **CODE**: Unique code name for API, CLI, and variable references

- **Shell Script**

  - **NAME**: Name of the Task
  - **CODE**: Unique code name for API, CLI, and variable references
  - **RESULT TYPE**: Single Value, Key/Value Pairs, or JSON
  - **SUDO**: Mark the box to run the script as `sudo`
- **CONTENT:** Script to execute is entered here if not pulled in from an outside repository

- **vRealize Orchestrator Workflow**

  - **NAME:** Name of the Task
  - **CODE:** Unique code name for API, CLI, and variable references
  - **RESULT TYPE:** Single Value, Key/Value Pairs, or JSON
  - **vRO INTEGRATION:** Select an existing vRO integration
  - **WORKFLOW:** Select a vRO workflow from the list synced from the selected integration
  - **PARAMETER BODY (JSON):**

**Task Management**

**Adding Tasks**

1. Select the Provisioning link in the navigation bar.
2. Select Automation from the sub-navigation menu.
3. Click the Add button.
4. From the New Task Wizard input a name for the task.
5. Select the type of task from from the type dropdown.
6. Input the appropriate details dependent on the task type you selected from the dropdown.
7. Save

**Editing Tasks**

1. Select the Provisioning link in the navigation bar.
2. Select Automation from the sub-navigation menu.
3. Click the Edit icon on the row of the task you wish to edit.
4. Modify information as needed.
5. Click the Save Changes button to save.

**Deleting Tasks**

1. Select the Provisioning link in the navigation bar.
2. Select Automation from the sub-navigation menu.
3. Click the Delete icon on the row of the task you wish to delete.
Task Results

Overview

Using Task results, the output from any preceding Tasks within the same Workflow phase is available to be called into additional Tasks. The results are stored on the `results` variable. Since results are available to all Tasks, we can use results from any or all prior Tasks so long as they are executed within the same provision phase.

In script type tasks, if a RESULT TYPE is set, Morpheus will store the output on the `results` variable. It’s important to understand that the result type indicates the format of the Task output Morpheus should expect. Morpheus will parse that output into a Groovy map which can be retrieved and further parsed by resolving the `results` variable. If the RESULT TYPE is incorrectly set, Morpheus may not be able to store the Task results correctly. Jump to the section on Script Config Examples to see how script results are processed in various example cases.

Results Types

- **Single Value** Entire task output is stored in `<%=results.taskCode%>` or `<%=results["Task Name"]%>` variable.

- **Key/Value pairs** Expects `key=value,key=value` output. Entire task output is available with `<%=results.taskCode%>` or `<%=results["Task Name"]%>` variable (output inside []). Individual Values are available with `<%=results.taskCode.key%>` variables.

- **JSON** Expects `key:value,key:value` json formatted output. Entire task output is available with `<%=results.taskCode%>` or `<%=results["Task Name"]%>` variable (output inside []). Individual Values are available with `<%=results.taskCode.key%>` variables.

**Important:** The entire output of a script is treated as results, not just the last line. Ensure formatting is correct for the appropriate result type. For example, if Results Type is `json` and the output is not fully json compatible, the result would not return properly.

**Important:** Task results are not supported for Library Script task types

Script Config Examples

**Single Value using Task Code**

**Source Task Config**

- NAME: Var Code (single)
- CODE: singleExample
- RESULT TYPE: Single Value
- SCRIPT: echo "string value"

**Source Task Output:** string value

**Results Task Config (using task code in variable)**

- NAME: N/A
- CODE: N/A
• RESULT TYPE: N/A
• SCRIPT: echo "single: <%=results.singleExample%>"

Results Task Output: single: string value

Single Value using Task Name

Source Task Config
- NAME: Var Code
- CODE: none
- RESULT TYPE: Single Value
- SCRIPT: echo "string value"

Source Task Output: string value

Results Task using task name in variable

Results Task Script: echo "task name: <%=results["Var Code"]%>">
Results Task Output: task name: test value

Key/Value Pairs

Source Task Config
- NAME: Var Code (keyval)
- CODE: keyvalExample
- RESULT TYPE: Key/Value pairs
- SCRIPT: echo "flash=bang, ping=pong"

Source Task Output: flash=bang, ping=pong

Results Task for all results

Results Task Script: echo "keyval: <%=results.keyvalExample%>"
Results Task Output: keyval: [flash=bang, ping=pong]

Results Task for a single value

Results Task Script: echo "keyval value: <%=results.keyvalExample.flash%>"
Results Task Output: keyval value: bang

JSON

Source Task Config
- NAME: Var Code (json)
- CODE: jsonExample
- RESULT TYPE: JSON
- SCRIPT: echo "{"ping":"pong","flash":"bang"}"

Source Task Output: {"ping":"pong","flash":"bang"}

Results Task for all results

Results Task Script: echo "json: <%=results.jsonExample%>"
Results Task Output  json:  [ping:pong, flash:bang]

Results Task for a single value

Results Task Script  
```bash
echo "json value: <%=results.jsonExample.ping%>"
```

Results Task Output  json value:  pong

Multiple Task Results

Results Task Script
```bash
echo "single: <%=results.singleExample%>"
echo "task name: <%=results["Var Code"]%>"
echo "keyval: <%=results.keyvalExample%>"
echo "keyval value: <%=results.keyval.flash%>"
echo "json: <%=results.jsonExample%>"
echo "json value: <%=results.jsonExample.ping%>"
```

Results Task Output
```plaintext
single: string value
task name: string value
keyval: [flash:bang, ping:pong]
keyval value: bang
json: [ping:pong, flash:bang]
json value: pong
```

Workflow Config

Add one or multiple tasks with Results Type configured to a workflow, and the results will be available to all tasks in the same phase of the workflow via the `<%=results.variables%>` during the workflow execution.

- Task Results are only available to tasks in the same workflow phase
- Task Results are only available during workflow execution

4.1.2 Workflows

Workflows are groups of Tasks, which are described in detail in the preceding section. Operational Workflows can be run on-demand against an existing Instance or server from the Actions menu on the Instance or server detail page. Additionally, they can be scheduled to run on a recurring basis through Morpheus Jobs (Provisioning > Jobs).

Provisioning Workflows are associated with Instances at provision time (in the Automation tab of the Add Instance wizard) or after provisioning through the Actions menu on the Instance detail page. Provisioning Workflows assign Tasks to various stages of the Instance lifecycle, such as Provision, Post Provision, and Teardown. When the Instance reaches a given stage, the appropriate Tasks are run. Task results and output can be viewed from the History tab of the Instance or server detail page.
## Provisioning Workflow Execution Phases

<table>
<thead>
<tr>
<th>Phase</th>
<th>Description</th>
<th>Usage Example</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
<td>Tasks are run prior to initial calls to the specified cloud API to initiate provisioning</td>
<td>Call to an external platform to dynamically generate a hostname prior to kicking off provisioning</td>
<td>Pre Provision can be used for a Blueprint so it is added before a script which is set at the Provision phase executes. Pre Provision for scripts is mainly for Docker as you can execute on the host before the container is running.</td>
</tr>
<tr>
<td>Pre Provision</td>
<td>For VMs, Tasks are run after the VM is running and prior to any Tasks in the Provision phase. For containers, Tasks in this phase are run on the Docker host and prior to <code>docker run</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provision</td>
<td>Like pre-provision, Tasks for VMs are run after the VM is running. For containers, these Tasks are run after the containers are running on the host. For many users, this is the most commonly-used phase.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Post Provision</td>
<td>Tasks are run after the entire provisioning process has completed</td>
<td>When adding a node to an Instance, Tasks in this phase will be run on all nodes in the Instance after the new node is provisioned. This is because Post Provision operations may need to affect all nodes, such as when joining a new node to a cluster. Tasks in Pre Provision and Provision phases would only be run on the new node in this scenario.</td>
<td></td>
</tr>
<tr>
<td>Start Service</td>
<td>Tasks in this phase are run when choosing start service from an Instance detail page. This action starts the service associated with the Instance type</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stop Service</td>
<td>Tasks in this phase are run when choosing stop service from an Instance detail page. This action stops the service associated with the Instance type</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pre Deploy</td>
<td>Tasks in this phase are run when a new deploy is triggered from the Deploy tab of the Instance detail page, prior to the deploy taking place</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deploy</td>
<td>Tasks in this phase are run when a new deploy is triggered from the Deploy tab of the Instance detail page, after the deploy has completed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reconfigure</td>
<td>Tasks in this phase are run when the reconfigure action is made against an Instance or host</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tear-down</td>
<td>Tasks are run during VM or container destroy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shutdown</td>
<td>Tasks are run immediately before the target is shutdown</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Add Workflow

1. Select the Provisioning link in the navigation bar
2. Select Automation from the sub-navigation menu
3. Click the Workflows tab to show the Workflows tab panel
4. Click the + Add dropdown and select a Workflow type (Operational or Provisioning, see the section above for more on Workflow type differences)
5. From the New Workflow Wizard input a name for the workflow
6. Optionally input a description and a target platform
7. Add Tasks and Inputs using the typeahead fields, Tasks must be added to the appropriate phases for Provisioning Workflows
8. If multiple tasks are added to the same execution phase, their execution order can be changed by selecting the grip icon and dragging the task to the desired execution order
9. For multi-Tenant environments, select Public or Private visibility for the Workflow
10. For Operational Workflows, optionally mark “Allow Custom Config” from the Advanced Options section if needed. See the next section for more on this selection
11. Click the SAVE CHANGES button to save

Note: When setting Workflow visibility to Public in a multi-Tenant environment, Tenants will be able to see the Workflow and also execute it directly from the Workflows list (if it’s an Operational Workflow). They will not be able to edit or delete the Workflow.

Allow Custom Config

When marked on Operational Workflows, the user is shown a text area for custom configuration at execution time. This could be used to pass extra variables that wouldn’t normally be in the script or for specifying extra configuration.

Edit Workflow

1. Select the Provisioning link in the navigation bar.
2. Select Automation from the sub-navigation menu.
3. Click the Workflows tab to show the workflows tab panel.
4. Click the Edit icon on the row of the workflow you wish to edit.
5. Modify information as needed.
6. Click the Save Changes button to save.
Delete Workflow

1. Select the Provisioning link in the navigation bar.
2. Select Automation from the sub-navigation menu.
3. Click the Workflows tab to show the workflows tab panel.
4. Click the Delete icon on the row of the workflow you wish to delete.

4.1.3 Scale Thresholds

Scale Thresholds are pre-configured settings for auto-scaling Instances. When adding auto-scaling to an instance, existing Scale Thresholds can be selected to determine auto-scaling rules.

Creating Scale Thresholds

1. Navigate to Library > Automation > Scale Thresholds
2. Select + ADD
3. Populate the following:

**NAME**  Name of the Scale Threshold

**AUTO UPSCALE**  Enable to automatically upscale per Scale Threshold specifications

**AUTO DOWNSCALE**  Enable to automatically downscale per Scale Threshold specifications

**MIN COUNT**  Minimum node count for Instance. Auto-scaling will not downscale below MIN COUNT, and will auto upscale if the MIN COUNT is not met.

**MAX COUNT**  Maximum node count for Instance. Auto-scaling will not upscale past MAX COUNT, and will auto downscale if MAX COUNT is exceeded.

**ENABLE MEMORY THRESHOLD**  Check to set auto-scaling by specified memory utilization threshold (%)

**MIN MEMORY**  Enter MIN MEMORY % for triggering downscaling.

**MAX MEMORY**  Enter MAX MEMORY % for triggering upscaling.

**ENABLE DISK THRESHOLD**  Check to set auto-scaling by specified disk utilization threshold (%)

**MIN DISK**  Enter MIN DISK % for triggering downscaling.

**MAX DISK**  Enter MAX DISK % for triggering upscaling.

**ENABLE CPU THRESHOLD**  Check to set auto-scaling by specified overall CPU utilization threshold (%)

**MIN CPU**  Enter MIN CPU % for triggering downscaling.

**MAX CPU**  Enter MAX CPU % for triggering upscaling.
4.1.4 Power Scheduling

Set weekly schedules for shutdown and startup times for Instances and VM’s, apply Power Schedules to Instances pre or post-provisioning, apply Power Schedule policies on Group or Clouds, or use Guidance to automatically recommend and apply optimized Power Schedules.

Create Power schedules

1. Navigate to Library > Automation > Power Scheduling
2. Select + ADD
3. Configure the following options:
   - **NAME**: Name of the Power Schedule
   - **DESCRIPTION**: Description for the Power Schedule
   - **TIME ZONE**: Time Zone the Power Schedule times correlate to.
   - **TYPE**
     - **Power On**: Power Up and then Down at scheduled times
     - **Power off**: Power Down then Up at scheduled times
     - **Enabled**: Check for Power Schedule to be Active. Uncheck to disable Power Schedule.
   - **DAYS**: Slide the start and end time controls for each day to configure each day’s Schedule. Green sections indicate Power on, red sections indicate Power Off. Time indicated applies to selected Time Zone.
4. Select SAVE CHANGES

**Tip:** To view the Instances a power schedule is currently set on, select the name of a Power Schedule to go to the Power Schedule Detail Page.
Add Power Schedule to Instance

1. Navigate to Provisioning > Instances
2. Select an Instance
3. Select EDIT
4. In the POWER SCHEDULE dropdown, select a Power Schedule.
5. Select SAVE CHANGES

Add Power Schedule to Virtual Machine

1. Navigate to Infrastructure > Compute > Virtual Machines
2. Select a Virtual Machine
3. Select EDIT
4. Expand the Advanced Options section
5. In the POWER SCHEDULE dropdown, select a Power Schedule.
6. Select SAVE CHANGES

Add Power Schedule Policy

Note: Power Schedule Policies apply to Instances created after the Policy is enabled.

1. Navigate to Administration > Policies
2. Select + ADD
3. Select TYPE Power Schedule
4. Configure the Power Schedule Policy:
   - NAME Name of the Policy
   - DESCRIPTION Add details about your Policy for reference in the Policies tab.
   - Enabled Policies can be edited and disabled or enabled at any time. Disabling a Power Schedule Policy will prevent the Power Schedule from running on the Clouds Instances until re-enabled.
   - ENFORCEMENT TYPE
     - User Configurable: Power Schedule choice is editable by User during provisioning.
     - Fixed Schedule: User cannot change Power Schedule setting during provisioning.
   - POWER SCHEDULE Select Power Schedule to use in the Policy. Power schedule can be added in Library > Automation > Power Scheduling
   - SCOPE
     - Global Applies to all Instances created while the Policy is enabled
     - Group Applies to all Instances created in or moved into specified Group while the Policy is enabled
     - Cloud Applies to all Instances created in specified Cloud while the Policy is enabled
     - User Applies to all Instances created by specified User while the Policy is enabled
Role  Applies to all Instances created by Users with specified Role while the Policy is enabled

Permissions- TENANTS  Leave blank to apply to all Tenants, or search for and select Tenants to enforce the Policy on specific Tenants.

5. Select SAVE CHANGES

4.1.5 Execute Scheduling

Execute Scheduling creates time schedules for Jobs, including Task, Workflow and Backup Jobs. Jobs, which are discussed in greater detail in another section of Morpheus docs, combine either a Task or Workflow with an Execute Schedule to run the selected Task or Workflow at the needed time. Backup Jobs are a special type of Job configured in the Backups section which also use Execute Schedules to time backup runs as needed.

Schedules use CRON expressions, such as 0 23 * * 2 equalling Executes every week on Tuesday at 23:00. CRON expressions can easily be created by clicking the corresponding translation in the create or edit Execution Schedule modal below the Schedule field and selecting a new value.

Note: For more on writing CRON expressions, see our KnowledgeBase article on the topic.

Create Execution Schedules

NAME  Name of the Execution Schedule

Note: When assigning Execution Schedules, the name value will appear in the selection drop-down. Using a name that references the time interval is often helpful

DESCRIPTION  Description of the Execution Schedule for reference in the Execution Schedules list

TIME ZONE  Time zone for execution

Enabled  Check to enable the schedule. Uncheck to disable all associated executions and remove the schedule as an option for Jobs in the future

SCHEDULE  Enter CRON expression for the Execution Schedule, for example 0 0 * * * equals Every day at 00:00

SCHEDULE TRANSLATION  The entered CRON schedule is translated below the SCHEDULE field. Highlighted values can be updated by selecting the value, and relevant options will be presented. The CRON expression will automatically be updated

4.2 Blueprints

4.2.1 Overview

The Blueprints section is used to compose provisioning catalogs. The Blueprints section is composed of:

• Instance Types
• Layouts
• Node Types
• App Blueprints
• Catalog Items
• Cluster Layouts

Additionally, items from Options and Templates sections are incorporated to call in custom options for users, IaaS spec files, scripts, and more. See Options and Templates within Morpheus Library for more information on creating or sourcing the items below from version control. In some cases, they may need to be pre-existing for the most efficient creation of Blueprints.

• Inputs
• Option Lists
• File Templates
• Scripts
• Spec Templates

4.2.2 Blueprint Development Overview

When provisioning, the User selects an INSTANCE TYPE from the provisioning wizard. At this stage, we can present custom INPUTS to the User which alter deployment in ways the administrator predetermines. Based on the selected Cloud technology and Version, the User is presented with applicable LAYOUTS selections. LAYOUTS can take advantage of Workflows which automate Tasks and can utilize a wide range of DevOps automation technologies. One or more NODE TYPES is associated with the LAYOUT. NODE TYPES are the bridge between LAYOUTS and Images. NODE TYPES can also take advantage of File Templates for custom configuration and Scripts which can be queued to run at any stage of the Instance lifecycle.
4.2.3 Instance Types

Adding an Instance Type creates a new Library item category. Multiple Layouts can be added to an Instance Type and these Layouts can have different Nodes attached. The Instance provisioning wizard will present the Layout options compatible with the selected Cloud. If Cloud selection is turned off, all Layouts will be presented for all Cloud types accessible by the User.
Name  Name of the Instance Type in the provisioning Library

Code  A useful shortcode for provisioning naming schemes and export reference

Description  The description of the Instance Type shown in the Provisioning Library. (255 characters max)

Category  For filtering in Instance sections and provisioning wizard

- Web
- SQL
- NoSQL
- Apps
- Network
- Messaging
- Cache
- OS
- Cloud
- Utility

4.2. Blueprints
Icon
An identifiable icon to display in-line with your Instance Type in the provisioning wizard (Suggested dimensions: 150 x 51)

Visibility
- Private: Only accessible by assigned Accounts/Tenants
- Public: Accessible by all Accounts/Tenants

Inputs Custom options presented to the user at provision time, Inputs are also created and stored in Morpheus Library

Environment Prefix Used for exportable environment variables when tying Instance Types together in App contexts. If not specified, a name will be generated

Environment Variables Name and value pairs for environment variables to be loaded on initialization

Enable Settings Allows for attachment of modifiable file templates to Node Types in a settings tab of the Instance after deployment

Enable Scaling (Horizontal) Enables load balancer assignment and auto-scaling features

Support Deployments Enables deployment features (Requires a data volume be configured on each version. Files will be copied into this location)

Upon saving, this Instance Type will be available in the provisioning catalog, per User Role access. However, we still need to add Layouts to the Instance Type, and prior to creating a Layout, we will add a Node Type.

4.2.4 Layouts

Layouts are attached to Instance Types. A Layout can only be attached to a single Instance Type and a single Technology. An Instance Type can have one or many Layouts attached to it, allowing for a single Instance Type to work with any Technology type. Node Types are added to Layouts. A Layout can have one or many node types attached to it. Node types can be shared across Layouts of matching Technology types.

Important: Once an Instance Type is defined on a Layout and saved, the Instance Type setting and Technology selections on the Layout cannot be changed.

Layout List View

The default page for Layouts is the Layout list view. Select + ADD to create a new Layout. Layouts can also be created from an Instance Type detail page.

The following fields are displayed for each Layout:

- NAME: Links to the Layout detail page
- VERSION
- INSTANCE TYPE: Links to the associated Instance Type
- DESCRIPTION

The Actions menu in each row reveals the following options:

- Permissions: Scope the Layout to Group(s) to narrow the list of available groups for a chosen Instance Type at provision time
- Edit: Edit the Layout
- Delete: Delete the Layout
Note: A Layout that is in use cannot be deleted.

Available Filters:

- **Technology**: Display Layouts by selected Cloud technology
- **Instance Type**: Display Layouts by the associated Instance Type

**Layout Detail View**

The Layout Detail view shows details on the Layout including Name, Short Name, Version, and Category. It also lists all associated Node Types.

- Select a Layout Name from the list page or Instance Type detail page to get to a Layout detail page.

**Layout Configuration Options**

**Instance Type**  Select the Instance Type to add to the new Layout. Custom Instance Types must already be created and one Layout cannot be added to multiple instance types. The Instance Type also cannot be changed after creation.

Note: Layouts cannot be added to Morpheus pre-defined Instance Types

**Name**  The name the Layout presents as in the Configuration Options dropdown of the provisioning wizard

**Version**  The version number or name for the Layout. Layouts in an Instance Type with the same version will all show under the Configuration Options dropdown when that version is selected while provisioning

**Description**  Description of the Layout, viewable on the Layout list view

**Creatable**  When checked, this Layout will be selectable at provision time for the associated Instance Type (assuming the Layout is otherwise compatible with provisioning conditions). Instance Types with no Creatable Layouts will not be selectable from the provisioning wizard

**Technology**  Technology determines which Cloud this layout will be available for and which Node Types can be added to it

**Minimum Memory**  Defines the minimum amount of memory required for this Layout. Only Service Plans that meet the defined memory minimum will be available during provisioning when this Layout is selected. Custom memory values must also meet this minimum. Entering a minimum memory value of zero (the default value) indicates no minimum. This minimum memory value will override any Virtual Image minimum memory requirements

**Workflow**  Select a Workflow to automatically run and be attached to associated Instances using this Layout. If a Workflow is defined, it is not presented in the provisioning wizard and is not user configurable

**Supports Convert to Managed**  Enabled to allow users to select this layout when converting a Discovered workload to Managed

**Enable Scaling (Horizontal)**  Enables Instances with this layout to use scaling features

**Environment Variables**  Custom environment variables to be added to the Instance when provisioned

**Inputs**  Search for and select one or multiple Inputs to add to the Layout. Inputs (except for Hidden Inputs) will appear in Provisioning, App, Blueprint, and Cloning wizards when this layout is selected

**Nodes**  Single or multiple nodes can be added to a Layout by searching for and selecting the Node(s)
4.2.5 Node Types

Node Types are the link between Images and Layouts.

Node Type Configuration Options

The following fields are for all Technology types:

**Name**  Name of the Node Type in Morpheus

**Short Name**  The short name is a lowercase name with no spaces used for display in your container list

**Version**  Version for the Node Type. Examples: 7.5, 2012 R2, latest

**Technology**  Select associated Technology. This will filter the available configuration options, images and which Layouts the Node Type can be added to

**Environment Variables**  Add pre-set environment variables to the Node Type

**Category**  Node Types of differing categories within the same Layout can have differing sizing

Technology-Specific Options

The Options fields will change depending on the Technology option selected. For VM provisioning technology options, select an image from the VM Image dropdown. This list is populated from the Morpheus Virtual Images section and will include images uploaded into Morpheus as well as synced images from added clouds.

---

**Note:** Amazon and Azure Marketplace Images can be added in the Virtual Images section for use as Node Types in custom library items.

---

Docker Options

For Docker, type in the name and version of the Docker Image, then select the integrated registry.

**Service Ports**  To open ports on the node, enter the name and port to expose. The Load Balancer HTTP, HTTPS, or TCP setting is required when attaching to Load Balancers.

Defining an Exposed port will also create a hyperlink(s) on the container location (IP) in the VM or Container section of the associated Instance detail page.

**Scripts**  Search for and select one or multiple scripts to be executed when the Node Type is provisioned

**File Templates**  Search for and select one or multiple File Templates to be written when the Node Type is provisioned

Example port configuration:
### VMware Options

When VMware Technology Type is selected, EXTRA OPTIONS will be available in the VMware VM Options section. These allow defining advance vmx-file parameters during provisioning.

Some examples include:

```
tools.setinfo.sizeLimit : 1048576
vmci0.unrestricted : FALSE
isolation.tools.diskWiper.disable : TRUE
```

**Note:** Not all parameters can be set using extra config parameters. A sample reference list can be found at http://www.sanbarrow.com/vmx/vmx-advanced.html#vmx

**Important:** Use caution when setting Extra Options. Malformed config files can break provisioning. Troubleshooting issues related to Extra Options defined are beyond the scope of Morpheus product support.
4.2.6 App Blueprint Overview

App Blueprints support a vast array of providers and configurations with programmatic markup or Infrastructure as Code capabilities. Blueprints configs can be manually added or scoped to a git repo. Morpheus blueprints allows for full automation configuration, locked fields, tiered boots, and linked tiers with exported evars. All blueprints have permission settings for controlling group and tenant access.

4.2.7 App Blueprint Types

- Morpheus
- Terraform
- ARM (Azure)
- CloudFormation (AWS)
- Kubernetes
- Helm

Morpheus Blueprints

Morpheus App Blueprints allow pre-configured full multi-tier application deployments for multiple environments. Blueprints can be provisioned from the Provisioning > Apps section and can be fully configured for one click provisioning. Blueprints can be built within the Builder section or by code in the Raw section. Blueprints can also be exported as YAML or JSON and created with the Morpheus API and CLI.

A unique capability of the YAML/JSON based Morpheus blueprint structure is the ability to have multiple configurations per instance being provisioned within the app blueprint. This can be a scoped configuration that acts as overrides based on selected cloud, group, and/or environment the app is being provisioned in as a target. For example, maybe the “development” environment doesn’t need as many horizontally scaled nodes as the “production” environment. Another great aspect of this configuration markup is a blueprint can be defined as a hybrid cloud blueprint. This makes the app blueprint structure very powerful and in some ways better than alternative infrastructure as code orchestrators. For Example, ARM is locked into Azure, while CloudFormation is locked into AWS. Even Terraform does not allow a tf file to expand its bounds beyond a specific provider type.

Basic Blueprint Structure

In a Morpheus App Blueprint there are a few structural concepts to be aware of. Firstly there is a concept of a Tier. A Tier is a grouping of instances within an app blueprint. Tiers can be used for a variety of things including sequenced booting of instances or even properly creating endpoint groups and security group contexts in network security tools like Cisco ACI. An example of a Tier structure might be a Web tier and a Database tier. These tiers can also be marked as connected such that network communication rules can appropriately be defined. A basic 2 Tier blueprint skeleton might look something like this:

```yaml
name: Tier Example
type: morpheus
tiers:
  Web:
    linkedTiers:
      - Database
tier:
    bootOrder: 1
```

(continues on next page)
This example has defined 2 tiers as yaml properties under the tiers object. They are called Web and Database. A Tier can optionally define its connected tiers which are bi-directional even though only one tier has to define them. This is the linkedTiers array and simply lists the connected tiers by tier name. A Boot Order can also optionally be defined under a nested{" tier": {" bootOrder": 1}} object structure.

Configuration Scopes

Another capability of Morpheus App Blueprint structure is its configuration scoping. This allows properties to be overridden based on the app's target environment or even target group and cloud. For example, maybe we want to use a larger plan size in production vs. development.

An example of that can be done using "environments" overrides.

Note the new environments object. The object graph of the morpheus blueprint structure gets merged and flattened at provision time based on the scope of the configurations provided as well as the user's target cloud, group, and environment selection. In the above example, a selective override was done for the AWS Cali cloud when using a Production Environment and deploying to the group All Clouds Demo. This specific example changes the plan to a larger size. Scoped configurations have various levels of precedence. Cloud is the lowest level of precedence. A cloud configuration in a group is the next level higher and finally an environment configuration in a group in a cloud is the highest level of scoped precedence.
Getting Started

To get started, it may be best to look at a simple App Blueprint configuration. Docker templates are less complex than virtual machine based templates so let's look at a Blueprint that deploys a single Nginx container to a target cloud:

```json
name: Simple Nginx
type: morpheus
tiers:
  Web:
    linkedTiers: []
    instances:
      - instance:
          type: docker
          name: Sample Nginx
    clouds:
      AWS Cali:
        instance:
          layout:
            code: docker-1.7-single
            id: 206
          volumes:
            - rootVolume: true
              name: root
              size: 1
          backup:
            createBackup: false
          config:
            dockerImageVersion: latest
            dockerRegistryId: ''
            dockerImage: nginx
          plan:
            id: 68
            code: container-128
          ports:
            - name: HTTP
              port: 80
              lb: HTTP
```

There are some useful things to look at in the above docker example. One is there are different objects based on the different available configuration options for the target provision type. These options are actually data driven and can be extracted from the Inputs api in the morpheus api doc. That is a useful resource to look at while building morpheus blueprints or by using the morpheus-cli which provides prompts for helping build custom morpheus app blueprints.
Creating Morpheus App Blueprints

1. Navigate to Library > Blueprints > App Blueprints
2. Select + ADD
3. Enter a NAME for the Blueprint and select NEXT
4. Optionally add a Description, Category, and Image for the Blueprint.

Add Tiers

1. In the STRUCTURE section, select + to add a Tier
2. Select or enter a Tier Name.
3. Select the Tier to set Boot Order, rename, or once multiple Tiers are added, connect the Tier to other Tiers.
Add Instances to Tiers

1. In the STRUCTURE section, select + in a Tier to add an Instance
2. Select an Instance Type
3. Optionally add a name for the Instance. Instances with blank names will automatically be named based off the App name.

Tip: You can use the variable ${app.name} in your instance naming convention to reference the name of the application you’re deploying.

Add Configurations to Instances

1. In the STRUCTURE section, select + in an Instance to add a Configuration
2. Select at least one option from Group, Cloud or Environment.
3. Select ADD CONFIG to create the configuration
4. Populate the Configuration
   • Configurations can be fully partially or populated
   • Fields can be locked or hidden by selecting the Lock icon next to the Field. Locking prevents the field from being editable when provisioning an App using the Blueprint while hidden fields are not revealed to the user at all
   • ALLOW EXISTING INSTANCE will allow users to add existing Instances to the App when using the blueprint

Save

Once all desired Tiers, Instances and Configurations are added, select Save. The Blueprint will be created, can be edited after saving, and will available in the Apps section for provisioning.

Note: Blueprints are not provisioned when created. To provision a Blueprint, use Provisioning > Apps.

RAW

Blueprints can be create, edited or Exported in the RAW section when creating or editing a blueprint.
To Export a Blueprint as JSON or YAML:

1. Navigate to Library > Blueprints > App Blueprints
2. Edit an existing App by clicking on the pencil icon
3. On the Edit Blueprint modal, select the Raw tab
4. Select YAML or JSON from the dropdown in the top right
5. Click the Export button
6. Select the configurations to include in the export by selecting or deselecting configurations as needed. Selected configurations will be highlighted
7. Click the DOWNLOAD CONFIGURATION button
8. The Blueprint export file will be downloaded to your computer as `{app_name}-config.json` or `{app_name}-config.yaml`
Preview

In the APP BLUEPRINT modal, select the Preview section to display a graphical representation of your Blueprint Tiers, Instances and Tier Connections.

**Important:** When Tiers are connected, the Instances in a Tier will import the evars from Instances in connected Tiers, and if Morpheus is managing the Instance Firewalls, communication between the Instances will be facilitated based on the Instances port configurations.

Provisioning

To provision a Blueprint, navigate to Provisioning > Apps and select the Blueprint when creating an App. See the App section of Morpheus docs for more on provisioning Apps.

4.2.8 Terraform Blueprints

Terraform Blueprints are one way that Terraform can be integrated and leveraged with Morpheus, with the other being the Morpheus Terraform provider which is not discussed in this section. Morpheus and Terraform are complimentary technologies which together can increase efficiency and simplify automation across cloud environments. For more on this relationship, see our [whitepaper](#) on how Morpheus and Terraform are better together.

Currently, Morpheus supports provisioning Apps based on Terraform Blueprints to VMware, Amazon, Azure, and Oracle Clouds with additional Cloud support coming in future releases. On first attempt to provision a Terraform App, Morpheus will automatically install Terraform. It is possible in some operating system configurations for this
automated installation process to fail, requiring you to install Terraform manually. If needed, manual installation
instructions and guidance are provided here.

To create a new Terraform Blueprint, navigate to Library > Blueprints > App Blueprints. Click + ADD.

On the Name tab of the New Blueprint modal, enter a name for your new Blueprint. In the Type dropdown menu,
select Terraform. NEXT

In the Blueprint Summary section, complete the following fields as needed:

- **NAME**: Enter a name for this Blueprint as it will appear in the Morpheus Blueprints list
- **DESCRIPTION**: An optional description field for your Blueprint
- **CATEGORY**: An optional category tag for your Blueprint, such as web, utility, or app
- **IMAGE**: An optional image icon to more easily identify your Blueprint from a list. If no image is uploaded, a
default image will be used

The Terraform Configuration section is where the Terraform template file (.tf) is added or linked to the Blueprint.
Using a Config Type of “Terraform (.tf)” or “Terraform JSON (.tf.json)”, you can write or paste your configuration
directly into the new Blueprint. Alternatively, you can pull in config files from an integrated Git repository using the
“Git Repository” Config type.

In the Terraform Configuration section, complete the following fields as needed when entering your configuration
directly into the new Blueprint:

- **CONFIG TYPE**: “Terraform (.tf)” or “Terraform JSON (.tf.json)” to create or paste configuration directly into
  the new Blueprint
- **CONFIG**: Enter your configuration here
- **TFVAR SECRET**: Select an existing TFVar-formatted Cypher. See the Cyphers section or Morpheus docs for
  more information on Cyphers
- **OPTIONS**: Enter any additional options, such as a variable definition

In the Terraform Configuration section, complete the following fields as needed when syncing in configuration from a
Git repository:

- **CONFIG TYPE**: “Git Repository”
- **SCM INTEGRATION**: If a pre-existing SCM integration is selected here, the available selections in the
  “Repository” dropdown menu will be filtered to show only those associated with the chosen SCM integration
- **REPOSITORY**: Select the repository in which your configuration resides
- **BRANCH OR TAG**: The branch in which your configuration resides
- **WORKING PATH**: The path to your configuration files
- **CONFIG**: Your selected config file
• **TFVAR SECRET**: Select an existing TFVar-formatted Cypher. See the Cyphers section of Morpheus docs for more information on Cyphers

• **OPTIONS**: Enter any additional options, such as a variable definition

Once finished, click **COMPLETE**.

Your new Terraform Blueprint is now saved and should be visible in the list of Blueprints. Blueprints are deployed in the Provisioning > Apps section of Morpheus. See the Apps section of Morpheus docs for more information on that process.

**ARM Blueprints**

ARM Blueprints provide a simple and repeatable way of deploying infrastructure-as-code to Azure Clouds. Objects and properties are defined in a JSON file and are provisionable on-demand in |ProApp|

To create a new ARM Blueprint, navigate to Library > Blueprints > App Blueprints. Click + ADD.

On the Name tab of the New Blueprint modal, enter a name for your new Blueprint. In the Type dropdown menu, select ARM. **NEXT**

In the Blueprint Summary section, complete the following fields as needed:

• **NAME**: Enter a name for this Blueprint as it will appear in the Morpheus Blueprints list

• **DESCRIPTION**: An optional description field for your Blueprint

• **CATEGORY**: An optional category tag for your Blueprint, such as web, utility, or app

• **IMAGE**: An optional image icon to more easily identify your Blueprint from a list. If no image is uploaded, a default image will be used

The ARM template itself is defined in the ARM Configuration section. Using the Config Type dropdown menu, we can opt to write or paste JSON configuration directly into this modal, or we can choose to bring in a JSON which we’re keeping under version control in a Git repository.

Depending on whether we need the Morpheus Agent installed and/or cloud-init enabled, mark the following boxes in the next section:

• **INSTALL AGENT**

• **CLOUD INIT ENABLED**

If writing or pasting your configuration JSON directly into the modal, fill out the following fields:

• **OS TYPE**: Identify the resources to be created as Linux or Windows

• **CONFIG TYPE**: ARM Template JSON (.json)

• **CONFIG**: Your JSON configuration template

If bringing in a template from a Git repository, fill out the following fields:

• **OS TYPE**: Identify the resources to be created as Linux or Windows

• **CONFIG TYPE**: “Git Repository”

• **SCM INTEGRATION**: If a pre-existing SCM integration is selected here, the available selections in the “Repository” dropdown menu will be filtered to show only those associated with the chosen SCM integration

• **REPOSITORY**: Select the repository in which your configuration resides

• **BRANCH OR TAG**: The branch in which your configuration resides

• **WORKING PATH**: The path to your configuration files
Morpheus Documentation

- **CONFIG**: Your selected config file

Once finished, click **COMPLETE**.

Your new ARM Blueprint is now saved and should be visible in the list of Blueprints. Blueprints are deployed in the Provisioning > Apps section of Morpheus. See the Apps section of Morpheus docs for more information on that process.

**CloudFormation Blueprints**

CloudFormation Blueprints consume new or existing CloudFormation templates to create easily-deployable application stacks. CloudFormation templates in Morpheus are JSON or YAML-formatted text documents that declare all relevant AWS resources needed for the provisioned application. They can be created directly in the New Blueprint modal or pulled in from existing Git repositories.

If needed, Amazon has educational resources available for getting started with CloudFormation. They can be found in the AWS CloudFormation documentation.

To create a new CloudFormation Blueprint, navigate to Library > Blueprints > App Blueprints. Click **+ ADD**.

On the Name tab of the New Blueprint modal, enter a name for your new Blueprint. In the Type dropdown menu, select CloudFormation. Click **NEXT**

In the Blueprint Summary section, complete the following fields as needed:

- **NAME**: Enter a name for this Blueprint as it will appear in the Morpheus Blueprints list
- **DESCRIPTION**: An optional description field for your Blueprint
- **CATEGORY**: An optional category tag for your Blueprint, such as web, utility, or app
- **IMAGE**: An optional image icon to more easily identify your Blueprint from a list. If no image is uploaded, a default image will be used

Depending on whether we need the Morpheus Agent installed and/or cloud-init enabled, mark the following boxes in the next section:

- **INSTALL AGENT**
- **CLOUD INIT ENABLED**

In some cases, you must explicitly acknowledge that your template contains certain capabilities in order for the application to successfully be deployed. There is more information on this in Amazon’s documentation [here](#). If any of the following capabilities are contained in your application, acknowledge them by marking any of the following boxes that apply:

- **CAPABILITY_IAM**
- **CAPABILITY_NAMED_IAM**
- **CAPABILITY_AUTO_EXPAND**

Continuing on with the CloudFormation Configuration section, complete the following fields as needed when entering your configuration directly into the new Blueprint:

- **CONFIG TYPE**: “CloudFormation Template JSON (.json)”
- **CONFIG TYPE**: “CloudFormation Template YAML (.yaml)”
- **CONFIG**: Enter your configuration here

In the CloudFormation Configuration section, complete the following fields as needed when syncing in configuration from a Git repository:

- **CONFIG TYPE**: “Git Repository”
• **SCM INTEGRATION:** If a pre-existing SCM integration is selected here, the available selections in the “Repository” dropdown menu will be filtered to show only those associated with the chosen SCM integration

• **REPOSITORY:** Select the repository in which your configuration resides

• **BRANCH OR TAG:** The branch in which your configuration resides

• **WORKING PATH:** The path to your configuration files

• **CONFIG:** Your selected config file

Once finished, click **COMPLETE**.

Your new CloudFormation Blueprint is now saved and should be visible in the list of Blueprints. Blueprints are deployed in the Provisioning > Apps section of Morpheus. See the Apps section of Morpheus docs for more information on that process.

**Kubernetes Blueprints**

Morpheus allows you to store Kubernetes configuration YAML files for easy deployment on-demand. Kubernetes Blueprints can be built by pulling in Kubernetes spec stored as a Morpheus Spec Template object, those tracked under version control in a Git repository, or you can write them directly in the New Blueprint modal.

To create a new Kubernetes Blueprint, navigate to Library > Blueprints > App Blueprints. Click **ADD**.

On the Name tab of the New Blueprint modal, enter a name for your new Blueprint. In the Type dropdown menu, select Kubernetes. **NEXT**

In the Cluster Summary section, complete the following fields as needed:

- **NAME:** Enter a name for this Blueprint as it will appear in the Morpheus Blueprints list

- **DESCRIPTION:** An optional description field for your Blueprint

- **CATEGORY:** An optional category tag for your Blueprint, such as web, utility, or app

- **IMAGE:** An optional image icon to more easily identify your Blueprint from a list. If no image is uploaded, a default image will be used

Complete the Kubernetes Configuration section as follows depending on your Config Type selection.

To consume a Morpheus Spec Template containing Kubernetes spec:

- **CONFIG TYPE:** “Kubernetes Spec”

- **SPEC TEMPLATE:** Use the typeahead field to locate the desired Spec Template

To draft or paste configuration directly in the New Blueprint modal:

- **CONFIG TYPE:** “Kubernetes Yaml Spec”

- **CONFIG:** Enter your YAML configuration template here

To consume YAML configuration files tracked in a Git repository:

- **CONFIG TYPE:** “Git Repository”

- **SCM INTEGRATION:** If a pre-existing SCM integration is selected here, the available selections in the “Repository” dropdown menu will be filtered to show only those associated with the chosen SCM integration

- **REPOSITORY:** Select the repository in which your configuration resides

- **BRANCH OR TAG:** The branch in which your configuration resides

- **WORKING PATH:** The path to your configuration files

- **CONFIG:** Your selected config file
Once finished, click *COMPLETE*.

Your new Kubernetes Blueprint is now saved and should be visible in the list of Blueprints. Blueprints are deployed in the Provisioning > Apps section of Morpheus. See the Apps section of Morpheus docs for more information on that process.

**Helm Blueprints**

If you’re using Helm Charts to manage Kubernetes applications, Morpheus allows you to bring them in from a Git repository as a Blueprint. The selected repository must be integrated with Morpheus before creating the Blueprint.

To create a new Helm Blueprint, navigate to Library > Blueprints > App Blueprints. Click *+ ADD*.

On the Name tab of the New Blueprint modal, enter a name for your new Blueprint. In the Type dropdown menu, select Helm. Click *guilabel:NEXT*.

In the Blueprint Summary section, complete the following fields as needed:

- **NAME**: Enter a name for this Blueprint as it will appear in the Morpheus Blueprints list
- **DESCRIPTION**: An optional description field for your Blueprint
- **CATEGORY**: An optional category tag for your Blueprint, such as web, utility, or app
- **IMAGE**: An optional image icon to more easily identify your Blueprint from a list. If no image is uploaded, a default image will be used

In the Helm Configuration section, complete the following fields as needed to sync in configuration from a Git repository:

- **CONFIG TYPE**: “Git Repository”
- **SCM INTEGRATION**: If a pre-existing SCM integration is selected here, the available selections in the “Repository” dropdown menu will be filtered to show only those associated with the chosen SCM integration
- **REPOSITORY**: Select the repository in which your configuration resides
- **BRANCH OR TAG**: The branch in which your configuration resides
- **CHART PATH**: The path to the folder within the repository containing your configuration files, enter “./” if this is the top level folder within the repository
- **CONFIG**: Config files within your selected folder are displayed here for confirmation

Once finished, click *COMPLETE*.

Your new Helm Blueprint is now saved and should be visible in the list of Blueprints. Blueprints are deployed in the Provisioning > Apps section of Morpheus. See the Apps section of Morpheus docs for more information on that process.

**4.2.9 Self Service**

The Self Service catalog (Tools > Self Service) is where administrators can create easily-deployable items for consumption by users operating under the “Service Catalog” Persona in Morpheus. Catalog items can be fully-configured Morpheus Instances or Blueprints, complete with user input through Morpheus Inputs, automation Workflows, and more. The catalog items are presented in a simplified interface for ease of deployment without sacrificing configurability for administrators. All available catalog items are built in the Self Service area and users will see relevant items in their catalogs based on Role permissions.
Access is granted to the Self Service section through the Tools: Self Service Role permission. Users with Read rights can view the catalog while users with full rights can create and edit catalog items. Users without any rights to Self Service will not be able to access the page at all.

Additionally, a user’s Role determines access to the standard and/or service catalog persona and which service catalog items are available for a user under the service catalog persona. See the Roles section of Morpheus documentation for more information on administering Roles.

**Viewing the Self Service Catalog**

The complete Self Service catalog can be viewed by clicking on Self Service from the Tools menu. The complete list of items available for the Self Service catalog are shown here but users working in the Service Catalog Persona will see only those allowed based on their user role. In addition to the name and type of each catalog item, we can also see a description and whether not the catalog item is featured or active. Featured items are given special visibility in the Service Catalog Persona and inactive items will not appear as provisioning options.

**Building Catalog Instances**

An Instance in Morpheus is a set of one or more containers or virutal machines that correlate to a single, horizontally-scalable entity or service suite. From the Self Service section, we can pre-configure Morpheus Instances and present them to users viewing the Service Catalog Persona for one-click deployment.

From the Catalog Items List Page (Tools > Self Service), click *ADD*. From the dropdown menu, select Instance. The modal window will appear to configure and add a new catalog Instance.
Configure the following:

- **NAME**: A friendly name for the catalog item in Morpheus
- **DESCRIPTION**: An optional description identifying the catalog item
- **ENABLED**: When checked, this catalog item will be available for provisioning
- **FEATURED**: When checked, this catalog item will be given special visibility in the Service Catalog Persona view
- **VISIBILITY**: Set to private to keep the catalog item available only to users in the current Tenant. Master Tenant
administrators may set catalog items to public to make them viewable and usable by Subtenant users

- **LOGO:** Select or upload a logo to be associated with this catalog item

- **CONFIG:** Enter, view, or edit Instance config here. Click **CONFIGURATION WIZARD** to build this catalog item through the Morpheus Add Instance wizard

- **CONTENT:** Optionally include documentation content for this Catalog Item. Markdown-formatted text is accepted and displayed appropriately when the item is ordered from the Service Catalog. A new Catalog Item-type Wiki entry will also be added containing this information.

- **INPUTS:** If desired, select Inputs to present users with mandatory or optional selections prior to provisioning

Once done, click **SAVE CHANGES**

**Tip:** Building catalog items through the configuration wizard is similar to the typical provisioning process for Instances in Morpheus. For more details on selections available in the configuration wizard, take a look at other sections of Morpheus docs on provisioning Instances.

---

**Building Catalog Blueprints**

Morpheus Blueprints allow for full multi-tier application deployment. In the Self Service catalog, user can create catalog items based on pre-existing App Blueprints. If new Blueprints need to be created for the Service Catalog, see other sections of Morpheus docs on building App Blueprints of various supported types. Just like with catalog Instances, we can pre-configure Blueprints and present them to users viewing the Service Catalog Persona view for easy, one-click deployment.

From the Catalog Items List Page (Tools > Self Service), click **ADD**. From the dropdown menu, select Blueprint. The modal window will appear to configure and add a new catalog Blueprint.

Configure the following:

- **NAME:** A friendly name for the catalog item in Morpheus

- **DESCRIPTION:** An optional description identifying the catalog item

- **ENABLED:** When checked, this catalog item will be available for provisioning

- **FEATURED:** When checked, this catalog item will be given special visibility in the Service Catalog Persona view

- **VISIBILITY:** Set to private to keep the catalog item available only to users in the current Tenant. Master Tenant administrators may set catalog items to public to make them viewable and usable by Subtenant users

- **LOGO:** Select or upload a logo to be associated with this catalog item

- **CONFIGURE:** Click **CONFIGURE** to use the familiar App provisioning wizard to tie Blueprint and App deployment configuration to the Catalog Item

- **APP SPEC:** Inject App spec here for any fields required to provision an App from your Blueprint. You may also inject any overrides to the existing Blueprint spec that are desired. App Spec configuration must be YAML, a simple example that names the App and sets the Group and Cloud is included below:

```
#Example App Spec
name: '%<%= customOption.appName %>'
group:
  name: Dev Group
environment: Dev
```

(continues on next page)
tiers:
  Web:
    instances:
      - instance:
        type: nginx
        cloud: Dev AWS
  App:
    instances:
      - instance:
        type: apache
        cloud: Dev AWS

- CONTENT: Optionally include documentation content for this Catalog Item. Markdown-formatted text is accepted and displayed appropriately when the item is ordered from the Service Catalog. A new Catalog Item-type Wiki entry will also be added containing this information.

- INPUTS: If desired, select Inputs to present users with mandatory or optional selections prior to provisioning

Note: App spec custom option variables should be single quoted in YAML: `cloud: '{@% = customOption.cloud %}'}`

Once done, click **SAVE CHANGES**

### Building Catalog Workflows

From the Catalog Items List Page (Tools > Self Service), click **ADD**. From the dropdown menu, select Workflow. The modal window will appear to configure and add a new catalog Workflow.

Configure the following:

- **NAME**: A friendly name for the catalog item in Morpheus
- **DESCRIPTION**: An optional description identifying the catalog item
- **ENABLED**: When checked, this Workflow item will be available for selection in the Service Catalog
- **FEATURED**: When checked, this catalog item will be given special visibility in the Service Catalog Persona view
- **VISIBILITY**: Set to private to keep the catalog item available only to users in the current Tenant. Master Tenant administrators may set catalog items to public to make them viewable and usable by Subtenant users
- **LOGO**: Select or upload a logo to be associated with this catalog item
- **WORKFLOW**: Select an existing Workflow to be associated with this Catalog Item, new Workflows are created in Library > Automation
- **CONTEXT TYPE**: Optionally restrict users to a specific target context, Instance, Server, or None
- **CONTENT**: Optionally include documentation content for this Catalog Item. Markdown-formatted text is accepted and displayed appropriately when the item is ordered from the Service Catalog. A new Catalog Item-type Wiki entry will also be added containing this information.

Once done, click **SAVE CHANGES**
Editing and Deleting from the Self Service Catalog

Once created, Service Catalog items can be edited or deleted from the Catalog Items list view (Tools > Self Service). Click the pencil icon in the relevant row to edit the Service Catalog item or the trash can icon to delete it. Alternatively, Service Catalog items can be made inactive to remove them as provisioning options rather than deleting them.

4.2.10 Cluster Layouts

Note: Morpheus now syncs available (non-preview) AKS k8s versions daily. Existing synced versions that are no longer supported by Azure are automatically disabled. The table below includes available AKS versions at time of v5.3.4 release.

Users can add new cluster layouts using the +ADD button. Morpheus-provided cluster layouts can be cloned for use in creating custom layouts. Custom cluster layouts can also be deleted or edited from the list view using the pencil or trash can icons.

<table>
<thead>
<tr>
<th>NAME</th>
<th>CODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kubernetes 1.20.7 Cluster AKS</td>
<td>kubernetes-azure-aks-1.20.7</td>
</tr>
<tr>
<td>Kubernetes 1.20.5 Cluster AKS</td>
<td>kubernetes-azure-aks-1.20.5</td>
</tr>
<tr>
<td>Kubernetes 1.19.11 Cluster AKS</td>
<td>kubernetes-azure-aks-1.19.11</td>
</tr>
<tr>
<td>Kubernetes 1.19.9 Cluster AKS</td>
<td>kubernetes-azure-aks-1.19.9</td>
</tr>
<tr>
<td>Kubernetes 1.18.19 Cluster AKS</td>
<td>kubernetes-azure-aks-1.18.19</td>
</tr>
<tr>
<td>Kubernetes 1.18.17 Cluster AKS</td>
<td>kubernetes-azure-aks-1.18.17</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 Cluster on Ubuntu 18.04</td>
<td>kubernetes-1.20.2-ubuntu-18.04.5-xen-amd64-single</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 Cluster on Ubuntu 18.04</td>
<td>kubernetes-1.20.2-ubuntu-18.04.5-scvmm-amd64-single</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 Cluster on Ubuntu 18.04</td>
<td>kubernetes-1.20.2-ubuntu-18.04.5-opentelekom-amd64-single</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 Cluster on Ubuntu 18.04</td>
<td>kubernetes-1.20.2-ubuntu-18.04.5-nutanix-amd64-single</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 Cluster on Ubuntu 18.04</td>
<td>kubernetes-1.20.2-ubuntu-18.04.5-morpheus-amd64-single</td>
</tr>
<tr>
<td>External Kubernetes 1.20</td>
<td>kubernetes-external-1.20</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 Cluster on Ubuntu 18.04</td>
<td>kubernetes-1.20.2-ubuntu-18.04.5-hyperv-amd64-single</td>
</tr>
<tr>
<td>NAME</td>
<td>CODE</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-----------------------------------------------------------</td>
</tr>
<tr>
<td>Kubernetes 1.17 Cluster on Linux, Weave, OpenEBS</td>
<td>kubernetes-xen-1.17-ubuntu-16.04-single</td>
</tr>
<tr>
<td>Kubernetes 1.17 Cluster on Linux, Weave, OpenEBS</td>
<td>kubernetes-scvmm-ubuntu-18.04-cluster-weave-openebs</td>
</tr>
<tr>
<td>Kubernetes 1.17 Cluster on Linux, Weave, OpenEBS</td>
<td>kubernetes-openstack-ubuntu-18.04-cluster-weave-openebs</td>
</tr>
<tr>
<td>Kubernetes 1.17 Cluster on Ubuntu 16.04, Weave, OpenEBS</td>
<td>kubernetes-openstack-ubuntu-18.04-single</td>
</tr>
<tr>
<td>Kubernetes 1.17 Cluster on Ubuntu 18.04, Weave, OpenEBS</td>
<td>kubernetes-nutaniux-ubuntu-18.04-cluster-weave-openebs</td>
</tr>
<tr>
<td>Kubernetes 1.17 Cluster on Ubuntu 18.04, Weave, OpenEBS</td>
<td>kubernetes-1.17-morpheus-linux-cluster-weave-openebs</td>
</tr>
<tr>
<td>Kubernetes 1.17 Cluster on Ubuntu 18.04, Weave, OpenEBS</td>
<td>kubernetes-1.17-morpheus-linux-single</td>
</tr>
<tr>
<td>Kubernetes 1.17 Cluster on Ubuntu 18.04, Weave, OpenEBS</td>
<td>kubernetes-hyperv-ubuntu-18.04-cluster-weave-openebs</td>
</tr>
<tr>
<td>Kubernetes 1.17 Cluster on Ubuntu 18.04, Weave, OpenEBS</td>
<td>kubernetes-hyperv-ubuntu-18.04-single</td>
</tr>
<tr>
<td>Kubernetes 1.17 Cluster on Ubuntu 18.04, Weave, OpenEBS</td>
<td>kubernetes-huawei-ubuntu-18.04-single</td>
</tr>
<tr>
<td>Kubernetes 1.17 Cluster on Ubuntu 18.04, Weave, OpenEBS</td>
<td>kubernetes-google-ubuntu-18.04-cluster-weave-openebs</td>
</tr>
<tr>
<td>Kubernetes 1.17 Cluster on Ubuntu 18.04, Weave, OpenEBS</td>
<td>kubernetes-google-ubuntu-18.04-single</td>
</tr>
<tr>
<td>Kubernetes 1.17 Cluster on Ubuntu 18.04, Weave, OpenEBS</td>
<td>kubernetes-exsi-ubuntu-18.04-cluster-weave-openebs</td>
</tr>
<tr>
<td>Kubernetes 1.17 Cluster on Ubuntu 18.04, Weave, OpenEBS</td>
<td>kubernetes-exsi-ubuntu-18.04-single</td>
</tr>
<tr>
<td>Kubernetes 1.17 Cluster on Ubuntu 18.04, Weave, OpenEBS</td>
<td>kubernetes-digitalOcean-ubuntu-18.04-single</td>
</tr>
<tr>
<td>Kubernetes 1.17 Cluster on Ubuntu 18.04, Weave, OpenEBS</td>
<td>kubernetes-azure-ubuntu-18.04-cluster-weave-openebs</td>
</tr>
<tr>
<td>Kubernetes 1.17 Cluster on Ubuntu 18.04, Weave, OpenEBS</td>
<td>kubernetes-azure-ubuntu-18.04-single</td>
</tr>
<tr>
<td>Kubernetes 1.17 Cluster on Ubuntu 18.04, Weave, OpenEBS</td>
<td>kubernetes-amazon-ubuntu-18.04-cluster-weave-openebs</td>
</tr>
<tr>
<td>Kubernetes 1.17 Cluster on Ubuntu 18.04, Weave, OpenEBS</td>
<td>kubernetes-amazon-ubuntu-18.04-single</td>
</tr>
<tr>
<td>Kubernetes 1.17 Cluster on Ubuntu 18.04, Weave, OpenEBS</td>
<td>kubernetes-alibaba-ubuntu-18.04-single</td>
</tr>
<tr>
<td>Kubernetes 1.17 Cluster on Ubuntu 18.04, Weave, OpenEBS</td>
<td>kubernetes-vmware-ubuntu-18.04-cluster-weave-openebs</td>
</tr>
<tr>
<td>Kubernetes 1.17 Cluster on Ubuntu 18.04, Weave, OpenEBS</td>
<td>kubernetes-vmware-ubuntu-18.04-single</td>
</tr>
<tr>
<td>Copy of Kubernetes 1.14 Cluster on Ubuntu 16.04, Weave, OpenEBS</td>
<td>6441b891-a61d-4f0b-a7f-19c81d2f51</td>
</tr>
<tr>
<td>Kubernetes 1.17 Cluster on Ubuntu 18.04, Weave, OpenEBS</td>
<td>kubernetes-1.17-fusion-ubuntu-18.04-single</td>
</tr>
<tr>
<td>Kubernetes 1.16 Cluster on Ubuntu 18.04, Weave, OpenEBS</td>
<td>kubernetes-1.16-fusion-ubuntu-18.04-single</td>
</tr>
<tr>
<td>Kubernetes 1.15 Cluster on Ubuntu 18.04, Weave, OpenEBS</td>
<td>kubernetes-1.15-fusion-ubuntu-18.04-single</td>
</tr>
<tr>
<td>External Kubernetes 1.17 Cluster</td>
<td>kubernetes-external-1.17</td>
</tr>
<tr>
<td>External Kubernetes 1.16 Cluster</td>
<td>kubernetes-external-1.16</td>
</tr>
<tr>
<td>External Kubernetes 1.15 Cluster</td>
<td>kubernetes-external-1.15</td>
</tr>
<tr>
<td>External Kubernetes 1.14 Cluster</td>
<td>kubernetes-external-1.14</td>
</tr>
<tr>
<td>KVM on Ubuntu 16.04</td>
<td>kvm-vmware-ubuntu-16.04-single</td>
</tr>
<tr>
<td>Morpheus KVM and Container Cluster</td>
<td>morpheus-kvm-combo-cluster</td>
</tr>
<tr>
<td>VMware Docker CentOS 7.5</td>
<td>docker-vmware-centos-7.5-single</td>
</tr>
<tr>
<td>Oracle Cloud Docker Host</td>
<td>docker-oraclecloud-ubuntu-16.04-single</td>
</tr>
<tr>
<td>Morpheus Kubernetes Manual Cluster</td>
<td>morpheus-kubernetes-manual-cluster</td>
</tr>
</tbody>
</table>

4.2. Blueprints

233
<table>
<thead>
<tr>
<th>NAME</th>
<th>CODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alibaba Docker Host</td>
<td>docker-alibaba-ubuntu-16.04-single</td>
</tr>
<tr>
<td>SCVMM Docker Host</td>
<td>docker-scvmm-ubuntu-16.04-single</td>
</tr>
<tr>
<td>KVM on Ubuntu 16.04</td>
<td>kvm-fusion-ubuntu-16.04-single</td>
</tr>
<tr>
<td>UpCloud Docker Host</td>
<td>docker-upcloud-ubuntu-16.04-single</td>
</tr>
<tr>
<td>Morpheus KVM Ubuntu Cluster</td>
<td>morpheus-kvm-ubuntu-cluster</td>
</tr>
<tr>
<td>Morpheus KVM CentOS Cluster</td>
<td>morpheus-kvm-centos-cluster</td>
</tr>
<tr>
<td>Azure Docker Host</td>
<td>docker-azure-ubuntu-16.04-single</td>
</tr>
<tr>
<td>KVM on CentOS 7.5</td>
<td>kvm-vmware-centos-7.5-single</td>
</tr>
<tr>
<td>VMware Docker Host</td>
<td>docker-vmware-ubuntu-16.04-single</td>
</tr>
<tr>
<td>Kubernetes 1.17 Cluster on Ubuntu 16.04, Weave, OpenEBS</td>
<td>kubernetes-vcd-ubuntu-16.04-single</td>
</tr>
<tr>
<td>VCD Docker Host</td>
<td>docker-vcd-ubuntu-16.04-single</td>
</tr>
<tr>
<td>SoftLayer Docker Host</td>
<td>docker-softlayer-ubuntu-16.04-single</td>
</tr>
<tr>
<td>Open Telekom Docker Host</td>
<td>docker-opentelekom-ubuntu-16.04-single</td>
</tr>
<tr>
<td>Huawei Docker Host</td>
<td>docker-huawei-ubuntu-16.04-single</td>
</tr>
<tr>
<td>Google Docker Host</td>
<td>docker-google-ubuntu-16.04-single</td>
</tr>
<tr>
<td>ESXi Docker Host</td>
<td>docker-esxi-ubuntu-16.04-single</td>
</tr>
<tr>
<td>IBM Docker Host</td>
<td>docker-bluemix-ubuntu-16.04-single</td>
</tr>
<tr>
<td>Xen Docker Host</td>
<td>docker-xen-ubuntu-16.04-single</td>
</tr>
<tr>
<td>Digital Ocean Docker Host</td>
<td>docker-digitalOcean-ubuntu-16.04-single</td>
</tr>
<tr>
<td>Hyper-V Docker Host</td>
<td>docker-hyperv-ubuntu-16.04-single</td>
</tr>
<tr>
<td>Docker on Linux</td>
<td>manual-linux-docker-morpheus-single</td>
</tr>
<tr>
<td>Kubernetes 1.14 on Ubuntu 16.04, Weave, OpenEBS</td>
<td>kubernetes-morpheus-ubuntu-16.04-single</td>
</tr>
<tr>
<td>Docker on Bare Metal</td>
<td>docker-morphes-metal-ubuntu-16.04-single</td>
</tr>
<tr>
<td>Docker on Ubuntu 16.04</td>
<td>docker-morphes-ubuntu-16.04-single</td>
</tr>
<tr>
<td>Amazon Docker Host</td>
<td>docker-amazon-ubuntu-16.04-single</td>
</tr>
<tr>
<td>OpenStack Docker Host</td>
<td>docker-openstack-ubuntu-16.04-single</td>
</tr>
<tr>
<td>Nutanix Docker Ubuntu 16.04</td>
<td>docker-nutanix-ubuntu-16.04-single</td>
</tr>
<tr>
<td>VMware Docker Ubuntu 16.04</td>
<td>docker-vmware-ubuntu-16.04-single</td>
</tr>
<tr>
<td>Kubernetes 1.14 Cluster on Ubuntu 16.04, Weave, OpenEBS</td>
<td>kubernetes-fusion-ubuntu-16.04-single</td>
</tr>
<tr>
<td>Docker on Ubuntu 16.04</td>
<td>docker-fusion-ubuntu-16.04-single</td>
</tr>
</tbody>
</table>

Users can add new cluster layouts using the +ADD button. Morpheus-provided cluster layouts can be cloned for use in creating custom layouts. Custom cluster layouts can also be deleted or edited from the list view using the pencil or trash can icons.
4.3 Virtual Images

4.3.1 Overview

The Virtual Image section displays a list of all images, local and synced, that are available to deploy. Morpheus includes a rich catalog of pre-configured System Images available for every cloud type. User Images are automatically synced from Cloud Integrations and added to the Virtual Images section. Images can also be uploaded directly into Morpheus via local file or url. Amazon and Azure Marketplace images can also be added to the Virtual Images Section.

Understanding the process of prepping images for consumption in Morpheus is a very important step toward building an effective Morpheus environment. In addition to the information contained in this section on Virtual Images, it may be helpful to see a complete image prep example walkthrough. Our getting started guide for Morpheus and VMware includes a section on preparing images that may provide a helpful example.

Important: Invalid Image Settings cause provisioning failures. Morpheus syncs in as much meta-data as possible for synced images, but additional configuration may be needed to ensure successful provisioning.

Warning: Cloud-init is enabled by default for all Linux images. If your Linux image does not have Cloud-init installed, Cloud-init Enabled must be unchecked before provisioning the image or it will fail immediately.

4.3.2 Image Types

Morpheus provides a vast System Image repo with pre-configured images for every Cloud. All other images are User Images. User images can be added directly to Morpheus, or automatically synced from integrated clouds. It is important to configure synced User Images for metadata, including specifying the Platform and User Credentials, prior to provisioning. Provisioning a User Image that has not been configured may result in failed provisioning.

Important: Synced User Images need to be configured prior to provisioning.
4.3.3 Configuring Virtual Images

System Images

System Virtual Images are pre-configured with metadata and have Cloud-Init or Cloudbase-Init installed. These images are ready to be provisioned with no configuration necessary, however it is required to populate Administration > Settings > Provisioning, Cloud-Init section, with user data as well as User Profile(s) users data when creating additional users prior to provisioning, as the user data from these sections is required when provisioning System provided Virtual Images.

Note: System Images settings are not editable.

User Images

Typically Morpheus does not have sufficient metadata to successfully provision synced User Images. After integrating clouds and User Images have synced, it is highly recommended to configure the images prior to provisioning.

To edit and configure an existing Virtual Image:

1. Select the pencil icon at the right of any row on the Virtual Images list page, or click EDIT on a Virtual Image detail page.

2. Configure the following on the Image:

   Name Name of the Virtual Image in Morpheus. This can be changed from the name of the image, but editing will not change the name of the actual image

   Operating System Specifies the platform and OS of the image. All Windows images will need to have the operating system specified on the Virtual Image, as Morpheus will assign Linux as the platform for all images without an operating system specified

   Minimum Memory The Minimum Memory setting will filter available Service Plan options during provisioning. Service Plans that do not meet the minimum value set on the Virtual Image will not be provided as Service Plan choices

   Cloud Init Enabled? On by default, uncheck for any Image that does not have Cloud-Init or Cloudbase-Init installed

   Install Agent? On by default, uncheck to skip Agent install. Note this will result in the loss of utilization statistics, logs, script execution, and monitoring. (Some utilization stats are still collected for Agent-less hosts and VMs depending on the cloud)

   Username Existing username on the image. This is required for authentication, unless Morpheus is able to add user data, Cloud-Init, Cloudbase-Init or Guest Customizations. If Cloud-Init, Cloudbase-Init or Guest Customizations are used, credentials are defined in Administration > Settings > Provisioning and User Settings. If credentials are defined on the image and Cloud-Init is enabled, Morpheus will add that user during provisioning, so ensure that user does not already exist on the image (such as root). For Windows Guest Customizations, Morpheus will set the Administrator password to what is defined on the image if Administrator user is defined. Do not define any other user than Administrator for Windows Images unless using Cloudbase-init. Morpheus recommends running Guest Customizations for all Windows Images, which is required when joining Domains as the SID will change.

   Password Password for the user on the image if username is populated

   Bucket Location where the Virtual Image will be stored. Default Virtual Image Storage location is /var/opt/morpheus/morpheus-ui/vms. Additional Storage Providers can be configured in Infrastructure > Storage.
**Cloud-Init User Data**  Accepts what would go in `runcmd` and can assume Bash syntax. Example use: Script to configure satellite registration at provision time

**Create Image ID**  Select FILE to browse locally for an image or drop an image file into the dropzone. Alternatively, select URL to download the image from an accessible URL. It is recommend to configure the rest of the settings below prior to uploading the source Image File(s).

**Permissions**  Set Tenant permissions in a multi-tenant Morpheus environment. Select private visibility and select specific Tenants to which the Virtual Image will be made available. Select public visibility to share the Virtual Image with all Tenants

**Auto Join Domain?**  Enable to have Instances provisioned with this image auto-join configured domains (Windows only, domain controller must be configured in Infrastructure > Network and the configured domain set on the provisioned to Cloud or Network).

**VirtIO Drivers Loaded?**  Enable if VirtIO Drivers are installed on the image for provisioning to KVM-based hypervisors

**FIPS Compliant Image?**  When selected, Morpheus will install the FIPS-compliant Morpheus Agent package

**VM Tools Installed?**  On by default, uncheck if VMware Tools (including OpenVMTools) are not installed on the Virtual Image. Morpheus will skip network wait during provisioning when deselected

**Force Guest Customization?**  VMware only, forces guest customizations to run during provisioning, typically when provisioning to a DHCP network where guest customizations would not run by default

**Trial Version**  Enable to automatically re-arm the expiration on Windows Trial Images during provisioning

**Enabled Sysprep?**  Applicable to multiple Clouds, including VMware vCenter, SCVMM, Nutanix, Hyper-V, KVM, and Google GCP. Enable if the Windows Image has been sysprepped. If enabled, Morpheus will inject `unattend.xml`

3. Click Save Changes

---

**Note:**  Cloud-Init is enabled by default on all images. Images without Cloud-Init or Cloudbase-Init installed must have the `cloud-init` flag disabled on the Virtual Image setting or Provisioning may fail.

---

### 4.3.4 Provisioning Images

When provisioning a system image, Morpheus will stream the image from Amazon S3 to the target Cloud if the image is not local to the Cloud.

When using images that already exist in the destination Cloud, such as synced, marketplace, or previously copied images, no image stream from S3 through the Morpheus Appliance to the destination cloud will take place.

**Note:**  The Morpheus Appliance must be able to download from Amazon S3 when provisioning system images.

**Note:**  The Morpheus Appliance must be able reach and resolve the destination Host when provisioning System Images or uploaded Images for the first time. This included being able to resolve ESXi host names in VMware vCenter clouds, and reach the destination ESXi host over port 443.
4.3.5 Add Virtual Image

Virtual Images can be upload to Morpheus from local files or URL’s. Amazon and Azure Marketplace metadata can also be added to the Virtual Images library, enabling the creation of custom catalog Instance Type from Marketplace images (no image is transferred to Morpheus when adding Marketplace images).

**Warning:** Be conscious of your Storage Provider selection. The default Storage Provider is the Morpheus Appliance at `/var/opt/morpheus/morpheus-ui/vms`. Uploading large images to the Morpheus Appliance when there is inadequate space will cause upload failures and impact Appliance functionality. Ensure there is adequate space on your selected Storage Provider. Additional Storage Provider can be added at Infrastructure > Storage, which can be configured as the default Virtual Image Store or selected when uploading Images.

To Add Virtual Image:

1. Select + Add in the Virtual Images page.
2. Select Image format:
   - Alibaba
   - Amazon AMI
   - Azure Marketplace
   - Digital Ocean
   - ISO
   - PXE Boot
   - QCOW2
   - RAW
   - VHD
   - VMware (vmdk/ovf/ova)
3. Configure the following on the Virtual Image:
   - **Name** Name of the Virtual Image in Morpheus. This can be changed from the name of the image, but editing will not change the name of the actual image
   - **Operating System** Specifies the platform and OS of the image. All Windows images will need to have the operating system specified on the Virtual Image, as Morpheus will assign Linux as the platform for all images without an operating system specified
   - **Minimum Memory** The Minimum Memory setting will filter available Service Plan options during provisioning. Service Plans that do not meet the minimum value set on the Virtual Image will not be provided as Service Plan choices
   - **Cloud Init Enabled?** On by default, uncheck for any Image that does not have Cloud-Init or Cloudbase-Init installed
   - **Install Agent?** On by default, uncheck to skip Agent install. Note this will result in the loss of utilization statistics, logs, script execution, and monitoring. (Some utilization stats are still collected for Agentless hosts and VMs depending on the cloud)
   - **Username** Existing username on the image. This is required for authentication, unless Morpheus is able to add user data, Cloud-Init, Cloudbase-Init or Guest Customizations. If Cloud-Init, Cloudbase-Init or Guest Customizations are used, credentials are defined in Administration > Settings > Provisioning and User Settings. If credentials are defined on the image and Cloud-Init is enabled, Morpheus
will add that user during provisioning, so ensure that user does not already exist on the image (such as root). For Windows Guest Customizations, Morpheus will set the Administrator password to what is defined on the image if Administrator user is defined. Do not define any other user than Administrator for Windows Images unless using Cloudbase-init. Morpheus recommends running Guest Customizations for all Windows Images, which is required when joining Domains as the SID will change.

**Password**  Password for the user on the image if username is populated

**Bucket**  Location where the Virtual Image will be stored. Default Virtual Image Storage location is /var/opt/morpheus/morpheus-ui/vms. Additional Storage Providers can be configured in Infrastructure > Storage.

**Cloud-Init User Data**  Accepts what would go in runcmd and can assume Bash syntax. Example use:

Script to configure satellite registration at provision time

**Create Image ID**  Select FILE to browse locally for an image or drop an image file into the dropzone. Alternatively, select URL to download the image from an accessible URL. It is recommend to configure the rest of the settings below prior to uploading the source Image File(s).

**Permissions**  Set Tenant permissions in a multi-tenant Morpheus environment. Select private visibility and select specific Tenants to which the Virtual Image will be made available. Select public visibility to share the Virtual Image with all Tenants

**Auto Join Domain?**  Enable to have Instances provisioned with this image auto-join configured domains (Windows only, domain controller must be configured in Infrastructure > Network and the configured domain set on the provisioned to Cloud or Network).

**VirtIO Drivers Loaded?**  Enable if VirtIO Drivers are installed on the image for provisioning to KVM-based hypervisors

**FIPS Compliant Image?**  When selected, Morpheus will install the FIPS-compliant Morpheus Agent package

**VM Tools Installed?**  On by default, uncheck if VMware Tools (including OpenVMTools) are not installed on the Virtual Image. Morpheus will skip network wait during provisioning when deselected

**Force Guest Customization?**  VMware only, forces guest customizations to run during provisioning, typically when provisioning to a DHCP network where guest customizations would not run by default

**Trial Version**  Enable to automatically re-arm the expiration on Windows Trial Images during provisioning

**Enabled Sysprep?**  Applicable to multiple Clouds, including VMware vCenter, SCVMM, Nutanix, Hyper-V, KVM, and Google GCP. Enable if the Windows Image has been sysprepped. If enabled, Morpheus will inject unattend.xml

---

**Note:**  Default Storage location is /var/opt/morpheus/morpheus-ui/vms. Additional Storage Providers can be configured in Infrastructure > Storage. Ensure local folders are owned by morpheus-app.morpheus-app if used.

---

**Warning:**  Provisioning will fail if Cloud init Enabled is checked and Cloud-Init is not installed on the Image.

---

**Note:**  Existing Image credentials are required for Linux Images that are not Cloud-Init enabled and for Windows Images when Guest Customizations are not used. Cloud-Init and Windows user settings need to be configured in

---

### 4.3. Virtual Images 239
Administration > Settings > Provisioning when using Cloud-Init or Guest Customizations and new credentials are not set on the Virtual Image.

4. **Upload Image**

   Images can be uploaded by File or URL:

   - **File** Drag and Drop the image file, or select Add File to select the image file.
   - **Url** Select the URL radio button, and enter URL of the Image.

   **Note:** The Virtual Image configuration can be saved when using a URL and the upload will finish in the background. When selecting/drag and dropping a file, the image files must upload completely before saving the Virtual Image record or the Image will not be valid.

5. Save Changes.

### 4.4 Options

Options are user-defined custom inputs that are used throughout Morpheus. Depending on the type of Input being created, users may need to create only an Input, or it might need to be paired with an Option List. Option Lists are static or dynamic lists of selections that would be associated with an Input if the user must make choices from a select list or typeahead field. This section discusses how to create different types of Inputs depending on the situation and powerful tools the user can take advantage of, such as dynamically filtered cascading inputs, logically generated Option Lists called from local or remote sources, and more.

#### 4.4.1 Inputs

Inputs are custom input fields that can be added to Instance Types and Layouts, then presented in Instance, App, and Cloning wizards. The resulting value is available in the Instance config map as `<%=customOptions.fieldName%>`. The fieldName and value can also be exported as Tags.
Create Input

**Note:** All possible fields listed. Displayed fields depend on TYPE selection

**NAME** Name of the Input

**DESCRIPTION** Description for reference in Input list view

**FIELD NAME** This is the input fieldName property that the value gets assigned to

**Note:** Field names should only contain letters, numbers, and hyphen (-), underscore (_), or dot ’.’ for separation.

**EXPORT AS TAG** Creates Tags for fieldName/value (key/value) on Instances

**DEPENDENT FIELD** The Field Name value for a field that will reload this Option List to present a different set of selections. Take a look at the section below on Cascading Inputs as well as the associated article in our KnowledgeBase for documented examples of this feature

**VISIBILITY FIELD** A Field Name and selection value that will trigger this field to become visible. Currently, this only works when the Input is associated with a Service Catalog Item and viewed from the Service Catalog Persona perspective. See the section below on the Visibility Field for instructions on configuring this value

**DISPLAY VALUE ON DETAILS** When selected, the Input label and value (label: value) will be visible in a list of custom options on the Instance detail page

**TYPE**

- **Text:** Text Input Field
- **Text Area:** A text area input, when selected an additional option appears to allow the user to configure the default number of visible rows in the text area
Morpheus Documentation

- **Select List**: Populated by Option Lists, presents a manual or REST-populated dropdown list
- **Checkbox**: Checkbox for on or off values
- **Number**: Input field allowing only numbers
- **Typeahead**: Populated by Option Lists: Rather than presenting a potentially-large dropdown menu, the user can begin typing a selection into a text field and choose the desired option. Multiple selections can be allowed with this type by marking the ‘ALLOW MULTIPLE SELECTIONS’ box
- **Hidden**: No field will be displayed, but the field name and default value will be added to the Instance config map for reference
- **Password**: An input field with suitable encryption for accepting passwords
- **Radio List**: Populated by Option Lists, presents a selection of radio buttons for the provisioning user

**LABEL**  This is the input label that typically shows to the left of a custom option

**ROWS**  For Textarea type Option Lists, determines how many text rows will be given when the Input is presented

**PLACEHOLDER**  Background text that populates inside a field for adding example values, does not set a value

**DEFAULT VALUE**  Pre-populates field with a default value

**HELP BLOCK**  Helpful text that will appear under your Input field to inform users about their selection

**REQUIRED**  Prevents User from proceeding without setting value

**DEFAULT CHECKED**  For Checkbox types, when marked the Checkbox will be checked by default

**OPTION LIST**  For Select List types, select a pre-existing Option List to set dropdown values

---

**Note:** Select List and Typeahead Inputs require creation and association of an Option List

---

**Cascading Inputs**

One powerful facet of Morpheus Inputs is the ability to present users with different lists of input options based on their selections in other Inputs within the same wizard or modal. One common example, which is fully illustrated in this section, is to have a user select:

- The Group they wish to provision into…
- Then select the target Cloud from a list limited to Clouds which are in the selected Group…
- Then select the target network from a list limited to networks which are available to the selected Cloud and Group

To set this up, we will first configure our Inputs (custom option fields that can be applied to Instance Types and other Morpheus constructs) and Option Lists (dynamic lists of possible choices which can be associated with Inputs and presented in a dropdown or typeahead format). Once the custom options are configured, we will associate them with a new service catalog item and take a look at how the user would interact with them.
Group Custom Option

To begin, we will create a new Option List. In this case, we will select type of “Morpheus Api” which will populate the list based on a call to the internal Morpheus API. Option Lists can also be populated by calls to external REST APIs or even from static lists that you enter manually. When dynamically populating Option Lists, whether via Morpheus API or an external API, translation and/or request scripts may be needed to prepare the request or translate the results. More on that as we build out the example.

I have called my Option List “Groups” and selected “Groups” from the OPTION LIST menu. This simply indicates that Groups are the construct we want to call into our list from Morpheus API. In this case, we want to present a list of all Groups to the user by their name and pass the Group database ID in the background. Since it is common to create Option Lists from Morpheus API where the construct name is displayed to the user and the ID is passed, we actually do not need to input any translation scripts in this case. However, I will include a translation script here which does the same thing simply to provide more clarity to the example. Morpheus Option List documentation includes additional details on available translation script inputs and which are available without translation as a convenience feature.

```javascript
for (var x = 0; x < data.length; x++) {
    results.push({name: data[x].name, value: data[x].id});
}
```

After saving the Option List, create the Input that presents the list we just created. I gave my Input the name of “Selected Group”, field name of “selectedGroup”, and label of “Group”. For type, choose “Select List” and a new field will appear at the bottom of the modal where we can select the Option List we just created. With this configuration, the Input will present as a dropdown list containing the options called from our Option List.

Cloud Custom Option

Adding the Option List and Input for Clouds will be similar to the prior step with the exception that we will be including a request script which effectively filters the list of available Clouds to only those associated with the selected group. Follow the same process to start a new Option List, I have configured mine as follows:

- **NAME:** Parsed Clouds
- **TYPE:** Morpheus Api
- **OPTION LIST:** Clouds

We also need a request script that loads the `siteId` attribute of the `results` variable with the Group ID if the user has made a group selection. Essentially it appends this input as a query parameter to the API call, calling (for example) `.../api/clouds?siteId=1` rather than `.../api/clouds`. It should be similar to the script below. Note that we are referencing the `selectedGroup` field name we created previously and that a “site” is the term for Groups in the Morpheus database.

```javascript
if (input.selectedGroup) {
    results.siteId = input.selectedGroup
}
```

We also need a translation script which will be identical to the one used previously with the exception that if there is no input on the `selectedGroups` field, nothing will be displayed for the Clouds option.

```javascript
if (input.selectedGroup) {
    for (var x = 0; x < data.length; x++) {
        results.push({name: data[x].name, value: data[x].id});
    }
}
```
We also need to create an Input to house this Option List. This process will be very similar to creating the previous Input except that we need to set selectedGroup as the Dependent Field. Setting a dependent field on an Input will trigger it to reload each time a selection is made in the indicated option. My configuration is as follows:

- **NAME:** Parsed Cloud
- **FIELD NAME:** parsedCloud
- **DEPENDENT FIELD:** selectedGroup
- **TYPE:** Select List
- **LABEL:** Cloud
- **OPTION LIST:** Parsed Clouds

Save your changes once done.

**Network Custom Option**

Finally, we will create an Option List/Input pair for network selection. In this case, it will be dependent on both the Group and Cloud selection. My Option List configuration is below:

- **NAME:** Parsed Networks
- **TYPE:** Morpheus Api
- **OPTION LIST:** Networks

**Request Script:**

```javascript
if (input.parsedCloud && input.selectedGroup) {
    results.cloudId = input.parsedCloud
    results.groupId = input.selectedGroup
}
```

**Translation Script:**

```javascript
if (input.parsedCloud && input.selectedGroup) {
    for (var x = 0; x < data.length; x++) {
        results.push({name:data[x].name, value:data[x].id});
    }
}
```

The Input is configured as follows:

- **NAME:** Parsed Networks
- **FIELD NAME:** parsedNetwork
- **DEPENDENT FIELD:** parsedCloud
- **TYPE:** Select List
- **LABEL:** Network
- **OPTION LIST:** Parsed Networks
Setting Custom Options at Provision Time

At this point, our dependent options are ready to be applied to custom Instance Types, Workflows or Service Catalog items as needed. When creating them, we can select an unlimited number of Inputs from a typeahead field on the create modal and they will be presented when a user goes to provision that element or run that Workflow. As an example, I have created a Service Catalog item that incorporates the three Inputs we have created. You can see how the dependent fields reload and present different options based on my selections.

Visibility Field

The Visibility field for Inputs allows users to set conditions under which the Input being created or edited is displayed. A very simple visibility configuration would look like the following:

```
config.customOptions.color:(red)
```

where “color” represents the fieldName for any other Input which will determine the visibility of the current one and “red” represents any JavaScript regular expression that matches to the values that meet your desired conditions.

Expanding on the simplified example above, we could trigger visibility based on any one of multiple selections from the same Input by using a different regular expression, such as

```
config.customOptions.color:(red|blue|yellow)
```

Additionally, we are not restricted to the conditions of just one Input to determine visibility as the following would also be valid:

```
config.customOptions.color:(red|blue|yellow),
config.customOptions.shape:(square)
```

In the previous example, the Input “Color” would have to be set to red, blue, or yellow OR the Input “Shape” would have to be set to square in order to trigger visibility of the Input currently being configured. Prepend the previous example with `matchAll::` in order to require both conditions to be met rather than one or the other (ex. `matchAll::config.customOptions.color:(red|blue|yellow),config.customOptions.shape:(square)`).

Putting it all together, you will first configure visibility for your selected Inputs as described above. You can see in the screenshot below I have set the Input being edited to have a visibility dependent on another Input which you can see in the background.

Next, ensure the relevant Inputs are associated with the Service Catalog Item (Tools > Self Service).
Finally, when Service Catalog Persona users interact with my Catalog Item, they will be able to toggle additional Inputs to be visible based on their selections.

### 4.4.2 Option Lists

Option Lists allow you to give the user more choices during provisioning to then be passed to scripts and/or automation. Option Lists, however, are pre-defined insofar as they are not free-form. They can be manually entered CSV or JSON, they can be dynamically compiled from REST calls via GET or POST requests, or populated by LDAP queries.

#### Generic Option List Fields

The displayed fields in the create/edit Option List modal depend on the TYPE value selected.

- **NAME**  Name of the Option List
- **DESCRIPTION**  Description of the Option List for reference in Option List list view
- **TYPE**  
  - REST: REST API call to populate Option List
  - Manual: Manually entered dataset, CSV or JSON
  - Morpheus API: Call to internal Morpheus API to populate the Option List
  - LDAP: Searches and returns a list of Active Directory objects

If the account assigned is not the master tenant, visibility will automatically change to private.
VISIBILITY If the account currently signed in is not in the master tenant, visibility will automatically change to private

Manual Option List Fields

DATASET Appears only for manual Option Lists. Add your CSV or JSON list to this field

Note: JSON entries must be formatted like the following example: [{"name":"Test","value":1},
{"name":"Testing","value":2}]

REST Option List Fields

SOURCE URL A REST URL used to fetch list data which is cached in the appliance database
REAL TIME When checked, a REST call will be made to update the Option List at the time its presented to the User
IGNORE SSL ERRORS Do not fail API query for self-signed or invalid certs on REST call target
SOURCE METHOD GET or POST
SOURCE HEADERS Custom HTTP Headers to include in the source request
INITIAL DATASET Create an initial JSON or CSV dataset to be used as the collection for this option list. It should be a list containing objects with properties ‘name’ and ‘value’
TRANSFORMATION SCRIPT Create a JS script to translate the result data object into an array containing objects with properties ‘name’ and ‘value’. The input data is provided as ‘data’ and the result should be put on the global variable ‘results’.

Example:
```
for(var x=0;x < data.length; x++) {
    results.push({name: data[x].name,value:data[x].id});
}
```

REQUEST SCRIPT Create a JS script to prepare the request. Return a data object as the body for a POST request, and return an array containing properties ‘name’ and ‘value’ for a GET request. The input data is provided as ‘data’ and the result should be put on the global variable ‘results’.

Example:
```
results.push({name: 'userId', value : data.users})
```

Morpheus API Option List Fields

OPTION LIST A list of available object types to return
TRANSFORMATION SCRIPT Create a JS script to translate the result data object into an array containing objects with properties ‘name’ and ‘value’. The input data is provided as ‘data’ and the result should be put on the global variable ‘results’.

Example:
```javascript
var i=0;
results = [];
for(i; i<data.length; i++) {
  results.push({name: data[i].name, value: data[i].value});
}
```

Translation script inputs:

**Clouds**
- id: <Number>
- value: <Number> // id, convenience
- name: <String>
- displayName: <String>
- category: <String>
- description: <String>
- apiKey: <String>
- status: <String>
- hourlyPrice: <Number>
- hourlyCost: <Number>
- instanceType: <Object>
  - id: <Number>
  - name: <String>
- plan: <Object>
  - id: <Number>
  - name: <String>
- site: <Object>
  - id: <Number>
  - name: <String>

**Environments**
- id: <Number>
- value: <Number> // id, convenience attribute to avoid requiring translation
- code: <String>
- name: <String>

**Groups**
- id: <Number>
- value: <Number> // id, convenience attribute to avoid requiring translation
- name: <String>
- code: <String>
- uuid: <String>
• location: <String>
• datacenterId: <Number>

Instances
• id: <Number>
• value: <Number> // id, convenience
• name: <String>
• displayName: <String>
• category: <String>
• description: <String>
• apiKey: <String>
• status: <String>
• hourlyPrice: <Number>
• hourlyCost: <Number>
• instanceType: <Object>
  – id: <Number>
  – name: <String>
• plan: <Object>
  – id: <Number>
  – name: <String>
• site: <Object>
  – id: <Number>
  – name: <String>

Instances Wiki
• id: <Number>
• value: <Number> // id, convenience
• name: <String>
• urlName: <String>
• category: <String>
• instanceId: <String>
• content: <String>
• contentFormatted: <String>
• format: <String>
• createdByUsername: <String>
• updatedByUsername: <String>

Networks
• id: <Number>
• value: <Number> // id, convenience
• code: <String>
• category: <String>
• name: <String>
• status: <String>
• cloudId: <Number>
• groupId: <Number>
• networkType: <Object>
  – id: <Number>
  – code: <String>
  – name: <String>
• externalId: <String>
• externalNetworkType: <String>
• networkDomain: <Object>
  – id: <Number>
  – name: <String>
• networkPool: <Object>
  – id: <Number>
  – name: <String>
• createdBy: <String>

Plans
• id: <Number>
• value: <Number> // id, convenience
• code: <String>
• name: <String>
• storage: <Integer, bytes>
• memory: <Integer, bytes>
• cores: <Number>

Resource Pools
• id: <Number>
• value: <Number> // id, convenience
• code: <String>
• externalId: <String>
• name: <String>
• serverGroupId: <Number>
• status: <String>
• regionCode: <String>
• parentPoolId: <Number>
• type: <String>

Security Groups
• id: <Number>
• value: <Number> // id, convenience
• code: <String>
• name: <String>
• externalType: <String>
• externalId: <String>
• cloudId: <Number>
• scopeMode: <String>
• scopeId: <Number>

Servers
• id: <Number>
• value: <Number> // id, convenience
• name: <String>
• displayName: <String>
• description: <String>
• category: <String>
• osType: <String>
• powerState: <String>
• lastStats: <String>
• zone: <Object>
  - id: <Number>
  - name: <String>
• capacityInfo: <Object>
  - maxStorage: <Integer, bytes>
  - maxMemory: <Integer, bytes>
  - maxCores: <Number>
  - usedMemory: <Integer, bytes>
  - usedStorage: <Integer, bytes>
• computeServerType: <Object>
  - id: <Number>
  - name: <String>
  - nodeType: <String>
REQUEST SCRIPT

The request script is used differently for Morpheus API Option List types. A Morpheus API option list type will use an internal API to return a list of objects instead of performing HTTP(S) requests to the Morpheus API. Due to this approach, the results object will not be used to generate query parameters or a JSON body. The results object will instead be used to contain a map of accepted key:value pairs that can be used to filter, sort and order the list of objects that get returned.

Below is a list of accepted key:value pairs for each object type:

**Generic options available for all object types**

- max: <integer>  // Maximum number of results to return. Default: 25
- offset: <integer>  // Offset for returned results. Default: 0
- sort: <string>  // Field to sort on. Default: ‘name’

**Example:**

```plaintext
results = {max: 5, order : 'desc'}
```

**Networks**

- zoneId
- siteId
- planId
- provisionTypeId: <Number>  // Id of the provision type (technology), filters to only networks associated with this provision type
- layoutId: <Number>  // Id of an Instance Layout, ignored if provisionTypeId is supplied, otherwise used to look up the provision type
- poolId: <Number>  // Id of a network pool, filters to only networks within the specified network pool

**Plans**

- zoneId
- siteId
• **layoutId**

• **provisionTypeId**: <Number> // Id of the provision type (technology), filters to only plans associated with this provision type

### Resource Pools

• **zoneId**

• **siteId**

• **planId**

• **layoutId**: <Number> // Id of an Instance Layout, used to get the associated provision type and filter to that provision type

### Security Groups

• **zoneId** // required

• **poolId**

### Clouds

• **zoneId**: <integer> // Database ID of cloud to return

• **tenantId**: <integer> // Database ID of tenant where clouds are added. Filters to only clouds added within the specified tenant. Only available in Master Tenant

• **zoneTypeId**: <integer> // Database ID of cloud type. Filters to only clouds with the specified cloud type

• **siteId**: <integer> // Database ID of group. Filters to only clouds within the specified group

• **tagName**: <string> // Filters to clouds with servers with tags containing the tagName

• **tagValue**: <mixed> // Requires tagName. Filters to clouds with servers that have tags containing the tagName and specified tagValue

• **phrase**: <string> // Fuzzy matches phrase on cloud name and description

**Example:** `results = {tenantId: 1, siteId: 1, tagName: "morpheus"}`

### Instances

• **appsId**: <integer> // Database ID of app to filter by. Returns instances linked to the app

• **tenantId**: <integer> // Database ID of tenant where instances are located. Filters to only instances within the specified tenant. Only available in Master Tenant

• **serverId**: <integer> // Database ID of server. Filters to the instance that contains the specified server

• **tagName**: <string> // Filters to instances with tags containing the tagName

• **tagValue**: <mixed> // Requires tagName. Filters to instances with tags containing the tagName and specified tagValue

• **phrase**: <string> // Fuzzy matches phrase on instance name and description

**Example:** `results = {tenantId:1, phrase: "ha"}`

### Groups

• **tenantId**: <integer> // Database ID of tenant where groups are located. Filters to only groups added within the specified tenant. Only available in Master Tenant
• zoneTypeId : <integer> Database ID of cloud type. Filters to only groups that contain clouds with the specified cloud type

• zoneId : <integer> // Database ID of cloud. Filters to only groups that contain the cloud with the specified ID

• siteId : <integer> // Database ID of group to return

• phrase : <string> // Fuzzy matches phrase on group name and location.

Servers

• tenantId : <integer> // Database ID of tenant where servers are located. Filters to only servers within the specified tenant. Only available in Master Tenant

• serverId : <integer> // Database ID of server. Filters to the server specified by the ID

• siteZoneId : <integer> // Database ID of cloud. Filters to servers contained within the specified cloud

• serverType : <string> // Type of server. Accepted values: ‘host’, ‘baremetal’, ‘vm’

• siteId : <integer> // Database ID of group. Filters to only servers contained within clouds that are added in the specified group

• tagName : <string> // Filters to servers with tags containing the tagName

• tagValue : <mixed> // Requires tagName. Filters to servers with tags containing the tagName and specified tagValue

• phrase : <string> // Fuzzy matches phrase on server name and description.

  Example: results = {max: 50, siteZoneId : 3}

instance-wiki

Contains same options for Instances Morpheus API type.

• phrase : <string> // Fuzzy matches phrase on wiki name, urlName and content

server-wiki

Contains same options for Servers Morpheus API type.

• phrase : <string> // Fuzzy matches phrase on wiki name, urlName and content

LDAP Option List Fields

LDAP URL  The URL pointing to the LDAP server

USERNAME  The fully qualified username (with @ suffix syntax) for the binding account

PASSWORD  The password for the above account

LDAP Query  The LDAP query to pull the appropriate objects. See the next section for an example use case

TRANSLATION SCRIPT  Create a JS script to translate the result data object into an array containing objects with properties ‘name’ and ‘value’. The input data is provided as ‘data’ and the result should be put on the global variable ‘results’.

Note:  Option Lists are set on one or multiple Select List or Typeahead Inputs. The Input is then set on an Instance Type, Layout, Cluster Layout, and/or Operational Workflow for input during provisioning or execution.
Creating an Option List Based on an LDAP Query

In Morpheus version 4.2.1 and higher, Option Lists can be populated from LDAP queries. This gives users the ability to search Active Directory, capture objects, and present them as custom options where needed.

It’s recommended that you connect LDAP-type Option Lists to Typeahead-type Inputs as the list of returned selections can be very large. This also allows you to select multiple options from the list, presuming you’ve allowed for that when creating the Input.

Populating LDAP-type Option Lists requires knowledge of LDAP query syntax. This guide provides one example and there are many publicly-available resources for help writing additional queries.

1. Create a new Option List (Library > Options > Option Lists > ADD)
2. Enter a name for the new LDAP Option List
3. Change the Type value to LDAP and the relevant fields will appear as shown in the screenshot:
4. Enter the LDAP URL in the following format (an example is also shown as a placeholder in the UI form field):

   ldap[s]://<hostname>:<port>/<base_dn>

5. Enter the fully qualified username with @ suffix syntax, such as: user@ad.mycompany.com
6. Enter the account password
7. Enter your LDAP query. You can even inject variables into your query structure to query based on the value the user has entered into the typeahead field as shown in the example below:

   (&(objectClass=user)(cn=<%=phrase%>*))

8. Finally, enter a translation script which will convert the returned LDAP object into a list of name:value pairs you can work with in Morpheus. The example script below shows the user DisplayName and sets the value to the SAMAccountName:

   ```javascript
   for(var x=0;x < data.length ; x++) {
     var row = data[x];
     var a = {};
     if(row.displayName != null) {
       a['name'] = row.displayName;
     } else {
       a['name'] = row.sAMAccountName;
     }
     a['value'] = row.sAMAccountName;
     results.push(a);
   }
   ```

9. Click SAVE CHANGES
4.5 Templates

Templates can be created directly in Morpheus and/or sourced from version control, depending on the type. They can be used to help users consume IaC technologies, generate configuration files, utilize scripts or store security scan packages. Once stored, they can be used with provisioned Instances, configured as part of Tasks or Workflows, or run regularly as part of security scan Jobs. Each section below discusses template types in greater detail.

4.5.1 Spec Templates

Spec Templates allow Morpheus users to leverage several major Infrastructure-as-Code solutions. These are typically JSON or YAML-based configuration files which make creating and managing multiple resource types easier. Morpheus allows users to create and/or manage a collection of these templates for different solutions and from different sources.

Morpheus currently supports Spec Templates of the following types:

- Kubernetes Spec
- Helm Chart
- Terraform
- ARM Template
- CloudFormation Template
Morpheus Documentation

- OneView Server Profile Template
- UCS Service Profile Template

Morpheus also allows users to leverage templates pulled from URL sources, online repositories (such as GitHub), or you can write a template locally inside the “NEW SPEC TEMPLATE” modal.

**Tip:** To see Morpheus Spec Templates in action, take a look at our guide on creating custom Instance Types using Terraform or see our KnowledgeBase for another example where a CloudFormation Spec Template is used to create a provisionable custom Instance Type.

### Creating a Spec Template

1. Navigate to Library > Templates > Spec Templates
2. Click **ADD**
3. Complete the following fields, then click **SAVE CHANGES**:
   - **NAME**
   - **TYPE:** See the previous section for a complete list of Spec Template types
   - **SOURCE:** Local, Repository, or URL
   - **CONTENT:** If this is a local Spec Template, supply the template in this field. If the template is supplied through a URL or online repository, the CONTENT field will change to allow the user to point Morpheus to that resource
   - **VERSION:** (Only displayed on Terraform Spec Templates) Enter a Terraform version number to force a specific version when provisioning your Terraform Instance Type or App, assuming your Terraform Runtime setting (Administration > Settings > Provisioning Tab) is “auto”. If Terraform Runtime is set to “manual”, Morpheus will use the version of Terraform installed on the appliance box

### 4.5.2 File Templates

File Templates are for generating config files, such as my.cnf, elasticsearch.yml, morpheus.rb, or any text file. With full config map variable support, Template Files are dynamically generated during a Workflow phase or ad hoc via Instance actions.

File Templates can also be exposed on Instances in the Settings Tab. Ensure the Instance Type supports settings, and Category is defined in Advance Options on the Library Template config.

**Note:** Morpheus variables are supported in Library Templates using `<%= variable.var %>` format

Examples:

HA Proxy Config (haproxy.cfg)

- **FILE NAME:** haproxy.cfg
- **FILE PATH:** /config/haproxy.cfg
- **PHASE:** Pre Provision
- **TEMPLATE:**
- **SETTING NAME:** haproxyConfig
• SETTING CATEGORY: haproxy

```bash
#!/bin/bash

global
   maxconn 256
   log /dev/log local0 warning
   log-tag <%=logTag%>

defaults
   mode http
   timeout connect 5000ms
   timeout client 50000ms
   timeout server 50000ms
   log global

frontend http-in
   bind *:<%=container.externalPort%>
   default_backend servers

backend servers
   # server server1 127.0.0.1:80 maxconn 32
```

mysql config (mysqld.cnf)

- FILE NAME: mysqld.cnf
- FILE PATH: /config/mysqld.cnf
- PHASE: Pre Provision

```bash
#!/bin/bash

[mysqld]
pid-file= /var/run/mysqld/mysqld.pid
socket= /var/run/mysqld/mysqld.sock
datadir= /var/lib/mysql
# Disabling symbolic-links is recommended to prevent assorted security risks
symbolic-links=0
explicit_defaults_for_timestamp = 1
```

### 4.5.3 Script Templates

Scripts are bash and Powershell scripts that can be attached to Node Types to always execute at the selected phase when that Node Type is provisioned, added to Workflows as Library Script Tasks, and/or executed ad-hoc on Instances.

**Creating Scripts**

1. Navigate to Library > Templates > Script Templates
2. Select + ADD
3. Enter the Following:
   - **NAME**: Name of the Script in Morpheus
   - **SCRIPT TYPE**
     - Bash
• Powershell

PHASE  Select which phase the Script will execute when attached to a Node Type. When a script is attached to a Node Type, it will execute according to the selected phase:

Start Service  Any time the Instance action Start Service is executed
Stop Service  Any time the Instance action Stop Service is executed

Pre-Provision
• Containers: Script will execute against the container host before the container is provisioned
• Virtual Machines: Script will execute before any provision phase Scripts or Tasks

 Provision
Script will execute once per new Instance node during the provision Phase. Provisioning will not be considered complete until all scripts and tasks in the provisioning phase are completed

 Note: Any Script or Task set to the provision phase will be included in the total provision time and impact success/warn/failure provisioning status messages. As an example, your VM could be up and running but if your Script is in the provision phase and fails, provisioning will be marked as a failure.

Post-Provision  Script will execute once per new Instance node after the provision phase is completed. Scripts and Tasks in the Post-Provision phase will show execution status and history, but are not considered part of the provision and do not impact provisioning status.

Pre-Deploy  Script will execute on target Instance any time a deployment is run against the Instance. The Script will run prior to the deployment file(s) being written

Deploy  Script will execute on target Instance any time a deployment is run against the Instance. The script will run after the deployment file(s) are written

Reconfigure  Script will execute on target Instance any time a reconfigure is executed against the Instance.

Teardown  Script will execute on target Instance upon Instance deletion. Script will execute against target Instance prior to the deletion/removal of resources.

SCRIPT  Enter Bash or Powershell script.

 Note: Morpheus variables are supported in Library Scripts using <%= variable.var %> format

RUN AS USER  By default Scripts are execute as morpheus-node. To execute as another User, populate RUN AS USER and ensure proper user permissions & group access

SUDO  Flag SUDO if sudo is required to execute the Script

To attach Scripts and templates that have been added to the Library to a Node Type, start typing the name and then select the script(s) and/or template(s).

• Multiple scripts and templates can be added to a Node Type
• Scripts and Templates can be added/shared among multiple Node Types
• The execution phase can be set for Scripts in the Scripts section
• Search will populate Scripts or Templates containing the characters entered anywhere in their name, not just the first letter(s) of the name
4.5.4 Security Packages

The Security Packages Section is for uploading SCAP packages which can then be consumed in Security Scan Jobs (Provisioning > Jobs).

Add a new Security Package

1. Navigate to Library > Templates > Security Packages
2. Click +ADD > SCAP Package
3. Provide a name in addition to a URL to source the package
4. Click SAVE CHANGES

Note: Currently URL is the only source option for security packages

4.6 Library Integrations

The integrations section within Morpheus Library lists existing integrations and allows for the creation of new integrations which are related to automation technologies. A complete list of integrated third party technologies is available in the Administration section (Administration > Integrations). More detailed information about each Morpheus integration with third party technologies is included in our Automation Integrations section.

4.7 Variables

A vast number of variables are available for use in Tasks, Scripts, Templates, Resource Names, Cloud-Init User Data and Option List configs.

Important: Variables are case sensitive
4.7.1 Pre-Provision Vars

A subset of variables are available for Instance, Host Name and Hostnames. These can be passed inside ${ }$ blocks during provisioning or in relevant policy configs. Groovy syntax can be resolved to allow for dynamic name generation as shown in some of the examples below.

Instance Naming Policy example: ${userInitials}-${cloudCode}-${platform == 'windows' ? 'W' : 'L'}-${sequence}

Available variables for Naming Policy naming patterns include:

```groovy
${account}
${accountId}
${accountName}
${accountNumber}
${accountType}
${cloudCode}
${cloudName}
${customerNumber}
${customOptions.fieldName}
${groupCode}
${groupName}
${instance.instanceContext} # Environment Code
${platform == 'windows' ? 'w': 'l'} # results in `w` for Windows platforms and `l` for Linux Platforms
${platform}
${provisionType}
${sequence} # results in 1
${sequence+100} # results in 101
${sequence.toString().padLeft(5,'0')} # results in 00001
${tenantId}
${tenant} # Tenant Name
${tenantSubdomain}
${type}
${userId}
${userInitials}
${username}
```

An example Instance Name Policy using a naming pattern with User Initials, Cloud Code, Instance Type, and a sequential number starting at 3000 is ${userInitials}-${cloudCode}-${type}-${sequence+3000}, resulting in an Instance Name of md-vmwd3-centos-3001 for the first instance, followed by md-vmwd3-centos-3002 and so on.

4.7.2 Syntax Examples

PowerShell Example: $app_id = "<%= instance.metadata.app_id %>"

Bash Example: HOSTNAME="<%= container.server.hostname %>"

Python Example: hostname = morpheus['server']['hostname']

HTTP Body Example: {"name": "<%= instance.createdByUsername %>"}
Note: customOptions values are defined from custom Inputs.

4.7.3 Common Examples

```plaintext
container.configGroup: <%=container.configGroup%>
container.configId: <%=container.configId%>
container.configPath: <%=container.configPath%>
container.configRole: <%=container.configRole%>
container.containerTypeCode: <%=container.containerTypeCode%>
container.containerTypeName: <%=container.containerTypeName%>
container.containerTypeShortName: <%=container.containerTypeShortName%>
container.cores: <%=container.cores%>
container.dataPath: <%=container.dataPath%>
container.dateCreated: <%=container.dateCreated%>
container.domainName: <%=container.domainName%>
container.environmentPrefix: <%=container.environmentPrefix%>
container.externalIp: <%=container.externalIp%>
container.hostMountPoint: <%=container.hostMountPoint%>
container.hostname: <%=container.hostname%>
container.image: <%=container.image%>
container.internalHostname: <%=container.internalHostname%>
container.internalIp: <%=container.internalIp%>
container.logsPath: <%=container.logsPath%>
container.memory: <%=container.memory%>
container.planCode: <%=container.planCode%>
container.provisionType: <%=container.provisionType%>
container.server: <%=container.server.serverTypeName%>
container.serverId: <%=container.serverId%>
container.sshHost: <%=container.sshHost%>
container.status: <%=container.status%>
container.storage: <%=container.storage%>
container.version: <%=container.version%>
customOptions: <%=customOptions.fieldName%>
evar: <%=evars.name%>
evars: <%=evars%>
group.code: <%=group.code%>
group.datacenterId: <%=group.datacenterId%>
group.location: <%=group.location%>
group.name: <%=group.name%>
instance.autoScale: <%=instance.autoScale%>
instance.configGroup: <%=instance.configGroup%>
instance.configId: <%=instance.configId%>
instance.configRole: <%=instance.configRole%>
instance.containers[0]: <%=instance.containers[0].containerTypeName
instance.cores: <%=instance.cores%>
instance.createdByEmail: <%=instance.createdByEmail%>
instance.createdByFirstName: <%=instance.createdByFirstName%>
instance.createdById: <%=instance.createdById%>
instance.createdByLastName: <%=instance.createdByLastName%>
instance.createdByUsername: <%=instance.createdByUsername%>
instance.deployGroup: <%=instance.deployGroup%>
instance.description: <%=instance.description%>
```

(continues on next page)
instance.displayName: <%=instance.displayName%>
instance.domainName: <%=instance.domainName%>
instance.environmentPrefix: <%=instance.environmentPrefix%>
instance.expireDate: <%=instance.expireDate%>
instance.firewallEnabled: <%=instance.firewallEnabled%>
instance.hostname: <%=instance.hostname%>
instance.instanceContext: <%=instance.instanceContext%> (tip: 

\[instanceContext = Environment\]

instance.instanceLevel: <%=instance.instanceLevel%>
instance.instanceTypeCode: <%=instance.instanceTypeCode%>
instance.instanceTypeName: <%=instance.instanceTypeName%>
instance.instanceVersion: <%=instance.instanceVersion%>
instance.memory: <%=instance.memory%>
instance.metadata: <%=instance.metadata%>
instance.name: <%=instance.name%>
instance.networkLevel: <%=instance.networkLevel%>
instance.plan: <%=instance.plan%>
instance.provisionType: <%=instance.provisionType%>
instance.status: <%=instance.status%>
instance.statusMessage: <%=instance.statusMessage%>
instance.storage: <%=instance.storage%>
instance.tags: <%=instance.tags%>
instance.userStatus: <%=instance.userStatus%>
server.agentInstalled: <%=server.agentInstalled%>
server.agentVersion: <%=server.agentVersion%>
server.apiKey: <%=server.apiKey%>
server.category: <%=server.category%>
server.commType: <%=server.commType%>
server.configGroup: <%=server.configGroup%>
server.configId: <%=server.configId%>
server.configRole: <%=server.configRole%>
server.consoleHost: <%=server.consoleHost%>
server.consolePort: <%=server.consolePort%>
server.consoleType: <%=server.consoleType%>
server.consoleUsername: <%=server.consoleUsername%>
server.dataDevice: <%=server.dataDevice%>
server.dateCreated: <%=server.dateCreated%>
server.description: <%=server.description%>
server.displayName: <%=server.displayName%>
server.domainName: <%=server.domainName%>
server.externalId: <%=server.externalId%>
server.externalIp: <%=server.externalIp%>
server.fqdn: <%=server.fqdn%>
server.hostname: <%=server.hostname%>
server.internalId: <%=server.internalId%>
server.internalIp: <%=server.internalIp%>
server.internalName: <%=server.internalName%>
server.internalSshUsername: <%=server.internalSshUsername%>
server.lastAgentUpdate: <%=server.lastAgentUpdate%>
server.lvmEnabled: <%=server.lvmEnabled%>
server.macAddress: <%=server.macAddress%>
server.managed: <%=server.managed%>
server.maxCores: <%=server.maxCores%>
server.maxMemory: <%=server.maxMemory%>
server.maxStorage: <%=server.maxStorage%>
server.name: <%=server.name%>
server.nodePackageVersion: <%=server.nodePackageVersion%>

(continues on next page)
4.7.4 Instance

instance {
    adminPassword,
    adminUsername,
    apps.[],
    assignedDomainName,
    autoScale,
    backup.[],
    configGroup,
    configId,
    configRole,
    container.[],
    containers.[]
}

cypher: <%=cypher.read('secret/' + zone.code)%> # Make variables more dynamic based off other variables
cores,
createBackup, true/false
createdByEmail,
createdByFirstName,
createdById,
createdByLastName,
createdByUser.
  username,
  displayName,
  firstName,
  lastName,
  email,
  linuxUsername,
  windowsUsername
},
createdByName,
creatorUser, # true/false
customOptions,
deployGroup,
description,
displayName,
domainName,
environmentPrefix,
evars:()
, expireDate, # YYYY-MM-DD-T00:00:00Z
expireDays,
expose.[],
firewallEnabled:true/false,
hid,
hidname,
id,
instanceContext,
inключенLevel,
inключенTypeCode,
inключенTypeName,
inключенVersion,
isEC2:true/false,
isVpcSelectible, # true/false
layoutCode,
layoutId,
layoutName,
layoutSize,
lbInstances[],
memory(bytes),
memoryDisplay, # MB/GB
metadata()
, name,
nestedVirtualization,
networkLevel,
noAgent,
plan,
poolProviderType,
ports,
provisionType,
resourcePoolId,
scheduleStatus,
servicePassword,
serviceUsername,
smbiosAssetTag,
sslCertId,
sslEnabled, # true/false
status,
statusMessage,
storage, # bytes
tags,
userStatus,
vmwareFolderId,
}

4.7.5 Container

container {
    configGroup,
    configId,
    configPath,
    configRole,
    containerTypeCode,
    containerTypeShortName,
    cores,
    dataPath,
    dateCreated,
    domainName,
    environmentPrefix,
    externalIp,
    hostMountPoint,
    hostname,
    image,
    internalHostname,
    internalIp,
    logsPath,
    memory,
    planCode,
    provisionType,
    server:{},
    serverId,
    sshHost,
    status,
    storage,
    version,
    containerTypeName
}
4.7.6 Server

```yaml
server {
  agentInstalled,
  agentVersion,
  apiKey,
  category,
  commType,
  configGroup,
  configId,
  configRole
  consoleHost,
  consolePort,
  consoleType,
  consoleUsername,
  dataDevice,
  dateCreated,
  description,
  displayName,
  domainName,
  externalId,
  externalIp,
  fqdn,
  hostname,
  internalId,
  internalIp,
  internalName,
  internalSshUsername,
  lastAgentUpdate,
  lvmEnabled,
  macAddress,
  managed,
  maxCores,
  maxMemory,
  maxStorage,
  name,
  nodePackageVersion,
  osDevice,
  osType,
  osTypeCode,
  parentServerId,
  plan,
  platform,
  platformVersion,
  powerState,
  serialNumber,
  serverModel,
  serverType,
  serverTypeCode,
  serverTypeName,
  serverVendor,
  softwareRaid,
  sourceImageId,
  sshHost,
  sshPort,
  sshUsername,
  status,
}```
statusMessage, tags, toolsInstalled, visibility, volumes {
  name
  id
deviceName
  maxStorage
  unitNumber
displayOrder
  rootVolume
}

### 4.7.7 Zone (Cloud)

```
zone {
  agentMode,
cloudTypeCode,
cloudTypeName,
  code,
datacenterId,
domainName,
  firewallEnabled,
  location,
  name,
  regionCode,
scalePriority
}
```

### 4.7.8 Group (Site)

```
group {
  code,
  location,
  datacenterId,
  name
}
```

### 4.7.9 Custom Options (Inputs)

```
customOptions {
  customOptions.fieldName
}
```
4.7.10 Global

ex: `<%= morpheus.user.id %>`

```
"morpheus":{
  "user":{
    "id":value,
    "account":{
      "id":value
    },
    "username":"value",
    "displayName":"value",
    "email":"value",
    "firstName":"value",
    "lastName":"value",
    "dateCreated":0000-00-00T00:00:00Z,
    "lastUpdated":0000-00-00T00:00:00Z,
    "enabled":true/false,
    "accountExpired":true/false,
    "accountLocked":false,
    "passwordExpired":false,
    "defaultGroupId":value,
    "defaultZoneId":value,
    "hasLinuxUser":true/false,
    "hasWindowsUser":true/false,
    "role":{
      "id":value
    },
    "instanceLimits":value
  }
}
```

4.7.11 User

```
'user': {'accountId': int,
  'attributes': {samlAttributes},
  'displayName': 'string',
  'email': 'string',
  'firstName': 'string',
  'id': int,
  'lastName': 'string',
  'linuxUsername': 'string',
  'username': 'string',
  'windowsUsername': 'string',
}
```
4.7.12 Script Variables Example

Below is an example of the variables available to a script running against an Instance context.

Note: Variable maps are determined by context, configurations and permissions, actual maps may contain additional or fewer options.

```json
'account': 'string',
'accountId': int,
'accountType': 'string',
'allowExisting': boolean,
'apps': [{
'description': 'string',
'id': int,
'name': 'string',
'cloud': 'string',
'cloudCode': 'string',
'cloudName': 'string',
'container': { 'allowExisting': boolean,
  'certificatePath': string,
  'certificateStyle': string,
  'changeManagementExtId': int,
  'changeManagementServiceId': int,
  'cloud': 'string',
  'cloudConfig': { 'agentInstall': agentInstallScript,
    'finalizeServer': finalizeServerScript,
    'meta': metaData,
    'user': userData},
  'configGroup': int,
  'configId': int,
  'configPath': 'string',
  'configRole': int,
  'containerTypeCategory': 'string',
  'containerTypeCode': 'string',
  'containerTypeName': 'string',
  'containerTypeShortName': 'string',
  'cores': int,
  'coresPerSocket': int,
  'createUser': boolean,
  'customOptions': { 'morph_ver': 'string',
    'dataPath': 'string',
    'dateCreated': 'string',
    'domainName': 'string',
    'environmentPrefix': 'string',
    'evars': {},
    'expireDays': 'string',
    'expose': ['string'],
    'exposedPorts': [[
      'loadBalanceProtocol': 'string',
      'name': 'string',
      'port': int]],
    'externalIp': 'string',
    'externalPort': int,
    'hostMountPoint': 'string',
    'hostName': 'string',
    'hostname': 'string',
    'hosts': [{ 'containerName': 'string',
```
`protocol': 'string',
 'visible': boolean},
 'provisionType': 'string',
 'publicKeyId': int,
 'server': [],
 'serverId': int,
 'shutdownDays': 'string',
 'site': {'accountId': int,
   'active': boolean,
   'id': int,
   'integrations': [],
   'location': 'string',
   'name': 'string',
   'visibility': 'string',
   'zones': []},
 'sshHost': 'string',
 'status': 'string',
 'storage': int,
 'storageController': int,
 'type': 'string',
 'userGroup': {'id': '',
 'version': 'string',
 'vm': boolean,
 'volumes': [{'datastoreId': int,
   'id': int,
   'maxIOPS': int,
   'maxStorage': int,
   'name': 'string',
   'rootVolume': boolean,
   'size': int,
   'storageType': int,
   'vId': int}]
  }
  },
 'containerName': 'string',
 'coresPerSocket': int,
 'createUser': boolean,
 'customOptions': {'morph_ver': 'string',
   'deployOptions': {},
   'evars': {},
   'expireDays': 'string',
   'expose': ['string'],
   'exposedPorts': [{'loadBalanceProtocol': 'string',
     'name': 'string',
     'port': int}],
 'externalIp': 'string',
 'group': {'code': 'string',
   'configCmdId': 'string',
   'configManagementId': 'string',
   'datacenterId': int,
   'dnsIntegrationId': 'string',
   'location': 'string',
   'name': 'string',
   'serviceRegistryId': 'string',
   'groupCode': 'string',
   'groupName': 'string',
   'host': '',
   'hostMountPoint': 'string',
   'hostName': 'string',
   '}
'hosts': {}
'input': {'backup': {
  'cloud': {},
  'computedHostName': 'string',
  'computedName': 'string',
  'copies': int,
  'domainOptions': {},
  'environmentVariables': {},
  'executionId': int,
  'expireDays': int,
  'group': {},
  'hostName': 'string',
  'instanceContext': 'string',
  'layout': {},
  'metadata': {},
  'name': 'string',
  'plan': {},
  'powerScheduleType': int,
  'securityGroups': {},
  'shutdownDays': int,
  'type': 'string',
  'version': 'string'},
'instance': {'adminPassword': 'maskedString',
  'adminUsername': 'string',
  'allowExisting': bool,
  'apps': [],
  'assignedDomainName': 'string',
  'autoScale': bool,
  'backup': {'backupRepository': int,
    'createBackup': bool,
    'enabled': bool,
    'jobAction': 'string',
    'jobRetentionCount': 'string',
    'providerBackupType': int,
    'showScheduledBackupWarning': bool},
  'cloud': 'string',
  'cloudConfig': {'agentInstall': agentInstallScript,
    'finalizeServer': finalizeServerScript,
    'meta': meta, 'user': userData},
  'configGroup': int,
  'configId': int,
  'configRole': int,
  'container': {},
  'containers': [],
  'cores': int,
  'createBackup': bool,
  'createUser': bool,
  'createdByEmail': 'string',
  'createdByFirstName': 'string',
  'createdById': int,
  'createdByLastEmail': 'string',
  'createdByFirstName': 'string',
  'createdById': int,
  'createdByLastName': 'string',
  'createdByUser': {'accountId': int,
    'displayName': 'string',
    'email': 'string',
    'firstName': 'string',
...}
'id': int,
'lastName': 'string',
'linuxUsername': 'string',
'username': 'string',
'windowsUsername': 'string',
'createdByUsername': 'string',
'customOptions': {'morph_ver': 'string',
'deployGroup': ,
'description': 'string',
'displayName': 'string',
'domainName': 'string',
'environemntPrefix': 'string',
'evars': {},
'expireDate': date,
'expireDays': 'string',
'expose': ['string'],
'firewallEnabled': boolean,
'hostName': 'string',
'hostname': 'string',
'id': int,
'instanceContext': 'string',
'instanceLevel': 'string',
'instanceType': {'code': 'string',
'instanceTypeCode': 'string',
'instanceTypeName': 'string',
'instanceVersion': 'string',
'layout': {'code': 'string',
'id': int},
'layoutCode': 'string',
'layoutId': int,
'layoutName': 'string',
'lbInstances': [{'balanceMode': 'string',
'enabled': boolean,
'externalAddress': 'string',
'id': int,
'instanceId': int,
'loadBalancer': {'id': int},
'loadBalancerId': int,
'name': 'string',
'port': int,
'protocol': 'string',
'sslCert': 'string',
'sslRedirectMode': 'string',
'sticklyMode': 'string',
'vipAddress': 'string',
'vipDirectAddress': 'string',
'vipHostname': 'string',
'vipName': 'string',
'vipPort': int,
'vipProtocol': 'string',
'vipScheme': 'string',
'vipShared': 'string',
'loadBalancerId': int,
'memory': int,
'memoryDisplay': 'string',
'metadata': {'ver': 'string',
'name': 'string',
'loadBalancerId': int,
'memory': int,
'memoryDisplay': 'string',
'metadata': {'ver': 'string',
'name': 'string',
(continues on next page)
networkLevel': 'string',
'plan': 'string',
'ports': {},
'powerScheduleType': ,
'provisionType': 'string',
'scheduleStatus': 'string',
'servicePassword': 'maskedString',
'serviceUsername': 'string',
'shutdownDays': 'string',
'site': {'accountId': int,
    'active': boolean,
    'id': int,
    'integrations': [],
    'location': 'string',
    'name': 'string',
    'visibility': 'string',
    'zones': [{},]
'sslCertId': int,
'sslEnabled': boolean,
'status': 'string',
'statusMessage': 'string',
'storage': int,
'tags': 'string',
'type': ,
'userGroup': {'id': 'string',
    'userStatus': 'string',
'instanceContext': 'string',
'instanceType': '{'code': 'string',
    'internalIp': 'string',
    'isDocker': boolean,
    'layout': {'code': 'string',
        'localScriptGitId': int,
        'localScriptGitRef': 'string',
        'logTag': 'string',
        'maxCores': int,
        'maxCpu': int,
        'maxMemory': int,
        'maxStorage': int,
    'memoryDisplay': 'string',
'morpheus': {'apiAccessToken': 'string',
    'applianceHost': 'string',
    'appliancePort': 'string',
    'applianceScheme': 'string',
    'applianceSsl': boolean,
    'applianceUrl': 'string',
'morpheusUser': 'string',
'mounts': [],
'name': 'string',
'networkId': int,
'networkInterfaces': [{'id': 'string',
    'ipAddress': 'string',
    'ipMode': 'string',
    'network': {'dhcpServer': ,
        'group': int,
        'id': int,
        'name': 'string',
        'pool': int},
4.7. Variables 275
'networkInterfaceTypeId': int,

'noAgent': boolean,
'platform': 'string',
'port': int,
'ports': [{'code': 'string',
    'displayName': 'string',
    'export': boolean,
    'exportName': 'string',
    'external': int,
    'index': int,
    'internal': int,
    'link': boolean,
    'loadBalance': boolean,
    'primaryPort': boolean,
    'protocol': 'string',
    'visible': boolean}],

'provisionType': 'string',
'publicKeyId': int,
'pythonAdditionalPackages': ,
'pythonArgs': ,
'pythonBinary': 'string',
'pythonScript': ,
'results': {},
'sequence': int,
'server': {'agentInstalled': boolean,
    'agentVersion': 'string',
    'apiKey': 'string',
    'category': ,
    'cloudConfig': {'agentInstall': agentInstallScript,
        'finalizeServer': finalizeServerScript,
        'meta': metaData,
        'user': userData
    },
    'commType': 'string',
    'computeTypeCode': 'string',
    'computeTypeName': 'string',
    'configGroup': int,
    'configId': int,
    'configRole': 'string',
    'consoleHost': 'string',
    'consolePort': int,
    'consoleType': 'string',
    'consoleUsername': 'string',
    'createdAtUser': {'accountId': int,
        'displayName': 'string',
        'email': 'string',
        'firstName': 'string',
        'id': int,
        'lastName': 'string',
        'linuxUsername': 'string',
        'username': 'string',
        'windowsUsername': 'string',
    },
    'dataDevice': 'string',
    'dateCreated': 'string',
    'description': 'string',
    'displayName': 'string',
    'domainName': 'string',

(continues on next page)
'externalId': 'string',
'externalIp': 'string',
'fqdn': 'string',
'hostname': 'string',
'id': int,
'interfaces': [{'dhcp': boolean,
'domain': {'fqdn': 'string',
'name': 'string',
'ouPath': 'string'},
'interfaceId': int,
'ipAddress': 'string',
'ipMode': 'string',
'ipSubnet': 'string',
'ipv6Address': 'string',
'ipv6Subnet': 'string',
'macAddress': 'string',
'network': {'cidr': 'string',
'cidrMask': 'string',
'gateway': 'string',
'name': 'string',
'netmask': 'string',
'vlanId': int},
'networkPosition': 'string',
'vlanId': int}
]
,'internalId': int,
'internalIp': 'string',
'internalName': 'string',
'internalSshUsername': 'string',
'lastAgentUpdate': 'string',
lvmEnabled': boolean,
'macAddress': 'string',
'managed': boolean,
'maxCores': int,
'maxMemory': int,
'maxStorage': int,
'name': 'string',
'nodePackageVersion': 'string',
'osDevice': 'string',
'osPassword': 'maskedString',
'osType': 'string',
'osTypeCode': 'string',
'osUsername': 'string',
'parentServerId': int,
'plan': 'string',
'platform': 'string',
'platformVersion': 'string',
'powerScheduleType': ,
'powerState': 'string',
'publicKeyId': int,
'serialNumber': 'string',
'serverModel': 'string',
'serverType': 'string',
'serverTypeCode': 'string',
'serverTypeName': 'string',
'serverVendor': 'string',
'softwareRaid': boolean,
'sourceImageId': int,
{'sshHost': 'string',
'sshPort': int,
'sshUsername': 'string',
'status': 'string',
'statusMessage': 'string',
'tags': [],
toolsInstalled': boolean,
'tagsInstalled': int,
uuid': 'string',
'visibility': 'string',
'veolumes': [{'deviceName': 'string',
'displayOrder': int,
'id': int,
'maxStorage': int,
'name': 'string',
'rootVolume': boolean,
'unitNumber': 'string'},

'serverId': 'string',
'serverName': 'string',
'shutdownDays': 'string',
'site': {'accountId': int,
'active': boolean,
'id': int,
'integrations': [],
'location': 'string',
'name': 'string',
'visibility': 'string',
'zones': []},

'sshKey': 'string',
'state': {},
'storageController': int,
'tenant': 'string',
'tenantId': int,
'tenantSubdomain': 'string',
'type': 'string',
'user': {'accountId': int,
'attributes': {samlAttributes},
'displayName': 'string',
'email': 'string',
'firstName': 'string',
'id': int,
'lastName': 'string',
'linuxUsername': 'string',
'username': 'string',
'windowsUsername': 'string',
'userGroup': {'id': 'string',
'userId': int,
'userInitials': 'string',
'username': 'string',
'vm': boolean,
'veolumes': [{'datastoreId': int,
'id': int,
'maxIOPS': int,
'maxStorage': int,
'name': 'string',
'rootVolume': boolean,
'size': int,

(continues on next page)
'storageType': int,
'vId': int],
'zone': {'agentMode': 'string',
'cloudTypeCode': 'string',
'cloudTypeName': 'string',
'code': 'string',
'datacenterId': int,
'domainName': 'string',
'firewallEnabled': boolean,
'location': 'string',
'name': 'string',
'regionCode': 'string',
'scalePriority': int))

Note: Variable maps are determined by context, configurations and permissions, actual maps may contain additional or fewer options.

4.7.13 Spec Template Variables
The heart of Morpheus is the ability to manage provisioning across any infrastructure, from bare metal to virtualized clouds and all the way to public infrastructure.

5.1 Groups

5.1.1 Overview

Groups in Morpheus define what resources a user has access to. Group access is defined by User Roles. Clouds are added to groups, and a User can only access the Clouds that are in the Groups their Role(s) gives them access to. Resources such as Networks, Datastores, Resources Pools, and Folders have additional Group access settings. Policies applied to a Group will be enforced on all Instances provisioned or moved into that Group.

Note: Groups are not multi-tenant. A group only exists in the tenant it is created in.

The Groups view displays all current groups, includes search feature, and also enables the addition of new groups.

To View Groups:

1. Select the Infrastructure link in the navigation bar
2. Click the Groups link

5.1.2 UI

1. Select the Infrastructure link in the navigation bar
2. Click the Groups link

5.1.3 CLI

View all groups: `groups list`
To use the group: `groups use <id>` or `groups use "group name"`
Json output of a specific group: `groups get <id> -j` or `groups get "group name" -j`
5.1.4 API

View all groups: `curl https://api.gomorpheus.com/api/groups -H "Authorization: BEARER access_token"`
View a specific group: `curl https://api.gomorpheus.com/api/groups/:id -H "Authorization: BEARER access_token"

5.1.5 Adding Groups

To add a group:

1. Select the Infrastructure link in the navigation bar
2. Click the Groups link
3. Click the Create Group button
4. Input out the Name and Location (optional) fields
5. Click the Save Changes button to save
5.1.6 Managing Groups

To view a Group:

1. Select the Infrastructure link in the navigation bar
2. Click the Groups link
3. Click the Group name to view/modify

Available tabs in group view

Hosts  Lists available hosts in the group and displays power, os, name, type, cloud, ip address, nodes, disc space, memory, and status. You can add a host from this tab panel by clicking Add Host.

Virtual Machines  List all Virtual Machines in the Group.

Bare Metal  List all Bare Metal Hosts added to the Group

Clouds  Lists Clouds added to the Group. Existing Clouds or new Clouds can be added from the Group by clicking Add Cloud.

Policies  Lists and allows creation or management of Policies applied to the Group.
5.1.7 Edit Group

To edit a group:

1. Select the Infrastructure link in the navigation bar.
2. Click the Groups link.
3. Click the name of the group you wish to edit.
4. Click the Edit button.
5. From the Edit Group Wizard modify information as needed.
6. Click the Save Changes button to save.

5.1.8 Delete Group

To delete a group:

1. Select the Infrastructure link in the navigation bar.
2. Click the Groups link.
3. Click the name of the group you wish to delete.
4. Click the Delete button.
5. Confirm

5.1.9 User Access

**Important:** User access to Groups is determined by their user Role(s). Group access for Roles can be configured in the Group Access section of a Roles Settings.

5.2 Clouds

5.2.1 Overview

Clouds are integrations or connections to public, private, hybrid clouds, or bare metal servers. Clouds can belong to many groups and contain many hosts. The clouds view includes clouds status, statistics, tenant assignment, and provides the option to add, edit, delete new clouds. Morpheus supports most Public Clouds and Private Clouds.

**Supported Cloud Types**

- Alibaba Cloud
- Amazon
- Azure (Public)
- Azure Stack (Private)
- Cloud Foundry
• Dell (Cloud type for PXE and manually added Dell EMC Hosts)
• DigitalOcean
• Google Cloud
• HPE (Cloud type for PXE and manually added HPE Hosts)
• HPE OneView
• Huawei
• Hyper-V
• IBM Cloud
• IBM Cloud Platform
• Kubernetes
• MacStadium
• Morpheus (Generic Cloud type for PXE/Bare Metal and manually added Hosts)
• Nutanix
• Open Telekom Cloud
• OpenStack
• Oracle Public Cloud
• Oracle VM
• Platform 9
• SCVMM
• SoftLayer
• Supermicro (Cloud type for PXE and manually added Supermicro Hosts)
• UCS
• UpCloud
• VMWare ESXi
• VMware Fusion
• VMWare on AWS
• VMware vCenter
• VMware vCloud Air
• VMware vCloud Director
• XenServer

Information on each cloud type can be found in the Guides section.

5.2. Clouds
5.2.2 Creating Clouds

Clouds can be added from Infrastructure > Clouds or in Infrastructure > Groups > (select Group) > Clouds. Individual Guides for adding specific Cloud Types can be found in the Guides section.

5.2.3 Cloud Detail View

The Cloud Detail view shows metrics on health, sync status, current month costs, average monthly costs, resource utilization statistics, and resource counts for Container Hosts, Hypervisors, Bare Metal, Virtual Machines, and Unmanaged resources.

To view the Cloud List View, select the name of a Cloud to display the clouds Detail View.

**EDIT** Edit the setup configuration of the Cloud.

**REFRESH** Force a sync with the Cloud. Last sync date, time and duration is shown under the Cloud name.

**DELETE** Delete the Cloud from Morpheus

---

**Important:** All Instances and managed Hosts and VM’s associated with the Cloud must be removed prior to deleting a cloud.
Cloud Detail Tabs

**Note:** Not all tabs are available for all Cloud Types.

**Clusters** The Clusters tab displays clusters provisioned into the Cloud being viewed, including their status, type, name, layout, workers, and compute, memory, and storage stats. You can add a cluster by clicking *ADD CLUSTER*.

**Hosts**

The Hosts tab displays available hosts in the Cloud and displays power, OS, name, type, cloud, IP address, nodes, disk space, memory, and status. You can add a resource by clicking *ADD RESOURCE*, add a hypervisor host by clicking *ADD HYPervisor*, or perform action an action by selecting one or more Hosts and clicking *ACTIONS*.

**VMs** Displays an inventory of existing Instances in your Cloud configuration and provides details such as power, OS, name, type, cloud, IP address, nodes, disk space, memory, and status.

**Bare Metal** Setup PXE Boot in the Boot section to add bare metal servers. Once set up you can view information such as power, OS, name, type, cloud, IP address, nodes, disk space, memory, and status.

**Security Groups** The Security Groups tab displays a list of existing security groups in the cloud. You can add a security group to this cloud by clicking *EDIT SECURITY GROUPS*.

**Load Balancers** The load balancers tab panel displays available load balancers in the cloud including the name, description, type, cloud and host. You can add a load balancer from this tab by clicking *ADD LOAD BALANCER*.

**Networks** Displays Networks synced or added to the Cloud, including their name, type, CIDR, pool, DHCP status, visibility and targeted Tenant.

**Data Stores** Displays Datastores synced or added to the Cloud, including their name, type, capacity, online status, visibility, and targeted Tenant.

**Resources** Displays Resource Pools synced from the Cloud, including their name, description, and targeted Tenant.

**Policies** Manages Policies enforced on the Cloud. Setting a policy on this tab is equal to creating a policy in Administration > Policies and scoping it to the selected Cloud.

**Profiles** Manages Terraform, Key/Value Profiles that create custom object associated secrets and metadata that will automatically be mapped per Cloud selection during provisioning and automation.

### 5.2.4 Deleting Clouds

To delete a cloud:

1. Select the Infrastructure link in the navigation bar.
2. Select the Clouds link in the sub navigation bar.
3. Click the Delete icon of the cloud to delete.

**Important:** All Instances, managed Hosts and VMs must be removed prior to deleting a Cloud. To remove Instances, hosts and VMs from Morpheus without deleting the Cloud resources they represent, select Delete on the host or VM, unselect “Remove Infrastructure”, and select “Remove Associated Instances” if Instance are associated with the selected Hosts or VMs.
5.2.5 Cloud Profiles

Role Permissions

Access to Profiles tab is determined by the following role permissions:

Role: Feature Access: Admin: Profiles

- None: Cannot access Profiles tab or create/view/edit/delete profiles
- Read: Can access Profiles tab, can view profiles, cannot create/edit/delete profiles
- Full: Can access Profiles tab, can create/view/edit/delete profiles

Terraform Profiles

- Terraform Profiles allow created cloud associated tfvars secrets, allowing tf apps and specs to be provisioned across multiple clouds that required different tfvars.
- Target Cloud Terraform Profiles are automatically mapped to tf apps/specs during provisioning, no scoping is required.
- Terraform Profiles are encrypted in Cypher and creating a profile creates a Cypher with key tf-vars/profile/cloud/$cloudCode/variables
- Terraform Profiles can be edited after creation
- Terraform Profiles are limited to one per Cloud

Create a Terraform Profile

1. Navigate to /infrastructure/clouds/ and select a Cloud
2. Select the Profiles tab
3. Select + ADD PROFILE
4. Select Terraform Profile Type
5. Enter tfvars in the Terraform Profile Variables field
   - example Terraform Profile Variables
     
     ```
     access_key="****acccessKey****"
     secret_key="********secretKey**********"
     region="us-west-1"
     ```
6. Select SAVE CHANGES

Now when provisioning a terraform Instance or App to the Cloud the profile was created in, the tfvars in the profile become available to the tf.
Key/Value Store Profiles

- Key/Value Profiles (Key/Value Store) expand provisioning, automation, billing and reporting capabilities by allowing dynamic custom object specific metadata in provisioning and automation mappings
- Key/Value Profile entries are available using `<%=cloud.profile.key%>`
- Terraform Profiles are limited to one Profile per Cloud, however multiple key/value pairs can be added to a single profile

Create a Key/Value Profile

1. Navigate to `/infrastructure/clouds/` and select a Cloud
2. Select the Profiles tab
3. Select + ADD PROFILE
4. Select Key/Value Profile Type
5. Enter key/value entries, selecting + to add additional entries
6. Select SAVE CHANGES

5.3 Clusters

5.3.1 Overview

`Infrastructure > Clusters` is for creating and managing Kubernetes Clusters, Morpheus manager Docker Clusters, KVM Clusters, or Cloud specific Kubernetes services such as EKS, AKS and GKE. The Combo Cluster is a combination Docker and KVM Cluster.
Cluster Types

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Provider Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kubernetes Cluster</td>
<td>Provisions by default a Kubernetes cluster consisting of 1 Kubernetes Master and 3 Kubernetes Worker nodes. Additional system layouts available including Master clusters. Custom layouts can be created.</td>
<td>Kubernetes</td>
</tr>
<tr>
<td>Docker Cluster</td>
<td>Provisions by default a Morpheus controlled Docker Cluster with 1 host. Additional hosts can be added. Custom layouts can be created. Existing Morpheus Docker Hosts are automatically converted to Clusters upon 4.0.0 upgrade.</td>
<td>Docker</td>
</tr>
<tr>
<td>EKS Cluster</td>
<td>Amazon EKS (Elastic Kubernetes Service) Clusters</td>
<td>Kubernetes</td>
</tr>
<tr>
<td>AKS Cluster</td>
<td>Azure AKS (Azure Kubernetes Service) Clusters</td>
<td>Kubernetes</td>
</tr>
<tr>
<td>KVM Cluster</td>
<td>Provisions by default a Morpheus controlled KVM Cluster with 1 host. Additional hosts can be added. Custom layouts can be created. Existing Morpheus KVM Hosts are automatically converted to Clusters upon 4.0.0 upgrade.</td>
<td>KVM</td>
</tr>
<tr>
<td>Combo Cluster</td>
<td>Provisions by default a Morpheus controlled Docker, VM and Functions* Cluster with 1 host. Additional hosts can be added.</td>
<td>Docker &amp; KVM</td>
</tr>
<tr>
<td>Ext Kubernetes</td>
<td>Brings an existing (brownfield) Kubernetes cluster into Morpheus</td>
<td>Kubernetes</td>
</tr>
<tr>
<td>GKE Cluster</td>
<td>Google Cloud GKE (Google Kubernetes Engine) Clusters</td>
<td>Kubernetes</td>
</tr>
</tbody>
</table>

Note: Refer to System Cluster Layouts for supported Clouds per Cluster Type.

5.3.2 Requirements

- Morpheus Role permission Infrastructure: Clusters > Full required for Viewing, Creating, Editing and Deleting Clusters.
- Morpheus Role permission Infrastructure: Clusters > Read required for Viewing Cluster list and detail pages.

5.3.3 Cluster Permissions

- Cluster Permissions Each Cluster has Group, Tenant and Service Plan access permissions settings (“MORE” > Permissions on the Clusters list page).
- Namespace Permissions Individual Namespaces also have Group, Tenant and Service Plan access permissions settings
5.3.4 System Cluster Layouts

System (Morpheus provided) Cluster Layouts at time of v5.3.4 release. Note: AKS & GKE Kubernetes versions will dynamically update to the providers supported versions.

<table>
<thead>
<tr>
<th>name</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alibaba Docker Host</td>
<td>This will provision a single docker host vm in alibaba</td>
</tr>
<tr>
<td>Amazon Docker Host</td>
<td>This will provision a single docker host vm in amazon</td>
</tr>
<tr>
<td>Azure Docker Host</td>
<td>This will provision a single docker host vm in azure</td>
</tr>
<tr>
<td>Copy of MKS Kubernetes 1.20 Cluster on Ubuntu 18.04</td>
<td>provision a kubernetes 1.20 cluster on ubuntu 18.04</td>
</tr>
<tr>
<td>Copy of VMware Docker CentOS 7.5</td>
<td>This will provision a single docker host vm in vmware</td>
</tr>
<tr>
<td>Digital Ocean Docker Host</td>
<td>This will provision a single docker host vm in digitalOcean</td>
</tr>
<tr>
<td>Docker Cluster on Ubuntu 18.04</td>
<td>provision a docker cluster on ubuntu 18.04 in fusion</td>
</tr>
<tr>
<td>Docker on Bare Metal</td>
<td>This will provision a single docker host</td>
</tr>
<tr>
<td>Docker on Linux</td>
<td>This will add a single docker host</td>
</tr>
<tr>
<td>Docker on Ubuntu 16.04</td>
<td>This will provision a single docker host vm in fusion</td>
</tr>
<tr>
<td>ESXi Docker Host</td>
<td>This will provision a single docker host vm in esxi</td>
</tr>
<tr>
<td>External Kubernetes 1.20</td>
<td>Connect to an external kubernetes cluster</td>
</tr>
<tr>
<td>External Kubernetes 1.21</td>
<td>Connect to an external kubernetes cluster</td>
</tr>
<tr>
<td>Google Docker Host</td>
<td>This will provision a single docker host vm in google</td>
</tr>
<tr>
<td>Huawei Docker Host</td>
<td>This will provision a single docker host vm in huawei</td>
</tr>
<tr>
<td>Hyper-V Docker Host</td>
<td>This will provision a single docker host vm in hyperv</td>
</tr>
<tr>
<td>IBM Docker Host</td>
<td>This will provision a single docker host vm in bluemix</td>
</tr>
<tr>
<td>Kubernetes 1.19.11 Cluster AKS</td>
<td>This provisions a single kubernetes master in Azure</td>
</tr>
<tr>
<td>Kubernetes 1.19.13 Cluster AKS</td>
<td>This provisions a single kubernetes master in Azure</td>
</tr>
<tr>
<td>Kubernetes 1.20 Cluster EKS</td>
<td>This will provision a single kubernetes master in amazom with weave and openebs</td>
</tr>
<tr>
<td>Kubernetes 1.20.7 Cluster AKS</td>
<td>This provisions a single kubernetes master in Azure</td>
</tr>
<tr>
<td>Kubernetes 1.20.9 Cluster AKS</td>
<td>This provisions a single kubernetes master in Azure</td>
</tr>
<tr>
<td>Kubernetes 1.21.1 Cluster AKS</td>
<td>This provisions a single kubernetes master in Azure</td>
</tr>
<tr>
<td>Kubernetes 1.21.2 Cluster AKS</td>
<td>This provisions a single kubernetes master in Azure</td>
</tr>
<tr>
<td>Kubernetes Cluster GKE</td>
<td>This will provision a single kubernetes master in google</td>
</tr>
<tr>
<td>KVM on CentOS 7.5</td>
<td>This will provision a single kvm host vm in fusion</td>
</tr>
<tr>
<td>KVM on CentOS 7.5</td>
<td>This will provision a single kvm host vm in vmware</td>
</tr>
<tr>
<td>KVM on Ubuntu 16.04</td>
<td>This will provision a single kvm host vm in fusion</td>
</tr>
<tr>
<td>KVM on Ubuntu 16.04</td>
<td>This will provision a single kvm host vm in fusion</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 Cluster on Ubuntu 18.04</td>
<td>provision a kubernetes 1.20 cluster on ubuntu 18.04</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 Cluster on Ubuntu 18.04</td>
<td>provision a kubernetes 1.20 cluster on ubuntu 18.04 in fusion</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 Cluster on Ubuntu 18.04</td>
<td>provision a kubernetes 1.20 cluster on ubuntu 18.04</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 Cluster on Ubuntu 18.04</td>
<td>provision a kubernetes 1.20 cluster on ubuntu 18.04 in hyperv</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 Cluster on Ubuntu 18.04</td>
<td>provision a kubernetes 1.20 cluster on ubuntu 18.04 in manual</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 Cluster on Ubuntu 18.04</td>
<td>provision a kubernetes 1.20 cluster on ubuntu 18.04</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 Cluster on Ubuntu 18.04</td>
<td>provision a kubernetes 1.20 cluster on ubuntu 18.04 in opentelekom</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 Cluster on Ubuntu 18.04</td>
<td>provision a kubernetes 1.20 cluster on ubuntu 18.04 in Openstack</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 Cluster on Ubuntu 18.04</td>
<td>provision a kubernetes 1.20 cluster on ubuntu 18.04 in scvmm</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 Cluster on Ubuntu 18.04</td>
<td>provision a kubernetes 1.20 cluster on ubuntu 18.04 in vmware</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 Cluster on Ubuntu 18.04</td>
<td>provision a kubernetes 1.20 cluster on ubuntu 18.04 in Huawei</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 Cluster on Ubuntu 20.04</td>
<td>provision a kubernetes 1.20 cluster on ubuntu 18.04 in xen</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 HA Cluster on Ubuntu 18.04</td>
<td>provision a high availability kubernetes 1.20 cluster on ubuntu 18.04</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 HA Cluster on Ubuntu 18.04</td>
<td>provision a high availability kubernetes 1.20 cluster on ubuntu 18.04 in Openstack</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 HA Cluster on Ubuntu 18.04</td>
<td>provision a high availability kubernetes 1.20 cluster on ubuntu 18.04 in hyperv</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 HA Cluster on Ubuntu 18.04</td>
<td>provision a high availability kubernetes 1.20 cluster on ubuntu 18.04 in manual</td>
</tr>
</tbody>
</table>
5.3.5 Kubernetes Clusters

Requirements

- Agent installation is required for Master and Worker Nodes. Refer to *Morpheus Agent* section for additional information.

- Access to Cloud Front, Image copy access and permissions for System and Uploaded Images used in Cluster Layouts
  Image(s) used in Cluster Layouts must either exist in destination cloud/resource or be able to be copied to destination by Morpheus, typically applicable for non-public clouds. For the initial provision, Morpheus System Images are streamed from Cloud Front through Morpheus to target destination. Subsequent provisions clone the local Image.

- System Kubernetes Layouts require Master and Worker nodes to access to the following over 443 during K8s install and configuration:
  - Morpheus Appliance url (443)
  - https://packages.cloud.google.com
  - https://storage.googleapis.com
  - https://docs.projectcalico.org
  - https://openebs.github.io
  - https://cloud.weave.works

- Morpheus Role permission *Infrastructure*: Clusters > Full required for Viewing, Creating, Editing and Deleting Clusters.

- Morpheus Role permission *Infrastructure*: Clusters > Read required for Viewing Cluster list and detail pages.
Creating Kubernetes Clusters

Provisions a new Kubernetes Cluster in selected target Cloud using selected Layout.

System (Morpheus provided) Kubernetes Layouts at time of v5.3.4 release. Note: AKS & GKE Kubernetes versions will dynamically update to the providers supported versions.

<table>
<thead>
<tr>
<th>Cluster Type Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kubernetes Cluster GKE</td>
<td>This will provision a single kubernetes master in google</td>
</tr>
<tr>
<td>Kubernetes 1.20 Cluster EKS</td>
<td>This will provision a single kubernetes master in amazon with weave and openebs</td>
</tr>
<tr>
<td>Morpheus Kubernetes Manual Cluster</td>
<td>This will create a kubernetes manual (self-managed) cluster</td>
</tr>
<tr>
<td>Kubernetes 1.19.11 Cluster AKS</td>
<td>This provisions a single kubernetes master in Azure</td>
</tr>
<tr>
<td>Kubernetes 1.20.7 Cluster AKS</td>
<td>This provisions a single kubernetes master in Azure</td>
</tr>
<tr>
<td>Kubernetes 1.21.1 Cluster AKS</td>
<td>This provisions a single kubernetes master in Azure</td>
</tr>
<tr>
<td>Kubernetes 1.21.2 Cluster AKS</td>
<td>This provisions a single kubernetes master in Azure</td>
</tr>
<tr>
<td>Kubernetes 1.20.13 Cluster AKS</td>
<td>This provisions a single kubernetes master in Azure</td>
</tr>
<tr>
<td>Kubernetes 1.20.9 Cluster AKS</td>
<td>This provisions a single kubernetes master in Azure</td>
</tr>
<tr>
<td>MKS Kubernetes 1.21 Cluster on Ubuntu 20.04</td>
<td>provision a kubernetes 1.21 cluster on ubuntu 20.04 in fusion</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 Cluster on Ubuntu 20.04</td>
<td>provision a kubernetes 1.20 cluster on ubuntu 18.04 in xen</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 Cluster on Ubuntu 18.04</td>
<td>provision a kubernetes 1.20 cluster on ubuntu 18.04 in vmware</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 Cluster on Ubuntu 18.04</td>
<td>provision a kubernetes 1.20 cluster on ubuntu 18.04 in scvmm</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 Cluster on Ubuntu 18.04</td>
<td>provision a kubernetes 1.20 cluster on ubuntu 18.04 in opentelekom</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 Cluster on Ubuntu 18.04</td>
<td>provision a kubernetes 1.20 cluster on ubuntu 18.04 in Openstack</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 Cluster on Ubuntu 18.04</td>
<td>provision a kubernetes 1.20 cluster on ubuntu 18.04 in manual</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 Cluster on Ubuntu 18.04</td>
<td>provision a kubernetes 1.20 cluster on ubuntu 18.04 in hyperv</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 Cluster on Ubuntu 18.04</td>
<td>provision a kubernetes 1.20 cluster on ubuntu 18.04 in Huawei</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 Cluster on Ubuntu 18.04</td>
<td>provision a kubernetes 1.20 cluster on ubuntu 18.04 in fusion</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 Cluster on Ubuntu 18.04</td>
<td>provision a kubernetes 1.20 cluster on ubuntu 18.04</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 Cluster on Ubuntu 18.04</td>
<td>provision a kubernetes 1.20 cluster on ubuntu 18.04</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 Cluster on Ubuntu 18.04</td>
<td>provision a kubernetes 1.20 cluster on ubuntu 18.04</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 HA Cluster on Ubuntu 18.04</td>
<td>provision a high availability kubernetes 1.20 cluster on ubuntu 18.04 in vmware</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 HA Cluster on Ubuntu 18.04</td>
<td>provision a high availability kubernetes 1.20 cluster on ubuntu 18.04 in opentelekom</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 HA Cluster on Ubuntu 18.04</td>
<td>provision a high availability kubernetes 1.20 cluster on ubuntu 18.04 in Openstack</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 HA Cluster on Ubuntu 18.04</td>
<td>provision a high availability kubernetes 1.20 cluster on ubuntu 18.04 in manual</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 HA Cluster on Ubuntu 18.04</td>
<td>provision a high availability kubernetes 1.20 cluster on ubuntu 18.04 in hyperv</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 HA Cluster on Ubuntu 18.04</td>
<td>provision a high availability kubernetes 1.20 cluster on ubuntu 18.04</td>
</tr>
<tr>
<td>MKS Kubernetes 1.20 HA Cluster on Ubuntu 18.04</td>
<td>provision a high availability kubernetes 1.20 cluster on ubuntu 18.04</td>
</tr>
<tr>
<td>External Kubernetes 1.21</td>
<td>Connect to an external kubernetes cluster.</td>
</tr>
<tr>
<td>External Kubernetes 1.20</td>
<td>Connect to an external kubernetes cluster.</td>
</tr>
</tbody>
</table>

To create a new Kubernetes Cluster:

1. Navigate to Infrastructure > Clusters
2. Select + ADD CLUSTER
3. Select Kubernetes Cluster
4. Select a Group for the Cluster
5. Select *NEXT*

6. Populate the following:
   - **CLOUD** Select target Cloud
   - **CLUSTER NAME** Name for the Kubernetes Cluster
   - **RESOURCE NAME** Name for Kubernetes Cluster resources
   - **DESCRIPTION** Description of the Cluster
   - **VISIBILITY**
     - *Public* Available to all Tenants
     - *Private* Available to Master Tenant
   - **LABELS** Internal label(s)

7. Select *NEXT*

8. Populate the following:

   **Note:** VMware sample fields provided. Actual options depend on Target Cloud

---

**LAYOUT** Select from available layouts. System provided layouts include Single Master and Cluster Layouts.

**PLAN** Select plan for Kubernetes Master

**VOLUMES** Configure volumes for Kubernetes Master

**NETWORKS** Select the network for Kubernetes Master & Worker VM’s

**CUSTOM CONFIG** Add custom Kubernetes annotations and config hash

**CLUSTER HOSTNAME** Cluster address Hostname (cluster layouts only)

**POD CIDR** POD network range in CIDR format ie 192.168.0.0/24 (cluster layouts only)

**WORKER PLAN** Plan for Worker Nodes (cluster layouts only)

**NUMBER OF WORKERS** Specify the number of workers to provision

**LOAD BALANCER** Select an available Load Balancer (cluster layouts only)

**User Config**

- **CREATE YOUR USER** Select to create your user on provisioned hosts (requires Linux user config in Morpheus User Profile)
- **USER GROUP** Select User group to create users for all User Group members on provisioned hosts (requires Linux user config in Morpheus User Profile for all members of User Group)

**Advanced Options**

- **DOMAIN** Specify Domain override for DNS records
- **HOSTNAME** Set hostname override (defaults to Instance name unless an Active Hostname Policy applies)

9. Select *NEXT*

10. Select optional Workflow to execute

11. Select *NEXT*

12. Review and select *COMPLETE*
• The Master Node(s) will provision first.

• Upon successful completion of VM provision, Kubernetes scripts will be executed to install and configure Kubernetes.

**Note:** Access to the sites listed in the Requirements section is required from Master and Worker nodes over 443.

• After Master or Masters are successfully provisioned and Kubernetes is successfully installed and configured, the Worker Nodes will provision in parallel.

• **Provision status can be viewed:**
  - From the Status next to the Cluster in **Infrastructure > Clusters**
  - Status bar with eta and current step available on Cluster detail page, accessible by selecting the Cluster name from **Infrastructure > Clusters**

• All process status and history is available - From the Cluster detail page History tab, accessible by selecting the Cluster name from **Infrastructure > Clusters** and the History tab - From **Operations - Activity - History** - Individual process output available by clicking i on target process.

13. Once all Master and Worker Nodes are successfully provisioned and Kubernetes is installed and configured, the Cluster status will turn green.

**Important:** Cluster provisioning requires successful creation of VMs, Agent Installation, and execution of Kubernetes workflows. Consult process output from **Infrastructure > Clusters - Details** and morpheus-ui current logs at **Administration - Health - Morpheus Logs** for information on failed Clusters.

---

**Intra-Kubernetes Cluster Port Requirements**

The table below includes port requirements for the machines within the cluster (not for the Morpheus appliance itself). Check that the following ports are open on Control-plane and Worker nodes:

**Table 3: Control-plane node(s)**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Direction</th>
<th>Port Range</th>
<th>Purpose</th>
<th>Used By</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>Inbound</td>
<td>6443</td>
<td>Kubernetes API Server</td>
<td>All</td>
</tr>
<tr>
<td>TCP</td>
<td>Inbound</td>
<td>6783</td>
<td>Weaveworks</td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>Inbound</td>
<td>2379-2380</td>
<td>etcd server client API</td>
<td>kube-apiserver, etcd</td>
</tr>
<tr>
<td>TCP</td>
<td>Inbound</td>
<td>10250</td>
<td>kubelet API</td>
<td>Self, Control plane</td>
</tr>
<tr>
<td>TCP</td>
<td>Inbound</td>
<td>10251</td>
<td>kube-scheduler</td>
<td>Self</td>
</tr>
<tr>
<td>TCP</td>
<td>Inbound</td>
<td>10252</td>
<td>kube-controller-manager</td>
<td>Self</td>
</tr>
</tbody>
</table>

**Table 4: Worker node(s)**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Direction</th>
<th>Port Range</th>
<th>Purpose</th>
<th>Used By</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>Inbound</td>
<td>10250</td>
<td>kubelet API</td>
<td>Self, Control plane</td>
</tr>
<tr>
<td>TCP</td>
<td>Inbound</td>
<td>30000-32767</td>
<td>NodePort Services</td>
<td>All</td>
</tr>
</tbody>
</table>

---

5.3. Clusters
Adding Worker Nodes

1. Navigate to Infrastructure – Clusters
2. Select MORE for the target cluster
3. Select ADD (type) Kubernetes Worker
   
   NAME Name of the Worker Node. Auto-populated with ${cluster.resourceName}-worker-${seq}
   
   DESCRIPTION Description of the Worker Node, displayed in Worker tab on Cluster Detail pages, and on Worker Host Detail page
   
   CLOUD Target Cloud for the Worker Node.

4. Select NEXT
5. Populate the following:

   Note: VMware sample fields provided. Actual options depend on Target Cloud

   SERVICE PLAN Service Plan for the new Worker Node
   
   NETWORK Configure network options for the Worker node.
   
   HOST If Host selection is enabled, optionally specify target host for new Worker node
   
   FOLDER
      
      Optionally specify target folder for new Worker node

      Advanced Options

      DOMAIN Specify Domain override for DNS records
      
      HOSTNAME Set hostname override (defaults to Instance name unless an Active Hostname Policy applies)

6. Select NEXT
7. Select optional Workflow to execute
8. Select NEXT
9. Review and select COMPLETE

Note: Ensure there is a default StorageClass available when using a Morpheus Kubernetes cluster with OpenEBS so that Kubernetes specs or HELM templates that use a default StorageClass for Persistent Volume Claims can be utilised.
Kubernetes Cluster Detail Pages

- Cluster status check results icon
- Name of the Cluster
- Last sync date, time and duration
- Edit, Delete and Actions buttons
  - Actions
    - Refresh
      - Sync the Cluster Status
    - Permissions  View and edit Cluster Group, Tenant and Service Plan Access
    - View API Token  Displays API Token for Cluster
    - View Kube Config  Displays Cluster Configuration
- Costs this month (to date, when Show Costing is enabled)
- Cluster resource utilization stats
- Counts for current Masters, Workers, Containers, Services, Jobs and Discovered Containers in the Cluster

SUMMARY

NAMESPACEs

WIKI

MASTERS

WORKERS

CONTAINERS

HISTORY

Kubernetes Cluster summary tab contains:
• More Cluster metadata including Name, Type, Created By, Worker CPU, Worker Memory (used/max), Worker Storage (used/max), Enabled: Yes/No, and Description.
• Memory chart with total Cluster Free and Used Memory over last 24 hours
• Storage chart with total Cluster Reserved and Used Storage over last 24 hours
• CPU chart with total Cluster CPU Utilization over last 24 hours
• IOPS Chart with total Cluster IOPS over last 24 hours
• IOPS Chart with total Cluster Network utilization over last 24 hours

---

```
Morpheus Documentation

298 Chapter 5. Infrastructure

---

```

---

```
vmwKubernetesCluster21
Last Updated By: Jeff Wheeler on 07/05/2019 10:48 PM

ADD IMPORTANT INFORMATION, NOTES, HOW-TO'S AND ANY OTHER INFO ABOUT YOUR CLUSTER TO THE WIKI PAGE.
All Wiki pages are also accessible under Operations -> Wiki with proper Role Permissions.

• API Token can be accessed via Actions -> View API Token
• Cluster Config can be accessed via Actions -> View Kube Config

---

```

---

```
To create a new Docker Cluster:

1. Navigate to Infrastructure > Clusters
2. Select + ADD CLUSTER
3. Select Docker Cluster
4. Populate the following:
Morpheus Documentation

CLOUD  Select target Cloud

CLUSTER NAME  Name for the Docker Cluster

RESOURCE NAME  Name for Docker Cluster resources

DESCRIPTION  Description of the Cluster

VISIBILITY
  Public  Available to all Tenants
  Private  Available to Master Tenant

LABELS  Internal label(s)

5. Select NEXT

6. Populate the following (options depend on Cloud Selection and will vary):

LAYOUT  Select from available layouts.

PLAN  Select plan for Docker Host

VOLUMES  Configure volumes for Docker Host

NETWORKS  Select the network for Docker Master & Worker VM’s

NUMBER OF HOSTS  Specify the number of hosts to be created

User Config

CREATE YOUR USER  Select to create your user on provisioned hosts (requires Linux user config in Morpheus User Profile)

USER GROUP  Select User group to create users for all User Group members on provisioned hosts (requires Linux user config in Morpheus User Profile for all members of User Group)

Advanced Options

DOMAIN  Specify Domain for DNS records

HOSTNAME  Set hostname (defaults to Instance name)

7. Select NEXT

8. Select optional Workflow to execute

9. Select NEXT

10. Review and select COMPLETE

5.3.7 EKS Clusters


Note:  EKS Cluster provisioning is different than creating a Kubernetes Cluster type in AWS EC2, which creates EC2 instances and configures Kubernetes, outside of EKS.

Morpheus currently supports EKS in the following regions: us-east-2, us-east-1, us-west-1, us-west-2, af-south-1, ap-east-1, ap-south-1, ap-northeast-3, ap-northeast-2, ap-southeast-1, ap-southeast-2, ap-northeast-1, ca-central-1, eu-central-1, eu-west-1, eu-west-2, eu-south-1, eu-west-3, eu-north-1, me-south-1, sa-east-1, us-gov-east-1, us-gov-west-1
Create an EKS Cluster

1. Navigate to Infrastructure - Clusters
2. Select + ADD CLUSTER
3. Select EKS Cluster
4. Populate the following:
   - **LAYOUT**  Select server layout for EKS Cluster
   - **PUBLIC IP**
     - **Subnet Default**  Use AWS configured Subnet setting for Public IP assignment
     - **Assigned EIP**  Assigned Elastic IP to Controller and Worker Nodes. Requires available EIP’s
   - **CONTROLLER ROLE**  Select Role for EKS Controller from synced role list
   - **CONTROLLER SUBNET**  Select subnet placement for EKS Controller
   - **CONTROLLER SECURITY GROUP**  Select Security Group assignment for EKS Controller
   - **WORKER SUBNET**  Select Subnet placement for Worker Nodes
   - **WORKER SECURITY GROUP**  Select Security Group assignment for Worker Nodes
   - **WORKER PLAN**  Select Service Plan (EC2 Instance Type) for Worker Nodes
   - **User Config**
     - **CREATE YOUR USER**  Select to create your user on provisioned hosts (requires Linux user config in Morpheus User Profile)
     - **USER GROUP**  Select User group to create users for all User Group members on provisioned hosts (requires Linux user config in Morpheus User Profile for all members of User Group)
   - **Advanced Options**
     - **DOMAIN**  Specify Domain for DNS records
     - **HOSTNAME**  Set hostname (defaults to Instance name)
5. Select NEXT
6. Select optional Workflow to execute
7. Select NEXT
8. Review and select COMPLETE

### 5.3.8 GKE Clusters


**Note:**  Ensure proper permissions exist for the Google Clouds service account to create, inventory and manage GKE clusters.
Create an GKE Cluster

1. Navigate to Infrastructure - Clusters
2. Select + ADD CLUSTER
3. Select GKE Cluster
4. Populate the following:
   - **CLOUD**  Select target Cloud
   - **CLUSTER NAME**  Name for the GKE Cluster
   - **RESOURCE NAME**  Name for GKE Cluster resources/hosts
   - **DESCRIPTION**  Description of the Cluster
   - **VISIBILITY**
     - **Public**  Available to all Tenants
     - **Private**  Available to Master Tenant
   - **LABELS**  Internal label(s)
   - **LAYOUT**  Select cluster layout for GKE Cluster
   - **RESOURCE POOL**  Specify an available Resource Pool from the selected Cloud
   - **GOOGLE ZONE**  Specify Region for the cluster
   - **VOLUMES**  Cluster hosts volume size and type
   - **NETWORKS**  Select GCP subnet(s) and config
   - **WORKER PLAN**  Service Plan for GKE worker nodes
   - **RELEASE CHANNEL**  Regular, Rapid, Stable or Static
   - **CONTROL PLANE VERSION**  Select from available synced GKE k8’s versions
   - **NUMBER OF WORKERS**  Number of worker nodes to be provisioned

5. Select NEXT
6. Select optional Workflow to execute
7. Select NEXT
8. Review and select COMPLETE

5.4 Compute

<table>
<thead>
<tr>
<th>Operations</th>
<th>Provisioning</th>
<th>Infrastructure</th>
<th>Backups</th>
<th>Logs</th>
<th>Monitoring</th>
<th>Tools</th>
<th>Administration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Groups</td>
<td>Clouds</td>
<td>Clusters</td>
<td>Compute</td>
<td>Network</td>
<td>Load Balancers</td>
<td>Storage</td>
<td>Keys &amp; Certs</td>
</tr>
</tbody>
</table>

**Note:** The Infrastructure Hosts page from previous versions has been renamed to Compute and updated with Container and Resource sections.

The *Infrastructure > Compute* section provides a universal stage for viewing and managing Hosts, Virtual Machines, Containers, Resources, and Bare Metal across Clouds.
In this section you can:

- View & Manage and Hosts, Virtual Machines, Containers, Resources, Bare Metal and Hypervisors
- Add manual Virtual Machines and Bare Metal Hosts
- Convert Hosts, Virtual Machines and Bare Metal to Managed

### 5.4.1 Hosts

**Section Features & Filters**

- Record
- Search
- Custom Views
- CSV Export
- JSON Export
- Paging
- Config

- Standard Filters: *OS Type*
- Advanced Filters: *Status Managed Server Type*

Hosts in Morpheus are Hypervisors and Container hosts that VMs and Containers are hosted on, such as ESXi Hosts and Kubernetes Master and Workers. These hosts are populated from integrated clouds, hosts and clusters provisioned from Morpheus, or manually added hosts.

Provisioning new hosts takes place in the Infrastructure > Clusters section of Morpheus. For example, provisioning a new Docker cluster in that section will begin the process of creating a Morpheus-managed Docker cluster with one host (by default). Additional hosts and custom layouts can also be created. See the Clusters section of Morpheus docs for more information.

### 5.4.2 Virtual Machines

**Section Features & Filters**

- Record
- Search
- Custom Views
- CSV Export
- JSON Export
- Paging
- Config

- Standard Filters: *OS Type*
- Advanced Filters: *Status Managed Server Type*

The Virtual Machines tab lists all managed and unmanaged VMs across Morpheus. Managed VMs are either provisioned by Morpheus, or are inventoried/discovered VMs that have been converted to managed. Unmanaged VMs are typically inventoried/discovered VMs from Cloud integrations.
5.4.3 Containers

The containers tab lists all Containers associated with Morpheus Instances accessible to the user. Note additional system level containers from Kubernetes and Docker Clusters are not listed here but are accessible in Cluster detail sections.

5.4.4 Resources

Resources represent objects that do not map to VM or Container types in Morpheus, such as IAC resources from Terraform, Cloudformation or ARM Templates like VPC’s, Gateways, Users, Policies, Brokers, API’s, Endpoints, Directories, ACL’s, Routes... well anything really. All resources created from IAC Templates map to iac provider resource types and Morpheus maintains a resource object record from the mapped resource.

Expand the Resource Types table below to see all Resource types that will be mapped to Resource objects in Morpheus:

- Resource Types Click to Expand/Hide

The following Resource Types are mapped when provisioning IAC templates including Terraform and CloudFormation templates.

<table>
<thead>
<tr>
<th>ICON</th>
<th>RESOURCE NAME</th>
<th>PROVIDER</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Accessanalyzer Analyzer</td>
<td>terraform</td>
</tr>
<tr>
<td></td>
<td>Acm Certificate</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>----------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Acm Certificate Validation</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>AcmPCA Certificate Authority</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Security Center" /></td>
<td>Advanced Threat Protection</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="API Gateway" /></td>
<td>Amazon API</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="API Gateway" /></td>
<td>Amazon API Authorizer</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="API Gateway" /></td>
<td>Amazon API Deployment</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="API Gateway" /></td>
<td>Amazon API Domain Name</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="API Gateway" /></td>
<td>Amazon API Integration</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="API Gateway" /></td>
<td>Amazon API Integration Response</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="API Gateway" /></td>
<td>Amazon API Mapping</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="API Gateway" /></td>
<td>Amazon API Model</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="API Gateway" /></td>
<td>Amazon API Route</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="API Gateway" /></td>
<td>Amazon API Route Response</td>
<td>cloudFormation</td>
</tr>
</tbody>
</table>
Table 5 – continued from previous page

<table>
<thead>
<tr>
<th>ICON</th>
<th>RESOURCE NAME</th>
<th>PROVIDER</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="API Gateway Icon" /></td>
<td>Amazon Api Stage</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="EC2 Icon" /></td>
<td>Ami</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="EC2 Icon" /></td>
<td>Ami Copy</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="EC2 Icon" /></td>
<td>Ami From Instance</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="EC2 Icon" /></td>
<td>Ami Launch Permission</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Analysis Services Icon" /></td>
<td>Analysis Server</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Analysis Services Icon" /></td>
<td>Analysis Server</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Azure Resource Icon" /></td>
<td>API</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Azure Resource Icon" /></td>
<td>API Authorization Server</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Azure Resource Icon" /></td>
<td>API Backend</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Azure Resource Icon" /></td>
<td>API Certificate</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Azure Resource Icon" /></td>
<td>API Diagnostic</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="API Gateway Icon" /></td>
<td>Api Gateway Account</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>---------------</td>
<td>----------</td>
</tr>
<tr>
<td><img src="image1.png" alt="Api Gateway" /></td>
<td>Api Gateway Api Key</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image2.png" alt="Api Gateway" /></td>
<td>Api Gateway Authorizer</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image3.png" alt="Api Gateway" /></td>
<td>Api Gateway Base Path Mapping</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image4.png" alt="Api Gateway" /></td>
<td>Api Gateway Client Certificate</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image5.png" alt="Api Gateway" /></td>
<td>Api Gateway Deployment</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image6.png" alt="Api Gateway" /></td>
<td>Api Gateway Documentation Part</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image7.png" alt="Api Gateway" /></td>
<td>Api Gateway Documentation Version</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image8.png" alt="Api Gateway" /></td>
<td>Api Gateway Domain Name</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image9.png" alt="Api Gateway" /></td>
<td>Api Gateway Gateway Response</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image10.png" alt="Api Gateway" /></td>
<td>Api Gateway Integration</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image11.png" alt="Api Gateway" /></td>
<td>Api Gateway Integration Response</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image12.png" alt="Api Gateway" /></td>
<td>Api Gateway Method</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image13.png" alt="Api Gateway" /></td>
<td>Api Gateway Method Response</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td><img src="image1.png" alt="API Gateway" /></td>
<td>Api Gateway Method Settings</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image2.png" alt="API Gateway" /></td>
<td>Api Gateway Model</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image3.png" alt="API Gateway" /></td>
<td>Api Gateway Request Validator</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image4.png" alt="API Gateway" /></td>
<td>Api Gateway Resource</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image5.png" alt="API Gateway" /></td>
<td>Api Gateway Rest Api</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image6.png" alt="API Gateway" /></td>
<td>Api Gateway Stage</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image7.png" alt="API Gateway" /></td>
<td>Api Gateway Usage Plan</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image8.png" alt="API Gateway" /></td>
<td>Api Gateway Usage Plan Key</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image9.png" alt="API Gateway" /></td>
<td>Api Gateway Vpc Link</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image10.png" alt="Azure Resource" /></td>
<td>API Group</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image11.png" alt="Azure Resource" /></td>
<td>API Group User</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image12.png" alt="Azure Resource" /></td>
<td>API Identity Provider AD</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image13.png" alt="Azure Resource" /></td>
<td>API Identity Provider Facebook</td>
<td>terraform</td>
</tr>
</tbody>
</table>
Table 5 – continued from previous page

<table>
<thead>
<tr>
<th>ICON</th>
<th>RESOURCE NAME</th>
<th>PROVIDER</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Azure Resource" /></td>
<td>API Identity Provider Google</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Azure Resource" /></td>
<td>API Identity Provider Microsoft</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Azure Resource" /></td>
<td>API Identity Provider Twitter</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Azure Resource" /></td>
<td>API Logger</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Azure Resource" /></td>
<td>API Management</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Azure Resource" /></td>
<td>API Named Value</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Azure Resource" /></td>
<td>API OpenID Provider</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Azure Resource" /></td>
<td>API Operation</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Azure Resource" /></td>
<td>API Operation Policy</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Azure Resource" /></td>
<td>API Policy</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Azure Resource" /></td>
<td>API Product</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Azure Resource" /></td>
<td>API Product API</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Azure Resource" /></td>
<td>API Product Group</td>
<td>terraform</td>
</tr>
</tbody>
</table>
### Table 5 – continued from previous page

<table>
<thead>
<tr>
<th>ICON</th>
<th>RESOURCE NAME</th>
<th>PROVIDER</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Azure Resource]</td>
<td>API Product Policy</td>
<td>terraform</td>
</tr>
<tr>
<td>![Azure Resource]</td>
<td>API Property</td>
<td>terraform</td>
</tr>
<tr>
<td>![Azure Resource]</td>
<td>API Schema</td>
<td>terraform</td>
</tr>
<tr>
<td>![Azure Resource]</td>
<td>API Subscription</td>
<td>terraform</td>
</tr>
<tr>
<td>![Azure Resource]</td>
<td>API User</td>
<td>terraform</td>
</tr>
<tr>
<td>![Azure Resource]</td>
<td>API Version Set</td>
<td>terraform</td>
</tr>
<tr>
<td>![API Gateway]</td>
<td>apigatewayv2 Api</td>
<td>terraform</td>
</tr>
<tr>
<td>![API Gateway]</td>
<td>apigatewayv2 Api Mapping</td>
<td>terraform</td>
</tr>
<tr>
<td>![API Gateway]</td>
<td>apigatewayv2 Authorizer</td>
<td>terraform</td>
</tr>
<tr>
<td>![API Gateway]</td>
<td>apigatewayv2 Deployment</td>
<td>terraform</td>
</tr>
<tr>
<td>![API Gateway]</td>
<td>apigatewayv2 Domain Name</td>
<td>terraform</td>
</tr>
<tr>
<td>![API Gateway]</td>
<td>apigatewayv2 Integration</td>
<td>terraform</td>
</tr>
<tr>
<td>![API Gateway]</td>
<td>apigatewayv2 Integration Response</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td><img src="image" alt="API Gateway" /></td>
<td>Apigatewayv2 Model</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="API Gateway" /></td>
<td>Apigatewayv2 Route</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="API Gateway" /></td>
<td>Apigatewayv2 Route Response</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="API Gateway" /></td>
<td>Apigatewayv2 Stage</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="API Gateway" /></td>
<td>Apigatewayv2 Vpc Link</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="App Configuration" /></td>
<td>App Configuration</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Elastic Load Balancing" /></td>
<td>App Cookie Stickiness Policy</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Application Insights" /></td>
<td>App Insights Analytics Item</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Application Insights" /></td>
<td>App Insights API Key</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Application Insights" /></td>
<td>App Insights Web Test</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Azure Resource" /></td>
<td>App Service</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Azure Resource" /></td>
<td>App Service Active Slot</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Azure Resource" /></td>
<td>App Service Certificate</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>-----------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td><img src="image" alt="Azure Resource" /></td>
<td>App Service Certificate Order</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Azure Resource" /></td>
<td>App Service Environment</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Azure Resource" /></td>
<td>App Service Host Binding</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Azure Resource" /></td>
<td>App Service Network Swift Connection</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Azure Resource" /></td>
<td>App Service Plan</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Azure Resource" /></td>
<td>App Service Slot</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Azure Resource" /></td>
<td>App Service Source Control Token</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Auto Scaling" /></td>
<td>Appautoscaling Policy</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Auto Scaling" /></td>
<td>Appautoscaling Scheduled Action</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Auto Scaling" /></td>
<td>Appautoscaling Target</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Compute" /></td>
<td>Application Definition</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Network" /></td>
<td>Application Gateway</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Network" /></td>
<td>Application Gateway</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>---------------------</td>
<td>----------</td>
</tr>
<tr>
<td><img src="image" alt="Application Insights" /></td>
<td>Application Insights</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Network" /></td>
<td>Application Security Group</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Network" /></td>
<td>Application Security Group</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Appmesh Mesh</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Appmesh Route</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Appmesh Virtual Node</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Appmesh Virtual Router</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Appmesh Virtual Service</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AppSync" /></td>
<td>Appsync Api Key</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AppSync" /></td>
<td>Appsync Datasource</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AppSync" /></td>
<td>Appsync Function</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AppSync" /></td>
<td>Appsync Graphql Api</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AppSync" /></td>
<td>Appsync Resolver</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>-----------------------</td>
<td>------------</td>
</tr>
<tr>
<td><img src="image" alt="Athena" /></td>
<td>Athen Named Query</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Athena" /></td>
<td>Athena Database</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Athena" /></td>
<td>Athen Named Query</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Athena" /></td>
<td>Athen Workgroup</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Automation" /></td>
<td>Automation Account</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Automation" /></td>
<td>Automation Certificate</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Automation" /></td>
<td>Automation Credential</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Automation" /></td>
<td>Automation DSC Config</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Automation" /></td>
<td>Automation DSC Node Config</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Automation" /></td>
<td>Automation Job Schedule</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Automation" /></td>
<td>Automation Module</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Automation" /></td>
<td>Automation Runbook</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Automation" /></td>
<td>Automation Schedule</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>---------------</td>
<td>----------</td>
</tr>
<tr>
<td><img src="Automation.png" alt="Automation" /></td>
<td>Automation Variable Boolean</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="Automation.png" alt="Automation" /></td>
<td>Automation Variable Datetime</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="Automation.png" alt="Automation" /></td>
<td>Automation Variable Int</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="Automation.png" alt="Automation" /></td>
<td>Automation Variable String</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="AutoScaling.png" alt="Auto Scaling" /></td>
<td>Autoscaling Attachment</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="AutoScaling.png" alt="Auto Scaling" /></td>
<td>Autoscaling Group</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="AutoScaling.png" alt="Auto Scaling" /></td>
<td>Autoscaling Lifecycle Hook</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="AutoScaling.png" alt="Auto Scaling" /></td>
<td>Autoscaling Notification</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="AutoScaling.png" alt="Auto Scaling" /></td>
<td>Autoscaling Policy</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="AutoScaling.png" alt="Auto Scaling" /></td>
<td>Autoscaling Schedule</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="Compute.png" alt="Compute" /></td>
<td>Availability Set</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="ElasticLoadBalancing.png" alt="Elastic Load Balancing" /></td>
<td>AWS ALB Listener</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="ElasticLoadBalancing.png" alt="Elastic Load Balancing" /></td>
<td>AWS ALB Listener Certificate</td>
<td>cloudFormation</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>-----------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td><img src="image" alt="Elastic Load Balancing" /></td>
<td>AWS ALB Listener Rule</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Elastic Load Balancing" /></td>
<td>AWS ALB Target Group</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="AWS App Mesh" /></td>
<td>AWS App Mesh</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="AWS App Mesh" /></td>
<td>AWS App Mesh Route</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="AWS App Mesh" /></td>
<td>AWS App Mesh Virtual Node</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="AWS App Mesh" /></td>
<td>AWS App Mesh Virtual Router</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="AWS App Mesh" /></td>
<td>AWS App Mesh Virtual Service</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Elastic Load Balancing" /></td>
<td>AWS Application Load Balancer</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Auto Scaling" /></td>
<td>AWS Auto Scaling Group</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Auto Scaling" /></td>
<td>AWS Auto Scaling Launch Configuration</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Auto Scaling" /></td>
<td>AWS Auto Scaling Lifecycle Hook</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Auto Scaling" /></td>
<td>AWS Auto Scaling Policy</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Auto Scaling" /></td>
<td>AWS Auto Scaling Scheduled Action</td>
<td>cloudFormation</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>----------------</td>
<td>----------</td>
</tr>
<tr>
<td><img src="image" alt="Elastic Load Balancing" /></td>
<td>AWS Elastic Load Balancer</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Elasticsearch Service" /></td>
<td>AWS Elasticsearch Domain</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="AWS SDB" /></td>
<td>AWS SDB Domain</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Secrets Manager" /></td>
<td>AWS Secrets Manager Resource Policy</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Secrets Manager" /></td>
<td>AWS Secrets Manager Rotation Schedule</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Secrets Manager" /></td>
<td>AWS Secrets Manager Secret</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Secrets Manager" /></td>
<td>AWS Secrets Manager Secret Target Attachment</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>AWS SES Configuration Set</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>AWS SES Configuration Set Event Destination</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>AWS SES Receipt Filter</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>AWS SES Receipt Rule</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>AWS SES Receipt Rule Set</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>AWS SES Template</td>
<td>cloudFormation</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>AWS SNS Subscription</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>AWS SNS Topic</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>AWS SNS Topic Policy</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="AWS SQS" /></td>
<td>AWS SQS Queue</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="AWS SQS" /></td>
<td>AWS SQS Queue Policy</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="WAF" /></td>
<td>AWS WAF Byte Match Set</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="WAF" /></td>
<td>AWS WAF IP Set</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="WAF" /></td>
<td>AWS WAF Regional Byte Match Set</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="WAF" /></td>
<td>AWS WAF Regional Geo Match Set</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="WAF" /></td>
<td>AWS WAF Regional IP Set</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="WAF" /></td>
<td>AWS WAF Regional Rate Based Rule</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="WAF" /></td>
<td>AWS WAF Regional Regex Pattern Set</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="WAF" /></td>
<td>AWS WAF Regional Rule</td>
<td>cloudFormation</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td><img src="image" alt="WAF" /></td>
<td>AWS WAF Regional Size Constraint Set</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="WAF" /></td>
<td>AWS WAF Regional Sql Injection Match Set</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="WAF" /></td>
<td>AWS WAF Regional Web ACL</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="WAF" /></td>
<td>AWS WAF Regional Web ACL Association</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="WAF" /></td>
<td>AWS WAF Regional Xss Match Set</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="WAF" /></td>
<td>AWS WAF Rule</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="WAF" /></td>
<td>AWS WAF Size Constraint Set</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="WAF" /></td>
<td>AWS WAF Sql Injection Match Set</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="WAF" /></td>
<td>AWS WAF Web ACL</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="WAF" /></td>
<td>AWS WAF Xss Match Set</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Workspaces" /></td>
<td>AWS Workspace</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Azure Resource" /></td>
<td>Azure Resource</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Azure Resource" /></td>
<td>Azure Resource</td>
<td>terraform</td>
</tr>
</tbody>
</table>
Table 5 – continued from previous page

<table>
<thead>
<tr>
<th>ICON</th>
<th>RESOURCE NAME</th>
<th>PROVIDER</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="backup.png" alt="Backup" /></td>
<td>Backup Plan</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="backup.png" alt="Backup" /></td>
<td>Backup Policy File Share</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="backup.png" alt="Backup" /></td>
<td>Backup Policy VM</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="backup.png" alt="Backup" /></td>
<td>Backup Protected File Share</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="backup.png" alt="Backup" /></td>
<td>Backup Protected VM</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="backup.png" alt="Backup" /></td>
<td>Backup Selection</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="backup.png" alt="Backup" /></td>
<td>Backup Storage Account</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="backup.png" alt="Backup" /></td>
<td>Backup Vault</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="bastion.png" alt="Network" /></td>
<td>Bastion Host</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="bastion.png" alt="Network" /></td>
<td>Bastion Host</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="batch.png" alt="Batch" /></td>
<td>Batch Account</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="batch.png" alt="Batch" /></td>
<td>Batch Account</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="batch.png" alt="Batch" /></td>
<td>Batch Application</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>---------------------------</td>
<td>----------</td>
</tr>
<tr>
<td><img src="image" alt="Batch Application" /></td>
<td>Batch Application</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Batch Certificate" /></td>
<td>Batch Certificate</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Batch Certificate" /></td>
<td>Batch Certificate</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Batch Compute Environment" /></td>
<td>Batch Compute Environment</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Batch Job Definition" /></td>
<td>Batch Job Definition</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Batch Job Queue" /></td>
<td>Batch Job Queue</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Batch Pool" /></td>
<td>Batch Pool</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Batch Pool" /></td>
<td>Batch Pool</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Bot Channel Email" /></td>
<td>Bot Channel Email</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Bot Channel Email" /></td>
<td>Bot Channel Email</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Bot Channel MS Teams" /></td>
<td>Bot Channel MS Teams</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Bot Channel MS Teams" /></td>
<td>Bot Channel MS Teams</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Bot Channel Registration" /></td>
<td>Bot Channel Registration</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Bot</td>
<td>Bot Channel Slack</td>
<td>terraform</td>
</tr>
<tr>
<td>Bot</td>
<td>Bot Connection</td>
<td>terraform</td>
</tr>
<tr>
<td>Bot</td>
<td>Bot Connection</td>
<td>terraform</td>
</tr>
<tr>
<td>Bot</td>
<td>Bot Direct Line</td>
<td>terraform</td>
</tr>
<tr>
<td>Bot</td>
<td>Bot Web App</td>
<td>terraform</td>
</tr>
<tr>
<td>Bot</td>
<td>Bot Web App</td>
<td>terraform</td>
</tr>
<tr>
<td>AWS Resource</td>
<td>Budgets Budget</td>
<td>terraform</td>
</tr>
<tr>
<td>CDN</td>
<td>CDN Endpoint</td>
<td>terraform</td>
</tr>
<tr>
<td>CDN</td>
<td>CDN Endpoint</td>
<td>terraform</td>
</tr>
<tr>
<td>CDN</td>
<td>CDN Profile</td>
<td>terraform</td>
</tr>
<tr>
<td>CDN</td>
<td>CDN Profile</td>
<td>terraform</td>
</tr>
<tr>
<td>AWS Resource</td>
<td>Cloud9 Environment Ec2</td>
<td>terraform</td>
</tr>
<tr>
<td>Cloud Formation</td>
<td>Cloudformation Stack</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>[CloudFormation]</td>
<td>Cloudformation Stack Set</td>
<td>terraform</td>
</tr>
<tr>
<td>[CloudFormation]</td>
<td>Cloudformation Stack Set Instance</td>
<td>terraform</td>
</tr>
<tr>
<td>[CloudFront]</td>
<td>Cloudfront Distribution</td>
<td>terraform</td>
</tr>
<tr>
<td>[CloudFront]</td>
<td>Cloudfront Origin Access Identity</td>
<td>terraform</td>
</tr>
<tr>
<td>[CloudFront]</td>
<td>Cloudfront Public Key</td>
<td>terraform</td>
</tr>
<tr>
<td>[AWS Resource]</td>
<td>Cloudhsm V2 Cluster</td>
<td>terraform</td>
</tr>
<tr>
<td>[AWS Resource]</td>
<td>Cloudhsm V2 Hsm</td>
<td>terraform</td>
</tr>
<tr>
<td>[CloudTrail]</td>
<td>Cloudtrail</td>
<td>terraform</td>
</tr>
<tr>
<td>[CloudWatch]</td>
<td>Cloudwatch Dashboard</td>
<td>terraform</td>
</tr>
<tr>
<td>[CloudWatch]</td>
<td>Cloudwatch Event Permission</td>
<td>terraform</td>
</tr>
<tr>
<td>[CloudWatch]</td>
<td>Cloudwatch Event Rule</td>
<td>terraform</td>
</tr>
<tr>
<td>[CloudWatch]</td>
<td>Cloudwatch Event Target</td>
<td>terraform</td>
</tr>
<tr>
<td>[CloudWatch]</td>
<td>Cloudwatch Log Destination</td>
<td>terraform</td>
</tr>
</tbody>
</table>

5.4. Compute
<table>
<thead>
<tr>
<th>ICON</th>
<th>RESOURCE NAME</th>
<th>PROVIDER</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="CloudWatch" /></td>
<td>Cloudwatch Log Destination Policy</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="CloudWatch" /></td>
<td>Cloudwatch Log Group</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="CloudWatch" /></td>
<td>Cloudwatch Log Metric Filter</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="CloudWatch" /></td>
<td>Cloudwatch Log Resource Policy</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="CloudWatch" /></td>
<td>Cloudwatch Log Stream</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="CloudWatch" /></td>
<td>Cloudwatch Log Subscription Filter</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="CloudWatch" /></td>
<td>Cloudwatch Metric Alarm</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="CodeBuild" /></td>
<td>Codebuild Project</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="CodeBuild" /></td>
<td>Codebuild Source Credential</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="CodeBuild" /></td>
<td>Codebuild Webhook</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="CodeCommit" /></td>
<td>Codecommit Repository</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="CodeCommit" /></td>
<td>Codecommit Trigger</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="CodeDeploy" /></td>
<td>Codedeploy App</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>---------------</td>
<td>----------</td>
</tr>
<tr>
<td><img src="image1.png" alt="CodeDeploy" /></td>
<td>Codedeploy Deployment Config</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image2.png" alt="CodeDeploy" /></td>
<td>Codedeploy Deployment Group</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image3.png" alt="CodePipeline" /></td>
<td>Codepipeline</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image4.png" alt="CodePipeline" /></td>
<td>Codepipeline Webhook</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image5.png" alt="CodeStar" /></td>
<td>Codestarnotifications Notification Rule</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image6.png" alt="Cognitive Services" /></td>
<td>Cognitive Account</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image7.png" alt="Cognitive Services" /></td>
<td>Cognitive Account</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image8.png" alt="AWS Resource" /></td>
<td>Cognito Identity Pool</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image9.png" alt="AWS Resource" /></td>
<td>Cognito Identity Pool Roles Attachment</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image10.png" alt="AWS Resource" /></td>
<td>Cognito Identity Provider</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image11.png" alt="AWS Resource" /></td>
<td>Cognito Resource Server</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image12.png" alt="AWS Resource" /></td>
<td>Cognito User Group</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image13.png" alt="AWS Resource" /></td>
<td>Cognito User Pool</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Cognito User Pool Client</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Cognito User Pool Domain</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Config Aggregate Authorization</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Config Config Rule</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Config Configuration Aggregator</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Config Configuration Recorder</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Config Configuration Recorder Status</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Config Delivery Channel</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Config Organization Custom Rule</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Config Organization Managed Rule</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Container" /></td>
<td>Container Group</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Container" /></td>
<td>Container Group</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Container" /></td>
<td>Container Registry</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>---------------</td>
<td>----------</td>
</tr>
<tr>
<td><img src="image1" alt="Container" /></td>
<td>Container Registry</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image2" alt="Container" /></td>
<td>Container Registry Webhook</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image3" alt="Container" /></td>
<td>Container Registry Webhook</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image4" alt="CosmosDB" /></td>
<td>CosmosDB Account</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image5" alt="CosmosDB" /></td>
<td>CosmosDB Cassandra Keyspace</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image6" alt="CosmosDB" /></td>
<td>CosmosDB Gremlin Database</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image7" alt="CosmosDB" /></td>
<td>CosmosDB Gremlin Graph</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image8" alt="CosmosDB" /></td>
<td>CosmosDB Mongo Collection</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image9" alt="CosmosDB" /></td>
<td>CosmosDB Mongo Database</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image10" alt="CosmosDB" /></td>
<td>CosmosDB SQL Container</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image11" alt="CosmosDB" /></td>
<td>CosmosDB SQL Database</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image12" alt="CosmosDB" /></td>
<td>CosmosDB Table</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image13" alt="CosmosDB" /></td>
<td>Cost Management Export Resource Group</td>
<td>terraform</td>
</tr>
</tbody>
</table>

5.4. Compute
<table>
<thead>
<tr>
<th>ICON</th>
<th>RESOURCE NAME</th>
<th>PROVIDER</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="icon" alt="CosmosDB" /></td>
<td>Cost Management Export Resource Group</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="icon" alt="AWS Resource" /></td>
<td>Cur Report Definition</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="icon" alt="Custom" /></td>
<td>Custom Provider</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="icon" alt="Custom" /></td>
<td>Custom Provider</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="icon" alt="VPC" /></td>
<td>Customer Gateway</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="icon" alt="Portal" /></td>
<td>Dashboard</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="icon" alt="Portal" /></td>
<td>Dashboard</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="icon" alt="Data Factory" /></td>
<td>Data Factory</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="icon" alt="Data Factory" /></td>
<td>Data Factory Data Lake Storage</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="icon" alt="Data Factory" /></td>
<td>Data Factory Integration Runtime</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="icon" alt="Data Factory" /></td>
<td>Data Factory MySQL Dataset</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="icon" alt="Data Factory" /></td>
<td>Data Factory MySQL Link</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="icon" alt="Data Factory" /></td>
<td>Data Factory Pipeline</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td><img src="image1.png" alt="Data Factory" /></td>
<td>Data Factory PostgreSQL Dataset</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image1.png" alt="Data Factory" /></td>
<td>Data Factory PostgreSQL Link</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image1.png" alt="Data Factory" /></td>
<td>Data Factory SQL Server Link</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image1.png" alt="Data Factory" /></td>
<td>Data Factory SQL Server Table</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image1.png" alt="Data Factory" /></td>
<td>Data Factory Trigger Schedule</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image2.png" alt="Data Lake" /></td>
<td>Data Lake Analytics Account</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image2.png" alt="Data Lake" /></td>
<td>Data Lake Analytics Firewall Rule</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image3.png" alt="Storage" /></td>
<td>Data Lake Filesystem</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image2.png" alt="Data Lake" /></td>
<td>Data Lake Store</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image2.png" alt="Data Lake" /></td>
<td>Data Lake Store File</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image2.png" alt="Data Lake" /></td>
<td>Data Lake Store Firewall Rule</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image4.png" alt="Data Share" /></td>
<td>Data Share Account</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image5.png" alt="Database Migration" /></td>
<td>Database Migration Project</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>---------------</td>
<td>----------</td>
</tr>
<tr>
<td><img src="database_migration.png" alt="Database Migration Service" /></td>
<td>Database Migration Service</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="databricks.png" alt="Databricks Workspace" /></td>
<td>Databricks Workspace</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="datapipeline.png" alt="Datapipeline Pipeline" /></td>
<td>Datapipeline Pipeline</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="datasync.png" alt="Datasync Agent" /></td>
<td>Datasync Agent</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="datasync_location_efs.png" alt="Datasync Location Efs" /></td>
<td>Datasync Location Efs</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="datasync_location_nfs.png" alt="Datasync Location Nfs" /></td>
<td>Datasync Location Nfs</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="datasync_location_s3.png" alt="Datasync Location S3" /></td>
<td>Datasync Location S3</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="datasync_location_smb.png" alt="Datasync Location Smb" /></td>
<td>Datasync Location Smb</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="datasync_task.png" alt="Datasync Task" /></td>
<td>Datasync Task</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="dax_cluster.png" alt="Dax Cluster" /></td>
<td>Dax Cluster</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="dax_parameter_group.png" alt="Dax Parameter Group" /></td>
<td>Dax Parameter Group</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="dax_subnet_group.png" alt="Dax Subnet Group" /></td>
<td>Dax Subnet Group</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="db_cluster_snapshot.png" alt="Db Cluster Snapshot" /></td>
<td>Db Cluster Snapshot</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>----------</td>
<td>------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>RDS</td>
<td>Db Event Subscription</td>
<td>terraform</td>
</tr>
<tr>
<td>RDS</td>
<td>Db Instance</td>
<td>terraform</td>
</tr>
<tr>
<td>RDS</td>
<td>Db Instance Role Association</td>
<td>terraform</td>
</tr>
<tr>
<td>RDS</td>
<td>Db Option Group</td>
<td>terraform</td>
</tr>
<tr>
<td>RDS</td>
<td>Db Parameter Group</td>
<td>terraform</td>
</tr>
<tr>
<td>RDS</td>
<td>Db Security Group</td>
<td>terraform</td>
</tr>
<tr>
<td>RDS</td>
<td>Db Snapshot</td>
<td>terraform</td>
</tr>
<tr>
<td>RDS</td>
<td>Db Subnet Group</td>
<td>terraform</td>
</tr>
<tr>
<td>Compute</td>
<td>Dedicated Host</td>
<td>terraform</td>
</tr>
<tr>
<td>Compute</td>
<td>Dedicated Host Group</td>
<td>terraform</td>
</tr>
<tr>
<td>VPC</td>
<td>Default Network Acl</td>
<td>terraform</td>
</tr>
<tr>
<td>VPC</td>
<td>Default Route Table</td>
<td>terraform</td>
</tr>
<tr>
<td>VPC</td>
<td>Default Security Group</td>
<td>terraform</td>
</tr>
</tbody>
</table>

5.4. Compute
<table>
<thead>
<tr>
<th>ICON</th>
<th>RESOURCE NAME</th>
<th>PROVIDER</th>
</tr>
</thead>
<tbody>
<tr>
<td>![VPC]</td>
<td>Default Subnet</td>
<td>terraform</td>
</tr>
<tr>
<td>![VPC]</td>
<td>Default Vpc</td>
<td>terraform</td>
</tr>
<tr>
<td>![VPC]</td>
<td>Default Vpc Dhcp Options</td>
<td>terraform</td>
</tr>
<tr>
<td>![AWS Resource]</td>
<td>Devicefarm Project</td>
<td>terraform</td>
</tr>
<tr>
<td>![DevSpace]</td>
<td>DevSpace Controller</td>
<td>terraform</td>
</tr>
<tr>
<td>![DevSpace]</td>
<td>DevSpace Controller</td>
<td>terraform</td>
</tr>
<tr>
<td>![DevTest]</td>
<td>DevTest Lab</td>
<td>terraform</td>
</tr>
<tr>
<td>![DevTest]</td>
<td>DevTest Lab</td>
<td>terraform</td>
</tr>
<tr>
<td>![DevTest]</td>
<td>DevTest Linux Vm</td>
<td>terraform</td>
</tr>
<tr>
<td>![DevTest]</td>
<td>DevTest Linux Vm</td>
<td>terraform</td>
</tr>
<tr>
<td>![DevTest]</td>
<td>DevTest Policy</td>
<td>terraform</td>
</tr>
<tr>
<td>![DevTest]</td>
<td>DevTest Policy</td>
<td>terraform</td>
</tr>
<tr>
<td>![DevTest]</td>
<td>DevTest Schedule</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td><img src="image" alt="DevTest" /></td>
<td>DevTest Schedule</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="DevTest" /></td>
<td>DevTest Virtual Network</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="DevTest" /></td>
<td>DevTest Virtual Network</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="DevTest" /></td>
<td>DevTest Windows Vm</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="DevTest" /></td>
<td>DevTest Windows Vm</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Directory Service Conditional Forwarder</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Directory Service Directory</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Directory Service Log Subscription</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Compute" /></td>
<td>Disk Encryption Set</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Dlm Lifecycle Policy</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Dms Certificate</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Dms Endpoint</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Dms Event Subscription</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>-----------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>🌐</td>
<td>Dms Replication Instance</td>
<td>terraform</td>
</tr>
<tr>
<td>🌐</td>
<td>Dms Replication Subnet Group</td>
<td>terraform</td>
</tr>
<tr>
<td>🌐</td>
<td>Dms Replication Task</td>
<td>terraform</td>
</tr>
<tr>
<td>🌐</td>
<td>DNS A Record</td>
<td>terraform</td>
</tr>
<tr>
<td>🌐</td>
<td>DNS A Record</td>
<td>terraform</td>
</tr>
<tr>
<td>🌐</td>
<td>DNS AAAA Record</td>
<td>terraform</td>
</tr>
<tr>
<td>🌐</td>
<td>DNS CAA Record</td>
<td>terraform</td>
</tr>
<tr>
<td>🌐</td>
<td>DNS CName Record</td>
<td>terraform</td>
</tr>
<tr>
<td>🌐</td>
<td>DNS CName Record</td>
<td>terraform</td>
</tr>
<tr>
<td>🌐</td>
<td>DNS MX Record</td>
<td>terraform</td>
</tr>
<tr>
<td>🌐</td>
<td>DNS MX Record</td>
<td>terraform</td>
</tr>
<tr>
<td>🌐</td>
<td>DNS NS Record</td>
<td>terraform</td>
</tr>
<tr>
<td>🌐</td>
<td>DNS NS Record</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>----------------------</td>
<td>----------</td>
</tr>
<tr>
<td>![DNS]</td>
<td>DNS PTR Record</td>
<td>terraform</td>
</tr>
<tr>
<td>![DNS]</td>
<td>DNS SRV Record</td>
<td>terraform</td>
</tr>
<tr>
<td>![DNS]</td>
<td>DNS SRV Record</td>
<td>terraform</td>
</tr>
<tr>
<td>![DNS]</td>
<td>DNS Txt Record</td>
<td>terraform</td>
</tr>
<tr>
<td>![DNS]</td>
<td>DNS Txt Record</td>
<td>terraform</td>
</tr>
<tr>
<td>![DNS]</td>
<td>DNS Zone</td>
<td>terraform</td>
</tr>
<tr>
<td>![DNS]</td>
<td>DNS Zone</td>
<td>terraform</td>
</tr>
<tr>
<td>![AWS Resource]</td>
<td>Docdb Cluster</td>
<td>terraform</td>
</tr>
<tr>
<td>![AWS Resource]</td>
<td>Docdb Cluster Instance</td>
<td>terraform</td>
</tr>
<tr>
<td>![AWS Resource]</td>
<td>Docdb Cluster Parameter Group</td>
<td>terraform</td>
</tr>
<tr>
<td>![AWS Resource]</td>
<td>Docdb Cluster Snapshot</td>
<td>terraform</td>
</tr>
<tr>
<td>![AWS Resource]</td>
<td>Docdb Subnet Group</td>
<td>terraform</td>
</tr>
<tr>
<td>![Direct Connect]</td>
<td>Dx Bgp Peer</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td><img src="image" alt="Direct Connect" /></td>
<td>Dx Connection</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Direct Connect" /></td>
<td>Dx Connection Association</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Direct Connect" /></td>
<td>Dx Gateway</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Direct Connect" /></td>
<td>Dx Gateway Association</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Direct Connect" /></td>
<td>Dx Gateway Association Proposal</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Direct Connect" /></td>
<td>Dx Hosted Private Virtual Interface</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Direct Connect" /></td>
<td>Dx Hosted Private Virtual Interface Acceptor</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Direct Connect" /></td>
<td>Dx Hosted Public Virtual Interface</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Direct Connect" /></td>
<td>Dx Hosted Public Virtual Interface Acceptor</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Direct Connect" /></td>
<td>Dx Hosted Transit Virtual Interface</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Direct Connect" /></td>
<td>Dx Hosted Transit Virtual Interface Acceptor</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Direct Connect" /></td>
<td>Dx Lag</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Direct Connect" /></td>
<td>Dx Private Virtual Interface</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>-----------------------------</td>
<td>------------</td>
</tr>
<tr>
<td><img src="image" alt="Dx Public Virtual Interface" /></td>
<td>Dx Public Virtual Interface</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Dx Transit Virtual Interface" /></td>
<td>Dx Transit Virtual Interface</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Dynamodb Global Table" /></td>
<td>Dynamodb Global Table</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Dynamodb Table" /></td>
<td>Dynamodb Table</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Dynamodb Table" /></td>
<td>Dynamodb Table</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Dynamodb Table Item" /></td>
<td>Dynamodb Table Item</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Ebs Default Kms Key" /></td>
<td>Ebs Default Kms Key</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Ebs Encryption By Default" /></td>
<td>Ebs Encryption By Default</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Ebs Snapshot" /></td>
<td>Ebs Snapshot</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Ebs Snapshot Copy" /></td>
<td>Ebs Snapshot Copy</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Ebs Volume" /></td>
<td>Ebs Volume</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Ec2 Availability Zone Group" /></td>
<td>Ec2 Availability Zone Group</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="EC2 Capacity Reservation" /></td>
<td>EC2 Capacity Reservation</td>
<td>cloudFormation</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>---------------</td>
<td>----------</td>
</tr>
<tr>
<td><img src="image" alt="Ec2" /></td>
<td>Ec2 Capacity Reservation</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Ec2" /></td>
<td>EC2 Client Vpn Authorization Rule</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Ec2" /></td>
<td>EC2 Client Vpn Endpoint</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Ec2" /></td>
<td>Ec2 Client Vpn Endpoint</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Ec2" /></td>
<td>Ec2 Client Vpn Network Association</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Ec2" /></td>
<td>EC2 Client Vpn Route</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Ec2" /></td>
<td>EC2 Client Vpn Target Network Association</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Ec2" /></td>
<td>EC2 Customer Gateway</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Ec2" /></td>
<td>EC2 DHCP Options</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Ec2" /></td>
<td>EC2 Egress Only Internet Gateway</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Ec2" /></td>
<td>EC2 EIP</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Ec2" /></td>
<td>EC2 EIP Association</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Ec2" /></td>
<td>EC2 Fleet</td>
<td>cloudFormation</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>![EC2]</td>
<td>Ec2 Fleet</td>
<td>terraform</td>
</tr>
<tr>
<td>![EC2]</td>
<td>EC2 Flow Log</td>
<td>cloudFormation</td>
</tr>
<tr>
<td>![EC2]</td>
<td>EC2 Host</td>
<td>cloudFormation</td>
</tr>
<tr>
<td>![EC2]</td>
<td>EC2 Instance</td>
<td>cloudFormation</td>
</tr>
<tr>
<td>![EC2]</td>
<td>EC2 Internet Gateway</td>
<td>cloudFormation</td>
</tr>
<tr>
<td>![EC2]</td>
<td>EC2 Launch Template</td>
<td>cloudFormation</td>
</tr>
<tr>
<td>![EC2]</td>
<td>EC2 Nat Gateway</td>
<td>cloudFormation</td>
</tr>
<tr>
<td>![EC2]</td>
<td>EC2 Network Acl</td>
<td>cloudFormation</td>
</tr>
<tr>
<td>![EC2]</td>
<td>EC2 Network Acl Entry</td>
<td>cloudFormation</td>
</tr>
<tr>
<td>![EC2]</td>
<td>EC2 Network Interface</td>
<td>cloudFormation</td>
</tr>
<tr>
<td>![EC2]</td>
<td>EC2 Network Interface Attachment</td>
<td>cloudFormation</td>
</tr>
<tr>
<td>![EC2]</td>
<td>EC2 Network Interface Permission</td>
<td>cloudFormation</td>
</tr>
<tr>
<td>![EC2]</td>
<td>EC2 Placement Group</td>
<td>cloudFormation</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>-----------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>EC2 Route</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>EC2 Route Table</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>EC2 Security Group</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>EC2 Security Group Egress</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>EC2 Security Group Ingress</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>EC2 Spot Fleet</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>EC2 Subnet</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>EC2 Subnet Cidr Block</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>EC2 Subnet Network Acl Association</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>EC2 Subnet Route Table Association</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>Ec2 Traffic Mirror Filter</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>Ec2 Traffic Mirror Filter Rule</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>Ec2 Traffic Mirror Session</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>---------------</td>
<td>----------</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>Ec2 Traffic Mirror Target</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>Ec2 Transit Gateway</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>EC2 Transit Gateway</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>EC2 Transit Gateway Attachment</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>Ec2 Transit Gateway Peering Attachment</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>Ec2 Transit Gateway Peering Attachment Accepter</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>Ec2 Transit Gateway Route</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>EC2 Transit Gateway Route</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>Ec2 Transit Gateway Route Table</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>EC2 Transit Gateway Route Table</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>Ec2 Transit Gateway Route Table Association</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>EC2 Transit Gateway Route Table Association</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>Ec2 Transit Gateway Route Table Propagation</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>---------------</td>
<td>----------</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>EC2 Transit Gateway Route Table Propagation</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>Ec2 Transit Gateway Vpc Attachment</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>EC2 Transit Gateway VPC Attachment</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>Ec2 Transit Gateway Vpc Attachment Accepter</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>EC2 Volume</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>EC2 Volume Attachment</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>EC2 VPC</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>EC2 VPC Cidr Block</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>EC2 VPC DHCP Options Association</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>EC2 VPC Endpoint</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>EC2 VPC Endpoint Connection Notification</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>EC2 VPC Endpoint Service</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>EC2 VPC Endpoint Service Permissions</td>
<td>cloudFormation</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>EC2</td>
<td>EC2 VPC Gateway Attachment</td>
<td>cloudFormation</td>
</tr>
<tr>
<td>EC2</td>
<td>EC2 VPC Peering Connection</td>
<td>cloudFormation</td>
</tr>
<tr>
<td>EC2</td>
<td>EC2 VPN Connection</td>
<td>cloudFormation</td>
</tr>
<tr>
<td>EC2</td>
<td>EC2 VPN Connection Route</td>
<td>cloudFormation</td>
</tr>
<tr>
<td>EC2</td>
<td>EC2 VPN Gateway</td>
<td>cloudFormation</td>
</tr>
<tr>
<td>EC2</td>
<td>EC2 VPN Gateway Route Propagation</td>
<td>cloudFormation</td>
</tr>
<tr>
<td>AWS Resource</td>
<td>Ecr Lifecycle Policy</td>
<td>terraform</td>
</tr>
<tr>
<td>AWS Resource</td>
<td>Ecr Repository</td>
<td>terraform</td>
</tr>
<tr>
<td>AWS Resource</td>
<td>Ecr Repository Policy</td>
<td>terraform</td>
</tr>
<tr>
<td>Elastic Container Service</td>
<td>Ecs Capacity Provider</td>
<td>terraform</td>
</tr>
<tr>
<td>Elastic Container Service</td>
<td>ECS Cluster</td>
<td>cloudFormation</td>
</tr>
<tr>
<td>Elastic Container Service</td>
<td>Ecs Cluster</td>
<td>terraform</td>
</tr>
<tr>
<td>Elastic Container Service</td>
<td>Ecs Service</td>
<td>terraform</td>
</tr>
</tbody>
</table>

5.4. Compute
Table 5 – continued from previous page

<table>
<thead>
<tr>
<th>ICON</th>
<th>RESOURCE NAME</th>
<th>PROVIDER</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="ECS Service" /></td>
<td>ECS Service</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Ecs Task Definition" /></td>
<td>Ecs Task Definition</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="ECS Task Definition" /></td>
<td>ECS Task Definition</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Efs File System" /></td>
<td>Efs File System</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="EFS File System" /></td>
<td>EFS File System</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Efs Mount Target" /></td>
<td>Efs Mount Target</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="EFS Mount Target" /></td>
<td>EFS Mount Target</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="VPC" /></td>
<td>Egress Only Internet Gateway</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>Eip</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>Eip Association</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="EKS Cluster" /></td>
<td>EKS Cluster</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Eks Cluster" /></td>
<td>Eks Cluster</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Eks Fargate Profile" /></td>
<td>Eks Fargate Profile</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>-----------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td><img src="image" alt="Eks Node Group" /></td>
<td>Eks Node Group</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Elastic Beanstalk Application" /></td>
<td>Elastic Beanstalk Application</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Elastic Beanstalk Application" /></td>
<td>Elastic Beanstalk Application</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Elastic Beanstalk Application Version" /></td>
<td>Elastic Beanstalk Application Version</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Elastic Beanstalk Application Version" /></td>
<td>Elastic Beanstalk Application Version</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Elastic Beanstalk Configuration Template" /></td>
<td>Elastic Beanstalk Configuration Template</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Elastic Beanstalk Configuration Template" /></td>
<td>Elastic Beanstalk Configuration Template</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Elastic Beanstalk Environment" /></td>
<td>Elastic Beanstalk Environment</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Elastic Beanstalk Environment" /></td>
<td>Elastic Beanstalk Environment</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="ElastiCache Cluster" /></td>
<td>ElastiCache Cluster</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="ElastiCache Cluster" /></td>
<td>ElastiCache Cluster</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="ElastiCache Parameter Group" /></td>
<td>ElastiCache Parameter Group</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="ElastiCache Parameter Group" /></td>
<td>ElastiCache Parameter Group</td>
<td>cloudFormation</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>---------------</td>
<td>----------</td>
</tr>
<tr>
<td><img src="image" alt="ElastiCache" /></td>
<td>Elasticache Replication Group</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="ElastiCache" /></td>
<td>ElastiCache Replication Group</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="ElastiCache" /></td>
<td>Elasticache Security Group</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="ElastiCache" /></td>
<td>ElastiCache Security Group</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="ElastiCache" /></td>
<td>ElastiCache Security Group Ingress</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="ElastiCache" /></td>
<td>Elasticache Subnet Group</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="ElastiCache" /></td>
<td>ElastiCache Subnet Group</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Elasticsearch Service" /></td>
<td>Elasticsearch Domain</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Elasticsearch Service" /></td>
<td>Elasticsearch Domain Policy</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Elastictranscoder Pipeline</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Elastictranscoder Preset</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Elastic Load Balancing" /></td>
<td>Elb</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Elastic Load Balancing" /></td>
<td>Elb Attachment</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>-----------------------------</td>
<td>------------</td>
</tr>
<tr>
<td><img src="image" alt="EMR Icon" /></td>
<td>EMR Cluster</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="EMR Icon" /></td>
<td>Emr Cluster</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="EMR Icon" /></td>
<td>EMR Instance Fleet Config</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="EMR Icon" /></td>
<td>Emr Instance Group</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="EMR Icon" /></td>
<td>EMR Instance Group Config</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="EMR Icon" /></td>
<td>Emr Security Configuration</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="EMR Icon" /></td>
<td>EMR Security Configuration</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="EMR Icon" /></td>
<td>EMR Step</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Messaging Icon" /></td>
<td>Event Grid Domain</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Messaging Icon" /></td>
<td>Event Grid Event Subscription</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Messaging Icon" /></td>
<td>Event Grid Topic</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Messaging Icon" /></td>
<td>Event Hub</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Messaging Icon" /></td>
<td>Event Hub Authorization Rule</td>
<td>terraform</td>
</tr>
</tbody>
</table>

5.4. Compute
<table>
<thead>
<tr>
<th>ICON</th>
<th>RESOURCE NAME</th>
<th>PROVIDER</th>
</tr>
</thead>
<tbody>
<tr>
<td>📩 Messaging</td>
<td>Event Hub Consumer Group</td>
<td>terraform</td>
</tr>
<tr>
<td>📩 Messaging</td>
<td>Event Hub Disaster Recovery Config</td>
<td>terraform</td>
</tr>
<tr>
<td>📩 Messaging</td>
<td>Event Hub Namespace</td>
<td>terraform</td>
</tr>
<tr>
<td>📩 Messaging</td>
<td>Event Hub Namespace Authorization Rule</td>
<td>terraform</td>
</tr>
<tr>
<td>⚡️ Network</td>
<td>Express Route Circuit</td>
<td>terraform</td>
</tr>
<tr>
<td>⚡️ Network</td>
<td>Express Route Circuit</td>
<td>terraform</td>
</tr>
<tr>
<td>⚡️ Network</td>
<td>Express Route Circuit Authorization</td>
<td>terraform</td>
</tr>
<tr>
<td>⚡️ Network</td>
<td>Express Route Circuit Peering</td>
<td>terraform</td>
</tr>
<tr>
<td>⚡️ Network</td>
<td>Express Route Circuit Peering</td>
<td>terraform</td>
</tr>
<tr>
<td>⚡️ Network</td>
<td>Express Route Gateway</td>
<td>terraform</td>
</tr>
<tr>
<td>⚡️ Network</td>
<td>Express Route Gateway</td>
<td>terraform</td>
</tr>
<tr>
<td>⚡️ Network</td>
<td>Firewall</td>
<td>terraform</td>
</tr>
<tr>
<td>⚡️ Network</td>
<td>Firewall Application Rule Collection</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>![Network]</td>
<td>Firewall Nat Rule Collection</td>
<td>terraform</td>
</tr>
<tr>
<td>![Network]</td>
<td>Firewall Nat Rule Collection</td>
<td>terraform</td>
</tr>
<tr>
<td>![Network]</td>
<td>Firewall Network Rule Collection</td>
<td>terraform</td>
</tr>
<tr>
<td>![VPC]</td>
<td>Flow Log</td>
<td>terraform</td>
</tr>
<tr>
<td>![AWS Resource]</td>
<td>Fms Admin Account</td>
<td>terraform</td>
</tr>
<tr>
<td>![Front Door]</td>
<td>Front Door</td>
<td>terraform</td>
</tr>
<tr>
<td>![Front Door]</td>
<td>Front Door</td>
<td>terraform</td>
</tr>
<tr>
<td>![Front Door]</td>
<td>Front Door Firewall Policy</td>
<td>terraform</td>
</tr>
<tr>
<td>![Front Door]</td>
<td>Front Door Firewall Policy</td>
<td>terraform</td>
</tr>
<tr>
<td>![FSx]</td>
<td>Fsx Lustre File System</td>
<td>terraform</td>
</tr>
<tr>
<td>![FSx]</td>
<td>Fsx Windows File System</td>
<td>terraform</td>
</tr>
<tr>
<td>![Azure Resource]</td>
<td>Function App</td>
<td>terraform</td>
</tr>
<tr>
<td>![Azure Resource]</td>
<td>Function App Slot</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>🌐</td>
<td>Gamelift Alias</td>
<td>terraform</td>
</tr>
<tr>
<td>🌐</td>
<td>Gamelift Build</td>
<td>terraform</td>
</tr>
<tr>
<td>🌐</td>
<td>Gamelift Fleet</td>
<td>terraform</td>
</tr>
<tr>
<td>🌐</td>
<td>Gamelift Game Session Queue</td>
<td>terraform</td>
</tr>
<tr>
<td>🌐</td>
<td>Glacier Vault</td>
<td>terraform</td>
</tr>
<tr>
<td>🌐</td>
<td>Glacier Vault Lock</td>
<td>terraform</td>
</tr>
<tr>
<td>🌐</td>
<td>Globalaccelerator Accelerator</td>
<td>terraform</td>
</tr>
<tr>
<td>🌐</td>
<td>Globalaccelerator Endpoint Group</td>
<td>terraform</td>
</tr>
<tr>
<td>🌐</td>
<td>Globalaccelerator Listener</td>
<td>terraform</td>
</tr>
<tr>
<td>🌐</td>
<td>Glue Catalog Database</td>
<td>terraform</td>
</tr>
<tr>
<td>🌐</td>
<td>Glue Catalog Table</td>
<td>terraform</td>
</tr>
<tr>
<td>🌐</td>
<td>Glue Classifier</td>
<td>terraform</td>
</tr>
<tr>
<td>🌐</td>
<td>Glue Connection</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td><img src="image" alt="Glue" /></td>
<td>Glue Crawler</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Glue" /></td>
<td>Glue Job</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Glue" /></td>
<td>Glue Security Configuration</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Glue" /></td>
<td>Glue Trigger</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Glue" /></td>
<td>Glue Workflow</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Guardduty" /></td>
<td>Guardduty Detector</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Guardduty" /></td>
<td>Guardduty Invite Accepter</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Guardduty" /></td>
<td>Guardduty Ipset</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Guardduty" /></td>
<td>Guardduty Member</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Guardduty" /></td>
<td>Guardduty Organization Admin Account</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Guardduty" /></td>
<td>Guardduty Organization Configuration</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Guardduty" /></td>
<td>Guardduty Threatintelset</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="HDInsight" /></td>
<td>HD Insight Hadoop Cluster</td>
<td>terraform</td>
</tr>
</tbody>
</table>

5.4. Compute
<table>
<thead>
<tr>
<th>ICON</th>
<th>RESOURCE NAME</th>
<th>PROVIDER</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="HDInsight" /></td>
<td>HD Insight HBase Cluster</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="HDInsight" /></td>
<td>HD Insight Kafka Cluster</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="HDInsight" /></td>
<td>HD Insight ML Services Cluster</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="HDInsight" /></td>
<td>HD Insight Query Cluster</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="HDInsight" /></td>
<td>HD Insight R Cluster</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="HDInsight" /></td>
<td>HD Insight Spark Cluster</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="HDInsight" /></td>
<td>HD Insight Storm Cluster</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Healthcare API" /></td>
<td>Healthcare Service</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Healthcare API" /></td>
<td>Healthcare Service</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Storage" /></td>
<td>HPC Cache</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Storage" /></td>
<td>HPC Cache Blob Target</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Storage" /></td>
<td>HPC Cache Blob Target</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Storage" /></td>
<td>HPC Cache NFS Target</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td><img src="image" alt="Storage" /></td>
<td>HPC Cache NFS Target</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>IAM Access Key</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Iam Access Key</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Iam Account Alias</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Iam Account Password Policy</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>IAM Group</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Iam Group</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Iam Group Membership</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Iam Group Policy</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Iam Group Policy Attachment</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Iam Instance Profile</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>IAM Instance Profile</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>IAM Managed Policy</td>
<td>cloudFormation</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>-----------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Iam Openid Connect Provider</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Iam Policy</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>IAM Policy</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Iam Policy Attachment</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Iam Role</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>IAM Role</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Iam Role Policy</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Iam Role Policy Attachment</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Iam Saml Provider</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Iam Server Certificate</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Iam Service Linked Role</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>IAM Service Linked Role</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Iam User</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>IAM User</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>IAM User Group Addition</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Iam User Group Membership</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Iam User Login Profile</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Iam User Policy</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Iam User Policy Attachment</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Iam User Ssh Key</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Compute" /></td>
<td>Image</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Inspector Assessment Target</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Inspector Assessment Template</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Inspector Resource Group</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>Instance</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="VPC" /></td>
<td>Internet Gateway</td>
<td>terraform</td>
</tr>
</tbody>
</table>

Table 5 – continued from previous page

5.4. Compute
<table>
<thead>
<tr>
<th>ICON</th>
<th>RESOURCE NAME</th>
<th>PROVIDER</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="IoT Central Application" /></td>
<td>IOT Central Application</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image2" alt="AWS Resource" /></td>
<td>Iot Certificate</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image3" alt="IoT Hub" /></td>
<td>IOT Hub</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image3" alt="IoT Hub" /></td>
<td>IOT Hub Access Policy</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image3" alt="IoT Hub" /></td>
<td>IOT Hub Consumer Group</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image3" alt="IoT Hub" /></td>
<td>IOT Hub DPS</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image3" alt="IoT Hub" /></td>
<td>IOT Hub DPS Certificate</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image3" alt="IoT Hub" /></td>
<td>IOT Hub Endpoint Event Hub</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image3" alt="IoT Hub" /></td>
<td>IOT Hub Endpoint Event Hub</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image3" alt="IoT Hub" /></td>
<td>IOT Hub Endpoint Queue</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image3" alt="IoT Hub" /></td>
<td>IOT Hub Endpoint Storage</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image3" alt="IoT Hub" /></td>
<td>IOT Hub Endpoint Topic</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image3" alt="IoT Hub" /></td>
<td>IOT Hub Fallback Route</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>![IoT Hub]</td>
<td>IOT Hub Route</td>
<td>terraform</td>
</tr>
<tr>
<td>![IoT Hub]</td>
<td>IOT Hub Shared Access Policy</td>
<td>terraform</td>
</tr>
<tr>
<td>![AWS Resource]</td>
<td>Iot Policy</td>
<td>terraform</td>
</tr>
<tr>
<td>![AWS Resource]</td>
<td>Iot Policy Attachment</td>
<td>terraform</td>
</tr>
<tr>
<td>![AWS Resource]</td>
<td>Iot Role Alias</td>
<td>terraform</td>
</tr>
<tr>
<td>![AWS Resource]</td>
<td>Iot Thing</td>
<td>terraform</td>
</tr>
<tr>
<td>![AWS Resource]</td>
<td>Iot Thing Principal Attachment</td>
<td>terraform</td>
</tr>
<tr>
<td>![AWS Resource]</td>
<td>Iot Thing Type</td>
<td>terraform</td>
</tr>
<tr>
<td>![AWS Resource]</td>
<td>Iot Topic Rule</td>
<td>terraform</td>
</tr>
<tr>
<td>![EC2]</td>
<td>Key Pair</td>
<td>terraform</td>
</tr>
<tr>
<td>![Key Vault]</td>
<td>Key Vault</td>
<td>terraform</td>
</tr>
<tr>
<td>![Key Vault]</td>
<td>Key Vault Access Policy</td>
<td>terraform</td>
</tr>
<tr>
<td>![Key Vault]</td>
<td>Key Vault Access Policy</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>---------------</td>
<td>----------</td>
</tr>
<tr>
<td><img src="image1" alt="Key Vault" /></td>
<td>Key Vault Certificate</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image2" alt="Key Vault" /></td>
<td>Key Vault Certificate</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image3" alt="Key Vault" /></td>
<td>Key Vault Key</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image4" alt="Key Vault" /></td>
<td>Key Vault Key</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image5" alt="Key Vault" /></td>
<td>Key Vault Secret</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image6" alt="Key Vault" /></td>
<td>Key Vault Secret</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image7" alt="Kinesis" /></td>
<td>Kinesis Analytics Application</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image8" alt="Kinesis" /></td>
<td>Kinesis Firehose Delivery Stream</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image9" alt="Kinesis" /></td>
<td>Kinesis Stream</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image10" alt="Kinesis" /></td>
<td>Kinesis Stream</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image11" alt="Kinesis" /></td>
<td>Kinesis Stream Consumer</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image12" alt="Kinesis" /></td>
<td>Kinesis Video Stream</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image13" alt="AWS Resource" /></td>
<td>Kms Alias</td>
<td>terraform</td>
</tr>
</tbody>
</table>
Table 5 – continued from previous page

<table>
<thead>
<tr>
<th>ICON</th>
<th>RESOURCE NAME</th>
<th>PROVIDER</th>
</tr>
</thead>
<tbody>
<tr>
<td>![AWS Resource Icon]</td>
<td>Kms Ciphertext</td>
<td>terraform</td>
</tr>
<tr>
<td>![AWS Resource Icon]</td>
<td>Kms External Key</td>
<td>terraform</td>
</tr>
<tr>
<td>![AWS Resource Icon]</td>
<td>Kms Grant</td>
<td>terraform</td>
</tr>
<tr>
<td>![AWS Resource Icon]</td>
<td>Kms Key</td>
<td>terraform</td>
</tr>
<tr>
<td>![Container Icon]</td>
<td>Kubernetes Cluster</td>
<td>terraform</td>
</tr>
<tr>
<td>![Container Icon]</td>
<td>Kubernetes Cluster</td>
<td>terraform</td>
</tr>
<tr>
<td>![Container Icon]</td>
<td>Kubernetes Node Pool</td>
<td>terraform</td>
</tr>
<tr>
<td>![Container Icon]</td>
<td>Kubernetes Node Pool</td>
<td>terraform</td>
</tr>
<tr>
<td>![Data Explorer Icon]</td>
<td>Kusto Cluster</td>
<td>terraform</td>
</tr>
<tr>
<td>![Data Explorer Icon]</td>
<td>Kusto Database</td>
<td>terraform</td>
</tr>
<tr>
<td>![Data Explorer Icon]</td>
<td>Kusto Database Principal</td>
<td>terraform</td>
</tr>
<tr>
<td>![Data Explorer Icon]</td>
<td>Kusto Event Data Connection</td>
<td>terraform</td>
</tr>
<tr>
<td>![Lambda Icon]</td>
<td>Lambda Alias</td>
<td>cloudFormation</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td><img src="image" alt="Lambda Alias" /></td>
<td>Lambda Alias</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Lambda Event Source Mapping" /></td>
<td>Lambda Event Source Mapping</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Lambda Event Source Mapping" /></td>
<td>Lambda Event Source Mapping</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Lambda Function" /></td>
<td>Lambda Function</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Lambda Function" /></td>
<td>Lambda Function</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Lambda Function Event Invoke Config" /></td>
<td>Lambda Function Event Invoke Config</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Lambda Layer Version" /></td>
<td>Lambda Layer Version</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Lambda Layer Version" /></td>
<td>Lambda Layer Version</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Lambda Layer Version Permission" /></td>
<td>Lambda Layer Version Permission</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Lambda Permission" /></td>
<td>Lambda Permission</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Lambda Permission" /></td>
<td>Lambda Permission</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Lambda Provisioned Concurrency Config" /></td>
<td>Lambda Provisioned Concurrency Config</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Lambda Version" /></td>
<td>Lambda Version</td>
<td>cloudFormation</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>Launch Configuration</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>Launch Template</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Elastic Load Balancing" /></td>
<td>Lb</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Elastic Load Balancing" /></td>
<td>Lb Cookie Stickiness Policy</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Elastic Load Balancing" /></td>
<td>Lb Listener</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Elastic Load Balancing" /></td>
<td>Lb Listener Certificate</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Elastic Load Balancing" /></td>
<td>Lb Listener Rule</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Elastic Load Balancing" /></td>
<td>Lb Ssl Negotiation Policy</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Elastic Load Balancing" /></td>
<td>Lb Target Group</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Elastic Load Balancing" /></td>
<td>Lb Target Group Attachment</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Licensemanager Association</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Licensemanager License Configuration</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Amazon Lightsail" /></td>
<td>Lightsail Domain</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td><img src="image" alt="Amazon Lightsail" /></td>
<td>Lightsail Instance</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Amazon Lightsail" /></td>
<td>Lightsail Key Pair</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Amazon Lightsail" /></td>
<td>Lightsail Static Ip</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Amazon Lightsail" /></td>
<td>Lightsail Static Ip Attachment</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Compute" /></td>
<td>Linux VM Scale Set</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Load Balancer" /></td>
<td>Load Balancer</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Load Balancer" /></td>
<td>Load Balancer</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Load Balancer" /></td>
<td>Load Balancer Address Pool</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Load Balancer" /></td>
<td>Load Balancer Address Pool</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Elastic Load Balancing" /></td>
<td>Load Balancer Backend Server Policy</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Elastic Load Balancing" /></td>
<td>Load Balancer Listener Policy</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Load Balancer" /></td>
<td>Load Balancer Nat Pool</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Load Balancer" /></td>
<td>Load Balancer Nat Pool</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>-----------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>![Load Balancer]</td>
<td>Load Balancer Nat Rule</td>
<td>terraform</td>
</tr>
<tr>
<td>![Load Balancer]</td>
<td>Load Balancer Nat Rule</td>
<td>terraform</td>
</tr>
<tr>
<td>![Load Balancer]</td>
<td>Load Balancer Outbound Rule</td>
<td>terraform</td>
</tr>
<tr>
<td>![Load Balancer]</td>
<td>Load Balancer Outbound Rule</td>
<td>terraform</td>
</tr>
<tr>
<td>![Load Balancer]</td>
<td>Load Balancer Policy</td>
<td>terraform</td>
</tr>
<tr>
<td>![Load Balancer]</td>
<td>Load Balancer Probe</td>
<td>terraform</td>
</tr>
<tr>
<td>![Load Balancer]</td>
<td>Load Balancer Probe</td>
<td>terraform</td>
</tr>
<tr>
<td>![Load Balancer]</td>
<td>Load Balancer Rule</td>
<td>terraform</td>
</tr>
<tr>
<td>![Load Balancer]</td>
<td>Load Balancer Rule</td>
<td>terraform</td>
</tr>
<tr>
<td>![Network]</td>
<td>Local Network Gateway</td>
<td>terraform</td>
</tr>
<tr>
<td>![Log Analytics]</td>
<td>Log Analytics Linked Service</td>
<td>terraform</td>
</tr>
<tr>
<td>![Log Analytics]</td>
<td>Log Analytics Linked Service</td>
<td>terraform</td>
</tr>
<tr>
<td>![Log Analytics]</td>
<td>Log Analytics Solution</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>---------------</td>
<td>----------</td>
</tr>
<tr>
<td><img src="image" alt="Log Analytics Solution" /></td>
<td>Log Analytics Solution</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Log Analytics Windows Event" /></td>
<td>Log Analytics Windows Event</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Log Analytics Windows Event" /></td>
<td>Log Analytics Windows Event</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Log Analytics Windows Performance Counter" /></td>
<td>Log Analytics Windows Performance Counter</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Log Analytics Windows Performance Counter" /></td>
<td>Log Analytics Windows Performance Counter</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Log Analytics Workspace" /></td>
<td>Log Analytics Workspace</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Log Analytics Workspace" /></td>
<td>Log Analytics Workspace</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Logic App Custom Action" /></td>
<td>Logic App Custom Action</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Logic App Custom Action" /></td>
<td>Logic App Custom Action</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Logic App Custom Trigger" /></td>
<td>Logic App Custom Trigger</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Logic App Custom Trigger" /></td>
<td>Logic App Custom Trigger</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Logic App Http Action" /></td>
<td>Logic App Http Action</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Logic App Http Action" /></td>
<td>Logic App Http Action</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td><img src="image" alt="Logic App" /></td>
<td>Logic App Http Request</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Logic App" /></td>
<td>Logic App Http Request</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Logic App" /></td>
<td>Logic App Trigger Recurrence</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Logic App" /></td>
<td>Logic App Trigger Recurrence</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Logic App" /></td>
<td>Logic App Workflow</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Logic App" /></td>
<td>Logic App Workflow</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Machine Learning" /></td>
<td>Machine Learning Workspace</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Macie Member Account Association</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Macie S3 Bucket Association</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="VPC" /></td>
<td>Main Route Table Association</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Maintenance" /></td>
<td>Maintenance Configuration</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Maintenance" /></td>
<td>Maintenance Configuration</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Compute" /></td>
<td>Managed Application</td>
<td>terraform</td>
</tr>
</tbody>
</table>
Table 5 – continued from previous page

<table>
<thead>
<tr>
<th>ICON</th>
<th>RESOURCE NAME</th>
<th>PROVIDER</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Compute Icon" /></td>
<td>Managed Disk</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Management Icon" /></td>
<td>Management Group</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Management Icon" /></td>
<td>Management Group</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Management Icon" /></td>
<td>Management Lock</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Management Icon" /></td>
<td>Management Lock</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Maps Icon" /></td>
<td>Maps Account</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Maps Icon" /></td>
<td>Maps Account</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Database Icon" /></td>
<td>MariaDb Configuration</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Database Icon" /></td>
<td>MariaDb Database</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Database Icon" /></td>
<td>MariaDb Firewall Rule</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Database Icon" /></td>
<td>MariaDb Server</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Database Icon" /></td>
<td>MariaDb Virtual Network Rule</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Compute Icon" /></td>
<td>Marketplace Agreement</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>---------------</td>
<td>----------</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Media Convert Queue</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Media Package Channel</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Media" /></td>
<td>Media Services Account</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Media" /></td>
<td>Media Services Account</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Media Store Container</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Media Store Container Policy</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Monitor" /></td>
<td>Monitor Action Group</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Monitor" /></td>
<td>Monitor Action Group</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Monitor" /></td>
<td>Monitor Activity Log Alert</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Monitor" /></td>
<td>Monitor Activity Log Alert</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Monitor" /></td>
<td>Monitor Autoscale Setting</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Monitor" /></td>
<td>Monitor Autoscale Setting</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Monitor" /></td>
<td>Monitor Diagnostic Setting</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>----------------------------</td>
<td>------------</td>
</tr>
<tr>
<td><img src="image" alt="Monitor" /></td>
<td>Monitor Diagnostic Setting</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Monitor" /></td>
<td>Monitor Log Profile</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Monitor" /></td>
<td>Monitor Log Profile</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Monitor" /></td>
<td>Monitor Metric Alert</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Monitor" /></td>
<td>Monitor Metric Alert</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Monitor" /></td>
<td>Monitor Scheduled Query Rules Alert</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Monitor" /></td>
<td>Monitor Scheduled Query Rules Alert</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Monitor" /></td>
<td>Monitor Scheduled Query Rules Log</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Monitor" /></td>
<td>Monitor Scheduled Query Rules Log</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="MQ" /></td>
<td>MQ Broker</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="MQ" /></td>
<td>Mq Broker</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="MQ" /></td>
<td>MQ Configuration</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="MQ" /></td>
<td>Mq Configuration</td>
<td>terraform</td>
</tr>
</tbody>
</table>
Table 5 – continued from previous page

<table>
<thead>
<tr>
<th>ICON</th>
<th>RESOURCE NAME</th>
<th>PROVIDER</th>
</tr>
</thead>
<tbody>
<tr>
<td>🎄 MQ</td>
<td>MQ Configuration Association</td>
<td>cloudFormation</td>
</tr>
<tr>
<td>🇺🇸 Database</td>
<td>MS SQL Database</td>
<td>terraform</td>
</tr>
<tr>
<td>🇺🇸 Database</td>
<td>MS SQL Elastic Pool</td>
<td>terraform</td>
</tr>
<tr>
<td>🇺🇸 Database</td>
<td>MS SQL Security Alert Policy</td>
<td>terraform</td>
</tr>
<tr>
<td>🇺🇸 Database</td>
<td>MS SQL Server</td>
<td>terraform</td>
</tr>
<tr>
<td>🇺🇸 Database</td>
<td>MS SQL Vm</td>
<td>terraform</td>
</tr>
<tr>
<td>🇺🇸 Database</td>
<td>MS SQL Vulnerability Assessment</td>
<td>terraform</td>
</tr>
<tr>
<td>🇺🇸 Database</td>
<td>MS SQL Vulnerability Assessment Rule Baseline</td>
<td>terraform</td>
</tr>
<tr>
<td>🌐 AWS Resource</td>
<td>Msk Cluster</td>
<td>terraform</td>
</tr>
<tr>
<td>🌐 AWS Resource</td>
<td>Msk Configuration</td>
<td>terraform</td>
</tr>
<tr>
<td>🇺🇸 Database</td>
<td>MySQL Configuration</td>
<td>terraform</td>
</tr>
<tr>
<td>🇺🇸 Database</td>
<td>MySQL Database</td>
<td>terraform</td>
</tr>
<tr>
<td>🇺🇸 Database</td>
<td>MySQL Firewall Rule</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>---------------</td>
<td>----------</td>
</tr>
<tr>
<td>📖Database</td>
<td>MySQL Server</td>
<td>terraform</td>
</tr>
<tr>
<td>📖Database</td>
<td>MySQL Virtual Network Rule</td>
<td>terraform</td>
</tr>
<tr>
<td>💌Messaging</td>
<td>Namespace Authorization Rule</td>
<td>terraform</td>
</tr>
<tr>
<td>🌐Network</td>
<td>Nat Gateway</td>
<td>terraform</td>
</tr>
<tr>
<td>🌐Network</td>
<td>Nat Gateway</td>
<td>terraform</td>
</tr>
<tr>
<td>🌐Neptune</td>
<td>Neptune Cluster</td>
<td>terraform</td>
</tr>
<tr>
<td>🌐Neptune</td>
<td>Neptune Cluster Instance</td>
<td>terraform</td>
</tr>
<tr>
<td>🌐Neptune</td>
<td>Neptune Cluster Parameter Group</td>
<td>terraform</td>
</tr>
<tr>
<td>🌐Neptune</td>
<td>Neptune Cluster Snapshot</td>
<td>terraform</td>
</tr>
<tr>
<td>🌐Neptune</td>
<td>Neptune DB Cluster</td>
<td>cloudFormation</td>
</tr>
<tr>
<td>🌐Neptune</td>
<td>Neptune DB Cluster Parameter Group</td>
<td>cloudFormation</td>
</tr>
<tr>
<td>🌐Neptune</td>
<td>Neptune DB Instance</td>
<td>cloudFormation</td>
</tr>
<tr>
<td>🌐Neptune</td>
<td>Neptune DB Parameter Group</td>
<td>cloudFormation</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td><img src="image" alt="Neptune" /></td>
<td>Neptune DB Subnet Group</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Neptune" /></td>
<td>Neptune Event Subscription</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Neptune" /></td>
<td>Neptune Parameter Group</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Neptune" /></td>
<td>Neptune Subnet Group</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="NetApp" /></td>
<td>NetApp Account</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="NetApp" /></td>
<td>NetApp Account</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="NetApp" /></td>
<td>NetApp Pool</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="NetApp" /></td>
<td>NetApp Snapshot</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="NetApp" /></td>
<td>NetApp Snapshot</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="NetApp" /></td>
<td>NetApp Volume</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="NetApp" /></td>
<td>NetApp Volume</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="VPC" /></td>
<td>Network Acl</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="VPC" /></td>
<td>Network Acl Rule</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td></td>
<td>Network DDos Protection Plan</td>
<td>terraform</td>
</tr>
<tr>
<td></td>
<td>Network Gateway</td>
<td>terraform</td>
</tr>
<tr>
<td></td>
<td>Network Interface</td>
<td>terraform</td>
</tr>
<tr>
<td></td>
<td>Network Interface Application Gateway Backend Address Pool Association</td>
<td>terraform</td>
</tr>
<tr>
<td></td>
<td>Network Interface Application Security Group Association</td>
<td>terraform</td>
</tr>
<tr>
<td></td>
<td>Network Interface Attachment</td>
<td>terraform</td>
</tr>
<tr>
<td></td>
<td>Network Interface Backend Address Pool Association</td>
<td>terraform</td>
</tr>
<tr>
<td></td>
<td>Network Interface Nat Rule Association</td>
<td>terraform</td>
</tr>
<tr>
<td></td>
<td>Network Interface Security Group Association</td>
<td>terraform</td>
</tr>
<tr>
<td></td>
<td>Network Interface Sg Attachment</td>
<td>terraform</td>
</tr>
<tr>
<td></td>
<td>Network Packet Capture</td>
<td>terraform</td>
</tr>
<tr>
<td></td>
<td>Network Profile</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>![Network]</td>
<td>Network Security Group</td>
<td>terraform</td>
</tr>
<tr>
<td>![Network]</td>
<td>Network Security Rule</td>
<td>terraform</td>
</tr>
<tr>
<td>![Network]</td>
<td>Network Watcher</td>
<td>terraform</td>
</tr>
<tr>
<td>![Network]</td>
<td>Network Watcher Flow Log</td>
<td>terraform</td>
</tr>
<tr>
<td>![Messaging]</td>
<td>Notification Hub</td>
<td>terraform</td>
</tr>
<tr>
<td>![Messaging]</td>
<td>Notification Hub Authorization Rule</td>
<td>terraform</td>
</tr>
<tr>
<td>![Messaging]</td>
<td>Notification Hub Namespace</td>
<td>terraform</td>
</tr>
<tr>
<td>![AWS Resource]</td>
<td>Opsworks Application</td>
<td>terraform</td>
</tr>
<tr>
<td>![AWS Resource]</td>
<td>Opsworks Custom Layer</td>
<td>terraform</td>
</tr>
<tr>
<td>![AWS Resource]</td>
<td>Opsworks Ganglia Layer</td>
<td>terraform</td>
</tr>
<tr>
<td>![AWS Resource]</td>
<td>Opsworks Haproxy Layer</td>
<td>terraform</td>
</tr>
<tr>
<td>![AWS Resource]</td>
<td>Opsworks Instance</td>
<td>terraform</td>
</tr>
<tr>
<td>![AWS Resource]</td>
<td>Opsworks Java App Layer</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>---------------------</td>
<td>----------</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Opsworks Memcached Layer</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Opsworks Mysql Layer</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Opsworks Nodejs App Layer</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Opsworks Permission</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Opsworks Php App Layer</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Opsworks Rails App Layer</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Opsworks Rds Db Instance</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Opsworks Stack</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Opsworks Static Web Layer</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Opsworks User Profile</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Organizations Account</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Organizations Organization</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Organizations Organizational Unit</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>-----------------------------</td>
<td>----------</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Organizations Policy</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Organizations Policy Attachment</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Network" /></td>
<td>Packet Capture</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Pinpoint Adm Channel</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Pinpoint Apns Channel</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Pinpoint Apns Sandbox Channel</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Pinpoint Apns Voip Channel</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Pinpoint Apns Voip Sandbox Channel</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Pinpoint App</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Pinpoint Baidu Channel</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Pinpoint Email Channel</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Pinpoint Event Stream</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Pinpoint Gcm Channel</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>----------------------</td>
<td>----------------------------</td>
<td>----------</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Pinpoint Sms Channel</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Compute" /></td>
<td>Placement Group</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="EC2" /></td>
<td>Placement Group</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Network" /></td>
<td>Point To Site VPN Gateway</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Policy" /></td>
<td>Policy Assignment</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Policy" /></td>
<td>Policy Assignment</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Policy" /></td>
<td>Policy Definition</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Policy" /></td>
<td>Policy Definition</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Policy" /></td>
<td>Policy Remediation</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Policy" /></td>
<td>Policy Remediation</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Policy" /></td>
<td>Policy Set Definition</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Policy" /></td>
<td>Policy Set Definition</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Database" /></td>
<td>PostgreSQL Configuration</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td><img src="image" alt="Database" /></td>
<td>PostgreSQL Database</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Database" /></td>
<td>PostgreSQL Firewall Rule</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Database" /></td>
<td>PostgreSQL Server</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Database" /></td>
<td>PostgreSQL Virtual Network Rule</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="PowerBI" /></td>
<td>PowerBI</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="DNS" /></td>
<td>Private DNS A Record</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="DNS" /></td>
<td>Private DNS A Record</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="DNS" /></td>
<td>Private DNS AAAA Record</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="DNS" /></td>
<td>Private DNS AAAA Record</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="DNS" /></td>
<td>Private DNS CName Record</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="DNS" /></td>
<td>Private DNS CName Record</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="DNS" /></td>
<td>Private DNS MX Record</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="DNS" /></td>
<td>Private DNS MX Record</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>----------</td>
<td>--------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>![DNS]</td>
<td>Private DNS Ptr Record</td>
<td>terraform</td>
</tr>
<tr>
<td>![DNS]</td>
<td>Private DNS Ptr Record</td>
<td>terraform</td>
</tr>
<tr>
<td>![DNS]</td>
<td>Private DNS Srv Record</td>
<td>terraform</td>
</tr>
<tr>
<td>![DNS]</td>
<td>Private DNS Srv Record</td>
<td>terraform</td>
</tr>
<tr>
<td>![DNS]</td>
<td>Private DNS Text Record</td>
<td>terraform</td>
</tr>
<tr>
<td>![DNS]</td>
<td>Private DNS Text Record</td>
<td>terraform</td>
</tr>
<tr>
<td>![DNS]</td>
<td>Private DNS Text Record</td>
<td>terraform</td>
</tr>
<tr>
<td>![DNS]</td>
<td>Private DNS Zone</td>
<td>terraform</td>
</tr>
<tr>
<td>![DNS]</td>
<td>Private DNS Zone</td>
<td>terraform</td>
</tr>
<tr>
<td>![DNS]</td>
<td>Private DNS Zone Virtual Network Link</td>
<td>terraform</td>
</tr>
<tr>
<td>![DNS]</td>
<td>Private DNS Zone Virtual Network Link</td>
<td>terraform</td>
</tr>
<tr>
<td>![Network]</td>
<td>Private Endpoint</td>
<td>terraform</td>
</tr>
<tr>
<td>![Network]</td>
<td>Private Link Service</td>
<td>terraform</td>
</tr>
<tr>
<td>![Network]</td>
<td>Private Link Service</td>
<td>terraform</td>
</tr>
<tr>
<td>ICON</td>
<td>RESOURCE NAME</td>
<td>PROVIDER</td>
</tr>
<tr>
<td>------</td>
<td>---------------</td>
<td>----------</td>
</tr>
<tr>
<td><img src="image" alt="Elastic Load Balancing" /></td>
<td>Proxy Protocol Policy</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Network" /></td>
<td>Public IP</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Network" /></td>
<td>Public IP Prefix</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Qldb Ledger</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Messaging" /></td>
<td>Queue Authorization Rule</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Messaging" /></td>
<td>Queue Authorization Rule</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Quicksight" /></td>
<td>Quicksight Group</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Quicksight" /></td>
<td>Quicksight User</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Ram Principal Association</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Ram Resource Association</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Ram Resource Share</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="AWS Resource" /></td>
<td>Ram Resource Share Accepter</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="RDS" /></td>
<td>Rds Cluster</td>
<td>terraform</td>
</tr>
</tbody>
</table>

5.4. Compute 379
<table>
<thead>
<tr>
<th>ICON</th>
<th>RESOURCE NAME</th>
<th>PROVIDER</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="ICON" alt="RDS" /></td>
<td>Rds Cluster Endpoint</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="ICON" alt="RDS" /></td>
<td>Rds Cluster Instance</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="ICON" alt="RDS" /></td>
<td>Rds Cluster Parameter Group</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="ICON" alt="RDS" /></td>
<td>RDS DB Cluster</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="ICON" alt="RDS" /></td>
<td>RDS DB Cluster ParameterGroup</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="ICON" alt="RDS" /></td>
<td>RDS DB Instance</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="ICON" alt="RDS" /></td>
<td>RDS DB Parameter Group</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="ICON" alt="RDS" /></td>
<td>RDS DB Security Group</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="ICON" alt="RDS" /></td>
<td>RDS DB Security Group Ingress</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="ICON" alt="RDS" /></td>
<td>RDS DB Subnet Group</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="ICON" alt="RDS" /></td>
<td>RDS Event Subscription</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="ICON" alt="RDS" /></td>
<td>Rds Global Cluster</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="ICON" alt="RDS" /></td>
<td>RDS Option Group</td>
<td>cloudFormation</td>
</tr>
</tbody>
</table>
### Table 5 – continued from previous page

<table>
<thead>
<tr>
<th>ICON</th>
<th>RESOURCE NAME</th>
<th>PROVIDER</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Recovery" /></td>
<td>Recovery Services Vault</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Recovery" /></td>
<td>Recovery Services Vault</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Recovery" /></td>
<td>Redis Cache</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Recovery" /></td>
<td>Redis Firewall Rule</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Redshift" /></td>
<td>Redshift Cluster</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Redshift" /></td>
<td>Redshift Cluster</td>
<td>terraform</td>
</tr>
<tr>
<td><img src="image" alt="Redshift" /></td>
<td>Redshift Cluster Parameter Group</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Redshift" /></td>
<td>Redshift Cluster Security Group</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Redshift" /></td>
<td>Redshift Cluster Security Group Ingress</td>
<td>cloudFormation</td>
</tr>
<tr>
<td><img src="image" alt="Redshift" /></td>
<td>Redshift Cluster Subnet Group</td>
<td>cloudFormation</td>
</tr>
</tbody>
</table>

#### 5.4.5 Bare Metal

- Standard Filters: OS Type
- Advanced Filters: Status Managed Server Type

---

**Section Features & Filters**
- Record Search
- Custom Views
- CSV Export
- JSON Export
- Export Paging
- Config
Bare Metal hosts are from discovered, PXE Boot or manually added Bare Metal hosts. Bare Metal hosts that are also Hypervisors will be listed in the Hosts section.

5.5 Network

5.5.1 Networks

Infrastructure > Network > Networks

Overview

The Networks section is for configuring networks across all clouds in Morpheus. Existing networks from Clouds added in Morpheus will auto-populate in the Networks section.

Networks can be configured for DHCP or Static IP assignment, assigned IP pools, and configured for visibility and account assignment for multi-tenancy usage. Inactive Networks are unavailable for provisioning use. In addition, Morpheus allows administrators to restrict management of Morpheus-created Networks through Role permissions.

Configuring Networks

DHCP

To configure a network for DHCP:

1. Navigate to Infrastructure > Network > Networks
2. Search for the target network
3. Edit the Network by either:
   - Select Actions > Edit
   - Select the Network, then select Edit
4. In the Network Config modal, set the DHCP flag as Active (default)
5. Save Changes

Important:  The DHCP flag tells Morpheus this network has a DHCP server assigning IP Addresses to hosts. Morpheus does not act as the DHCP server, and provisioning to a network that has the DHCP server flag active in Morpheus, but no DHCP server actually on the network will in most cases cause the instance to not receive an IP address.

Note: When selecting a network with DHCP enabled during provisioning, “DHCP” will populate to the right of the selected network:
**Static and IP Pools**

To configure a network for Static IP Assignment:

1. Navigate to *Infrastructure > Network > Networks*
2. Search for the target network
3. Edit the Network by either:
   - Select *Actions > Edit*
   - Select the Network, then select *Edit*
4. In the Network Config modal, add the following:
   - Gateway
   - DNS Primary
   - DNS Secondary
   - CIDR ex 10.10.10.0/22
   - VLAN ID (if necessary)
   - Network Pool * Leave as “choose a pool” for entering a static IP while provisioning * Select a Pool to use a pre-configured Morpheus or IPAM Integration IP Pool
   - The Permissions settings are used for Multi-Tenant resource configuration
     - Leave settings as default if used in a single-tenant environment (only one Tenant in your Morpheus appliance)
     - To share this network across all accounts in a multi-tenant environment, select the Master Tenant and set the Visibility to Public
     - To assign this network to be used by only one account in a multi-tenant environment, select the account and set visibility to Private
   - Active
     - Leave as enabled to use this network
     - Disable the active flag to remove this network from available network options
5. Save Changes

---

**Note:** When selecting a network with DHCP disabled and no IP Pool assigned during provisioning, an IP entry field will populate to the right of the selected network(s):

---

**Note:** When selecting a network with an IP Pool assigned during provisioning, the name of the IP pool will populate to the right of the selected network(s). IP Pools override DHCP.
Advanced Options (Scan Network)

When adding or editing a network there is an option to scan network. If checked scan network will ping the IP’s in the network range, and if ping is successful Morpheus will quickly check for listening ports on the IP.

**Important:** Network scanning may cause network monitoring or other alerts

Subnets

Subnet details can be viewed from the *SUBNETS* tab on the detail page of a specific network. From the *SUBNETS* tab, Morpheus allows the user to search and edit existing subnets.

In an Azure VNet, you can also create new subnets with the +*ADD* button.
CREATE SUBNET

- **TYPE**: Azure Subnet
- **SUBNET NAME**: 
- **SUBNET CIDR**: 
  The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network.
- **ACTIVE**: 
- **CIDR**: 0.0.0.0/1
- **DHCP SERVER**: 
- **ALLOW IP OVERRIDE**: 
- **NETWORK POOL**: Choose a pool
- **Group Access**
- **Tenant Permissions**

**SAVE CHANGES**
5.5.2 Network Groups

Network Groups are useful for grouping networks during provisioning and scaling or grouping availability subnets together such that during provisioning vm’s within an instance can be round robin provisioned across availability zones.

Adding Network Groups

1. Navigate to Infrastructure > Network > Networks Groups
2. Select ADD
3. Enter the following:
   Group info:
   - Name: Name of the Network Group in Morpheus
   - Description: Details of the Network Group in Morpheus

   Networks
   - Search for and select target Networks for the Network Group
   - Search for and select target Subnets for the Network Group

   Group Access
   - Set Group Access and Defaults for the Network Group

   Tenant Permissions
   - Set Tenant Visibility for Network Group
4. Select SAVE CHANGES

5.5.3 Routers

Overview

Routers can be viewed, created, and managed from the Routers tab of the Infrastructure > Networks page. Morpheus supports the creation of the following router types depending on networks that are currently configured:

- Amazon Internet Gateway
- Huawei Router
- Neutron Router
- NSX Edge Gateway
- NSX Edge Logical Router
- NSX-T Cloud Tier0 Gateway
- NSX-T Cloud Tier1 Gateway
- NSX-T Tier0 Gateway
- NSX-T Tier1 Gateway
- Open Telekom Router
Create New Router

1. Navigate to Infrastructure > Networks > Routers tab
2. Click + ADD
3. Select the router type and complete the fields on the resulting modal
4. Once complete, click ADD NETWORK ROUTER

Editing Existing Routers

1. Navigate to Infrastructure > Networks > Routers tab
2. Click on the pencil icon for the appropriate router
3. After editing router fields, click SAVE

Deleting Existing Routers

1. Navigate to Infrastructure > Networks > Routers tab
2. Click on the trash can icon for the appropriate router
3. Acknowledge the pop-up banner ensuring you wish to delete the router

5.5.4 IP Pools

Infrastructure > Network > IP Pools

Overview

The IP Pools tab in the Networks section allows you to create Morpheus-type IP Pools (which is an IP address range Morpheus can use to assign available static IP addresses to Instances) and NSX-T IP Pools. The IP Pool section also displays pools synced from IPAM integrations like Infoblox, Bluecat and others.

To add a Morpheus Network Pool

1. Click + ADD in Infrastructure > Network > IP Pools
2. Enter the following:
   - **Name**: A friendly name for the IP Pool in Morpheus.
   - **Pool Type**: Currently Morpheus-type IP Pools and NSX-T IP Pools (with a configured integration) can be created directly from Morpheus
   - **Starting Address**: The starting IP address of the IP Pool address range. ex: 192.168.0.2
   - **Ending Address**: The ending IP address of the IP Pool address range. ex: 192.168.0.255
3. Save Changes

**Note**: Multiple Address Ranges can be added to a pool by selecting the + icon next to the address range.
After saving the IP pool will be available for assignment to networks in the NETWORK POOL dropdown when adding or editing a network.

### 5.5.5 Domains

**Infrastructure > Network > Domains**

**Overview**

The Domains section is for creating and managing domains for use in Morpheus. Domains are used for setting FQDNs, joining Domains, and creating DNS records. The Domains section is also a multi-tenant endpoint for managing domain settings across multiple tenants.

- Domains are synced in from Cloud, DNS and Network Integrations. Domains can also be user created.
- Active Domains are available for selection in the Domain dropdown when provisioning an Instance
- Default Domains can be set for Clouds and Networks in their Advanced Options sections.
- Images can be flagged to Auto-Join Domains in the `LibVir` section

**Important:** For an Instance to auto-join a Domain, a Domain must set in the Advanced Options section of the Cloud or Network used when provisioning

**Adding Domains**

1. Navigate to **Infrastructure > Network > Domains**
2. Select `ADD`
3. Enter the following:
   - **Domain Name** Ex. demo.example.com
   - **Description** Descriptive metadata for use in Morpheus
   - **Display Name** Overrides the displayed name in domain selection components, which is useful when using many OU paths
   - **Public Zone** Check for Public Zones, leave uncheck for Private Zones
   - **Workflow** Select an existing Workflow which will be applied to Instances at provision time when they are associated with the domain. This is useful for any domain-related scripting you may currently use. For example, you may want to ensure a machine is removed from the domain when it's torn down which could be accomplished by creating a Provisioning Workflow (with teardown phase Tasks) and associating the Workflow with the domain
   - **Active** Active Domains are available for selection in Domain selection fields across Morpheus. Inactive Domains are removed from Domain selection fields.
   - **Join Domain Controller** Check to have Windows instances join a Domain Controller
   - **Username** Admin user for Domain Controller. `domain\username` format required when specifying OU Path
   - **Password** Password for DC user account
   - **DC Server** (optional) Specify the URL or Path of the DC Server
**OU Path** (optional) Enter the OU Path for the connection string.

**Guest Username** (optional) If set, this will change the provisioned hosts RPC Service User after domain join. Useful when a domain policy disables the Administrator account that typically would be set as the RPC user on a host record. Morpheus will update the RPC username and password on the host(s) record after domain join with the specified Guest Username and Guest Password. The RPC username and password are used for auth during Remote Procedure Call (RPC) executions over winrm, ssh and guest tools.

**Guest Password** (optional) The password for the Guest User account indicated in the prior field.

4. Click *Save Changes*

The Domain has been added and will be selectable in the Domain dropdown during provisioning, and in Cloud and Network settings.

**Editing Domain Permissions**

To edit visibility permissions for a domain, navigate to **Infrastructure > Network > Domains**. In the row for the selected domain, click MORE > Permissions. Within the Permissions modal, set Group and Tenant access permissions.

**Note:** Only resources assigned to the Master Tenant can be set as Publicly visible. If the Tenant assigned is not the Master Tenant, visibility will automatically change to private. Additionally, only Master Tenant users can set visibility for domains. Domains originating in a subtenant will always be private to that subtenant.

**Group Access**

Configure the domain to be visible to all Infrastructure Groups or only to selected Groups. If the domain is scoped to specific Groups, Users whose Roles do not give them Group access will not have access to the domain. Additionally, users will not be able to set the domain as the default on a Cloud which is not a part of the selected Groups.

**Tenant Permissions**

When set to public, all Tenants will have visibility into the domain and can join their Instances to the domain. When set to private, users can select specific Tenants which should have access to the domain.

**Editing and Removing Domains**

- Domains can be edited by selecting the *Actions* dropdown for the Domain and selecting *Edit*, or by selecting the icon in list views.
- Added Domains can be removed from Morpheus by selecting the *Actions* dropdown for the Domain and selecting *Remove*, or the icon in list views.
Setting the default domain on a Cloud

1. Navigate to Infrastructure > Clouds.
2. Edit the target Cloud.
3. Expand Advanced Options section.
4. In the Domain dropdown, select the Domain.
5. Save Changes

Setting the default domain on a Network

1. Navigate to Infrastructure > Network.
2. Edit the target Network.
3. Expand Advanced Options section.
4. In the Domain dropdown, select the Domain.
5. Save Changes

Selecting a Domain while provisioning an instance

1. While creating an instance, in the Configure section, expand the DNS Options.
2. Select Domain from the Domain dropdown.

5.5.6 Proxies

Overview

In many situations, companies deploy virtual machines in proxy restricted environments for things such as PCI Compliance, or just general security. As a result of this, Morpheus provides out of the box support for proxy connectivity. Proxy authentication support is also provided with both Basic Authentication capabilities as well as NTLM for Windows Proxy environments. Morpheus is even able to configure virtual machines it provisions to utilize these proxies by setting up the operating systems proxy settings directly (restricted to cloud-init based Linux platforms for now, but can also be done on windows based platforms in a different manner).

To get started with Proxies, it may first be important to configure the Morpheus appliance itself to have access to proxy communication for downloading service catalog images. To configure this, visit the Administration > Settings page where a section labeled “Proxy Settings” is located. Fill in the relevant connection info needed to utilize the proxy. It may also be advised to ensure that the Linux environment’s http_proxy, https_proxy, and no_proxy are set appropriately.
Defining Proxies

Proxies can be used in a few different contexts and optionally scoped to specific networks with which one may be provisioning into or on a cloud integration as a whole. To configure a Proxy for use by the provisioning engines within Morpheus we must go to Infrastructure > Networks > Proxies. Here we can create records representing connection information for various proxies. This includes the host ip address, proxy port, and any credentials (if necessary) needed to utilize the proxy. Now that these proxies are defined we can use them in various contexts.

Cloud Communication

When morpheus needs to connect to various cloud APIs to issue provisioning commands or to sync in existing environments, we need to ensure that those api endpoints are accessible by the appliance. In some cases the appliance may be behind a proxy when it comes to public cloud access like Azure and AWS. To configure the cloud integration to utilize a proxy, when adding or editing a cloud there is a setting called “API Proxy” under “Advanced Options”. This is where the proxy of choice can be selected to instruct the Provisioning engine how to communicate with the public cloud. Simply adjust this setting and the cloud should start being able to receive/issue instructions.

Provisioning with Proxies

Proxy configurations can vary from operating system to operating system and in some cases it is necessary for these to be configured in the blueprint as a prerequisite. In other cases it can also be configured automatically. Mostly with the use of cloud-init (which all of our out of the box service catalog utilizes on all clouds). When editing/creating a cloud there is a setting for “Provisioning Proxy” in “Provisioning Options”. If this proxy is set, Morpheus will automatically apply these proxy settings to the guest operating system.

Overriding proxy settings can also be done on the Network record. Networks (or subnets) can be configured in Infrastructure > Networks or on the Networks tab of the relevant Cloud detail page. Here, a proxy can also be assigned as well as additional options like the No Proxy rules for proxy exceptions.

Docker

When provisioning Docker based hosts within a Proxy environment it is up to the user to configure the docker host proxy configuration manually. There are workflows that can be configured via the Automation engine to make this automatic when creating docker based hosts. Please see documentation on Docker and proxies for specific information.

Proxy setups can vary widely from company to company, and it may be advised to contact support for help configuring morpheus to work in the proxy environment.

5.5.7 Security Groups

Infrastructure > Network – Security Groups
Overview

A security group acts as a virtual firewall that controls the traffic for one or more Instances. When you launch an instance, you associate one or more security groups with the instance. You add rules to each security group that allow traffic to or from its associated Instances. You can modify the rules for a security group at any time; the new rules are automatically applied to all Instances that are associated with the security group.

**Important:** The Host Level Firewall must be enabled for Security Groups to be applied. The Host Level Firewall can be enabled in Administration > Settings > Provisioning > Host Level Firewall Enable/Disable

**Important:** When local firewall management is enabled, Morpheus will automatically set an IP table rule to allow incoming connections on tcp port 22 from the Morpheus Appliance.

Add Security Group

1. Navigate to *Infrastructure > Network - Security Groups*
2. Click the *+ Add Security Group* button.
3. From the Security Group Wizard input a name, and description.
4. Save Changes

Add Security Group Rule

1. Navigate to *Infrastructure > Network - Security Groups*
2. Click the name of the security group you wish to add a rule to.
3. From the security group page click the *+ Add Rule* button.
4. From the Rule Wizard select the rule type and input source and depending on the type selected protocol and input a port range.
5. Save Changes

Edit security group rule

1. Navigate to *Infrastructure > Network - Security Groups*
2. Click the name of the security group you wish to edit a rule in.
3. Click the edit icon on the row of the security group rule you wish to edit.
4. Modify information as needed.
5. Save Changes
Delete security group rule

1. Navigate to Infrastructure > Network - Security Groups
2. Click the name of the security group you wish to delete a rule from.
3. Click the delete icon on the row of the security group rule you wish to delete.

Add Cloud Security Group

To add Cloud security group

1. Navigate to Infrastructure > Clouds
2. Click the name of the desired cloud to add a security group
3. Click the Networks tab
4. Within the “Security Groups” section, click on a security group to edit its rules
5. Alternatively, click + ADD SECURITY GROUP to create a new one

Remove Cloud Security Group

1. Navigate to Infrastructure > Clouds
2. Click the name of the cloud to remove the Security Group from.
3. Click the Security Groups tab.
4. Click the Edit Security Groups button.
5. Click the - (Minus) button of the Security Group from the Added Security groups list to remove.
6. Save Changes

5.5.8 Integrations

Overview

The Network Integrations section allows you to add and manage IPAM, DNS, and Service Registry integrations. These services can also be added in the Administration > Integrations section.

The following integrations are currently supported:

Networking
- Cisco ACI
- VMWare NSX

IPAM
- Infoblox
- Bluecat
- phpIPAM

Security
- Cisco ACI
DNS
- Microsoft DNS
- PowerDNS
- Route 53

Scoping Services

NETWORKING  Networking integrations are available in the NETWORK MODE dropdown located under the Advanced Options section in Cloud configurations.

IPAM  IPAM integrations will populate pools in the IP Pool section, which are available for assignment to networks in the NETWORK POOL dropdown when configuring a network.

SECURITY  Security integrations are available in the SECURITY SERVER dropdown located under the Advanced Options section in Cloud configurations.

DNS  DNS integrations will populate domains in the Infrastructure > Network > Domains section, and are available in the DOMAIN dropdown located under the Advanced Options section in Cloud, Group, and Network configurations, as well as in the Configure section of the Create Instance wizard. DNS integrations are also available in the DNS SERVICE dropdown located under the Advanced Options section in Cloud and Group configurations.

Service Registry  Service Registry integrations are available in the SERVICE REGISTRY dropdown located under the Advanced Options section in Cloud and Group configurations.

Note:  Infoblox will also appear as a DNS INTEGRATION option in Clouds and Groups after adding Infoblox IPAM Integration.

5.6 Load Balancers

Infrastructure > Load Balancers

5.6.1 Overview

Morpheus can provision VM or Container HaProxy Load Balancers, Amazon Elastic and Application Load Balancers, Azure Load Balancers, and integrates with several external Load Balancers, including F5, A10, Citrix, and AVI.

Once created or integrated, Load Balancers are available as an option to be added during provision time or post-provisioning.

Once a Load Balancer is added to an instance, you can manually scale or configure auto-scaling based on thresholds or schedules, and burst across clouds with cloud priority.

In the Load Balancers page there are two sections:

Load Balancers  View or edit existing Load Balancers, add new Load Balancers.

Virtual Servers  View and link to Instances that are attached to load balancers.
5.6.2 Load Balancers

The Load Balancers tab list currently available Load Balancers, which you can select, edit or delete, and is where you can create new or integrate with external Load Balancers.

Add a new Load Balancer

Select + LOAD BALANCER, chose an option, and fill in the required information:

**A10 (aXAPI v3)**
- API Host
- API Port
- Username
- Password
- Internal IP
- Public IP
- VIP Address
- VIP Port

**Amazon ALB**
- Scheme
- Internal
- Internet-Facing
- Amazon Subnets (Select + to add additional) * Specify the subnets to enable for your load balancer. You can specify only one subnet per Availability Zone. You must specify subnets from at least two Availability Zones to increase the availability of your load balancer.
- Amazon Security Groups (Select + to add additional)

**AVI**
- API Host
- API Port
- Username
- Password
- Internal IP
- Public IP
- VIP Address
- VIP Port

**Azure Load Balancer**
- Cloud
- Resource Group * Populated from cloud selection

**Citrix NetScaler**
- API Host
• API Port
• Username
• Password

F5 BigIP (v11.4+)
• API Host
• API Port
• Username
• Password
• Management URL

FortiADC
• API HOST
• API PORT
• USERNAME
• PASSWORD
• INTERFACE (synced on auth)

HaProxy Container (Internal, will create a HaProxy container, must have available docker host to provision to)
• Group
• Cloud
• Name
• Description
• Plan * Select the size of HaProxy container to be provisioned

NSX-T Load Balancer
• NSX-T
• Name
• Description
• Enabled
• Admin State
• Size
• Tier-1 Gateways
• Log Level

Upon saving your new Load Balancer will be added to the Load Balancers list and available in the Load Balancer dropdown in the Provisioning Wizard Automation Section for Instance Types that have scaling enabled.
Load Balancer Detail Pages

In the main Load Balancer page, select an existing Load Balancer to go to that Load Balancers Details Page, which lists Stats, Settings, Actions and Virtual Servers for that load balancer.

5.6.3 Orchestrating Load Balancers

A large part of application orchestration and automation involves tying various web services and backend services into different load balancer configurations. If the automation tool is unable to communicate or integrate with this aspect of your infrastructure, a lot of gaps will be created in the full orchestrated flow of application deployment. This is why Morpheus provides deep integration with load balancers and explicit definitions with catalog items as to how they are connected to provisioned instances. Some of the functionality includes:

- Public Cloud Load Balancer Support
- Private Cloud Load Balancer Support
- Port Type definitions (Profiles like HTTP/HTTPS or UDP)
- SSL Certificate Management and SSL Certificate Upload
- SSL Passthrough or Forced Redirect

Not only does Morpheus have an ability to provision HAProxy based load balancer containers for easy consumption in development environments, but also has direct tie ins with several Load Balancer Types:

- F5 BigIP
- A10
- Netscaler
- AVI
- Amazon ELB
- Amazon ALB
- Azure Load Balancer
- Fortinet
- Openstack Octavia
- HA Proxy
- NSX-T

Morpheus exposes configuration options during provisioning of an Instance relevant and common to each supported LB Integration. In some cases, Morpheus also provides direct management and sync support for VIP configurations on the various Load Balancers (such as F5, and AVI), However in a day to day orchestrated workflow this would not be the ideal means by which a user should consume load balancer services.

By tying the Load Balancer associations into the provisioning of instances and the definition of the instance catalog item, the lifecycle of the VIP can more easily be maintained throughout the lifecycle of whatever application may be deployed.
Setting up an Instance for Load Balancer Consumption

Several of the provided Morpheus instance types are ready to go with load balancer orchestration out of the box (Apache, Nginx, Tomcat, Node.js, etc). It is also fairly easy to extend existing generic instance types during provisioning to be tied to load balancers or to set up said catalog items in advanced for such functionality.

When creating a custom Instance Type (in Library), one can define a list of exposed ports that the node type within the instance exposes. When defining these exposed ports it prompts for a Name, Port Number, and LB Type. The LB Type is what enables load-balancer functionality. This can either be HTTP, HTTPS, or TCP. This specification helps build the correct profile for the VIP as well as setup the appropriate types of Health Monitors within the target load balancer integration.

Now, when a user consumes this custom instance type (either through single instance provisioning or full application blueprint provisioning), a section appears in the Automation phase of provisioning. Each port that is defined that exposes a load-balancer gets a dropdown to choose which load balancer integration attach to the exposed port and various prompts become available.

These prompts control features ranging from target VIP Address to selecting an SSL Certificate to be applied to the VIP. These SSL Certificates will even go so far as to create SSL Profiles in integrations for things like an F5 automatically for the application. There are also external integrations for SSL Certificate management with Venafi which allows for the consumption of certificates managed by that external system.

Once the instance is provisioned, as part of the final phase, the load balancer configuration will be applied and maintained on the instance. This association can be manipulated after the fact via the “Scale” tab found on the Instance Detail page.

Another benefit to associating load-balancers this way is that the pool members are automatically maintained during scaling events, either via auto-scaling thresholds or manual node additions / removals.

5.6.4 F5 Load Balancers

Add F5 Load Balancer

To add a F5 Load Balancer Integration:

1. Navigate to Infrastructure > Load Balancers
2. Select + ADD
3. Select F5 BigIP
4. Fill in the following:
   - GROUP  Select the Group the Load Balancer will be available for
   - CLOUD  Select the Cloud the Load Balancer will be available for
   - NAME   Name of the Load Balancer in Morpheus
   - DESCRIPTION  Identifying information displayed on the Load Balancer list page.
   - VISIBILITY  Define Multi-Tenant permissions
   - API HOST  IP or resolvable hostname url.
   - API PORT  Typically 8443
   - USERNAME  API user
   - PASSWORD  API user password
MANAGEMENT URL  Example: https://10.30.20.31:8443/xui/

Advanced Options (optional)

- VIRTUAL NAME
- POOL NAME
- SERVER NAME

5. Save Changes

Virtual Servers

Instances attached to an F5 will be listed in the Virtual servers tab. Virtual servers can also be manually added in this section.

Add Virtual Server

1. Navigate to Infrastructure > Load Balancers
2. Select F5 Integration name to drill into the detail page
3. Select + ADD in the VIRTUAL SERVERS tab
4. Fill in the following:
   - **NAME**  Name of the Virtual Server in Morpheus
   - **DESCRIPTION**  Description of the Virtual Server in Morpheus
   - **Enabled**  Uncheck to keep the configuration but disable F5 availability in Morpheus
   - **VIP TYPE**
     - Standard
     - Forwarding (Layer 2)
     - Forwarding (IP)
     - Performance (HTTP)
     - Performance (Layer 4)
     - Stateless
     - Reject
     - DHCP
     - Internal
     - Message Routing
   - **VIP HOSTNAME**  Enter Hostname of the VIP (optional)
   - **VIP ADDRESS**  Enter IP address for the VIP
   - **VIP PORT**  Enter port used for the VIP
   - **SOURCE ADDRESS**  Enter Virtual Server source address
   - **PROTOCOL**  tcp, udp, or sctp
   - **PROFILES**  Search for and select from available PROFILES
Policies

Search for and select from available POLICIES

IRULES

Search for and select from available RUEL SCRIPTS

PERSISTENCE

- cookie
- dest-addr
- global-settings
- hash
- msrdp
- sip
- source-addr
- ssl
- universal

DEFAULT POOL

Select from available POOLS

5. Select SAVE CHANGES

Policies

Policies will be synced and listed in the Policies tab. These policies will be available options when creating Virtual Servers.

Pools

Create Pool

NAME

Name of the POOL in Morpheus

DESCRIPTION

Description of the POOL in Morpheus

BALANCE MODE

- Round Robin
- Least Connections

SERVICE PORT

Specify SERVICE PORT for the POOL

MEMBERS

Search for and select from available NODES

MONITORS

Search for and select from available Monitors
Profiles

SSL Profiles are synced and will be created when an SSL Certificate is assigned in the Load balancer section when provisioning or editing a Load balancer on an Instance.

Monitors

Create Monitor

NAME  Name of the MONITOR in Morpheus
DESCRIPTION  Description of the MONITOR in Morpheus
PARENT MONITOR  Select from available MONITORS
DESTINATION  Specify Destination, such a * : 443. Default is * : *
INTERVAL  Specify Monitor Interval. Default is 5
TIMEOUT  Specify Monitor Timeout. Default is 15
MONITOR CONFIG  Enter monitor config.

Nodes

Create Node

NAME  Name of the NODE in Morpheus
DESCRIPTION  Description of the NODE in Morpheus
ADDRESS  Enter node address
MONITOR  Select from available MONITORS
SERVICE PORT  Specify SERVICE PORT for the NODE

Rule Scripts

Rule Scripts will be synced and listed in the RULE SCRIPTS tab. These rules will be available options when creating Virtual Servers.

5.6.5 Citrix NetScaler
Add NetScaler Integration

To add a NetScaler Load Balancer Integration:

1. Navigate to *Infrastructure > Load Balancers*
2. Select + **ADD**
3. Select *Citrix NetScaler*
4. Fill in the following:
   - **GROUP** * Select the Group the Load Balancer will be available for.
   - **CLOUD** * Select the Cloud the Load Balancer will be available for.
   - **NAME** * Name of the Load Balancer in Morpheus.
   - **DESCRIPTION** Identifying information displayed on the Load Balancer list page.

**VISIBILITY**

Define Tenant Visibility

- **Public**: Available to all Tenants.
- **Private**: Only available to specified Tenant.

**Tenant** If Visibility is set to private, define the Tenant the Load Balancer will be available in.

**API URL** *

- **URL of the NetScaler API**
  - Example: http://10.30.21.55

**API PORT** *

- **NetScaler API port**
  - Example: 80

**USERNAME** * NetScaler service account username

**PASSWORD** * NetScaler service account password

**VIRTUAL NAME**

Naming Pattern for new NetScaler Virtual Servers

- If blank, defaults to *morph_lb_${loadBalancer.id}*

**SERVICE NAME**

Naming Pattern for new NetScaler Services

- If blank, defaults to *morph_service_${container.id}*

**SERVER NAME**

Naming Pattern for new NetScaler Servers

- If blank, defaults to *morph_server_${server.id}*
Add Load Balancer to Instance

Load Balancers can be added to Instances during Provisioning or to existing Instances. For Load Balancer settings to appear during provisioning, or for the scale tab to be available on an Instance, the instances Node Type must have a LB port defined.

**Note:** For Load Balancer settings to appear during provisioning, or for the scale tab to be available on an Instance, the instances Node Type must have a LB port defined.

Add Load Balancer during Provisioning

In the Instance Provisioning wizard, Load Balancers can be configured in the Automation > Load Balancer section.

1. Navigate to Provisioning > Instances.
2. Select **+ ADD**.
3. Select an Instance Type that supports scaling. (ENABLE SCALING (HORIZONTAL) flagged on Instance Type configuration)
4. Proceed with Instance configuration to the Automation section.
5. Fill in the following:
   - **VIP ADDRESS**
     - Define IP Address for the Virtual Server
     - Example: 10.30.23.191
   - **VIP PORT**
     - Define port for the Virtual Server
     - Example: 80
   - **VIP HOSTNAME**
     - Define hostname that will resolve to the VIP IP.
     - Example: jwDemoHaApp59.den.example.com
   - **VIRTUAL SERVICE NAME** Define name for the Virtual Service. Defaults to `${instance.name}`
   - **BALANCE MODE** Specify balance mode for the VIP
     - Least Connections
     - Round Robin
   - **STICKY MODE** Specify sticky session options for the VIP
     - Source IP
     - Cookie
   - **SHARED VIP ADDRESS** Select if VIP is shared, then enter DIRECT VIP ADDRESS
   - **SSL CERT**
SSL Certificate that will be applied to the VIP.

- No SSL
- Select existing Certificate from Infrastructure > Keys & Certs or from a Trust Provider Integration.

**USE EXTERNAL ADDRESS FOR Backend NODES**

- Select if traffic from LB to Backend Nodes needs to be sent to the External Addresses, or leave deselected to use Internal Addresses for Backed Nodes.

6. Optionally configure auto-scaling configuration in the Scale section

7. Select NEXT and provision the Instance.

After all nodes in the Instance are provisioned, the LB configuration will be added to the Instance and Virtual Servers, Services and Servers will be created and configured on the NetScaler. The Load Balancer settings and status will be visible in the Instance details page LOAD BALANCER section, with additional details, links, and configurations options available in the SCALE tab.

**5.7 Storage**

---

**Note:** In v3.5.2 STORAGE PROVIDERS has been split out into BUCKETS and FILE SHARES sections.

---

**5.7.1 Overview**

*Infrastructure > Storage* is for adding and managing Storage Buckets, File Shares, Volumes, Data Stores and Storage Servers for use with other Services in Morpheus.

**Role Requirements**

There are two Role permissions for the *Infrastructure > Storage* section: *Infrastructure: Storage* and *Infrastructure: Storage Browser*. *Infrastructure: Storage* give Full, Read or No access to the *Infrastructure > Storage* sections, while *Infrastructure: Storage Browser* is specific to *Buckets* and *Files Shares*. Full *Infrastructure: Storage Browser* permissions allows *Buckets* and *Files Shares* to be browsed and files and folders to be added, downloaded and deleted from the *Buckets* and *Files Shares*. Read *Infrastructure: Storage Browser* permissions allows *Buckets* and *Files Shares* to be browsed only.

**Default Storage**

The default Storage path for Virtual Images, Backups, Deployment Archives, Archive Service, and Archived Snapshots is *var/opt/morpheus/morpheus-ui/*. Its is recommended to add Storage Buckets and File Shares for these targets in the *Infrastructure > Storage* section to avoid running out of disk space on the Morpheus Appliance.
5.7.2 Storage Buckets

Storage Buckets are for Backup, Archives, Deployment and Virtual Images storage targets. Buckets can be browsed and files and folders can be uploaded, downloaded or deleted from the Bucket section. Retention Policies can be set on Storage Buckets for files to be deleted or backed up to another bucket after a set amount of time.

Supported Bucket Types

- Alibaba
- Amazon S3
- Azure
- Google Cloud Storage
- Openstack Swift
- Rackspace CDN

Alibaba Buckets

To Add an Alibaba Storage Bucket:

1. Select the Infrastructure link in the navigation bar.
2. Select the Storage link in the sub navigation bar.
3. In the BUCKETS tab, Click the + ADD button.
4. Select Alibaba from the dropdown list.
5. From the NEW BUCKET Wizard input the following:
   - NAME Name of the Bucket in Morpheus.
   - ACCESS KEY Alibaba Access Key
   - SECRET KEY Alibaba Secret Key
   - REGION Enter Alibaba Region for the Bucket
   - BUCKET NAME Enter existing Alibaba Bucket name, or to add a new Bucket enter a new name and select Create Bucket.
   - Create Bucket Enable if the Bucket entered in BUCKET NAME does not exist and needs to be created.
   - Default Backup Target Sets this Bucket as the default backup target when creating Backups. If selected the option to update existing Backup configuration to use this Bucket will be presented.
   - Archive Snapshots Enabled to export VM snapshots to this Bucket when creating VMware Backups, after which the snapshot will be removed from the target hypervisor.
   - Default Deployment Archive Target Sets this bucket as the default storage target when uploading Deployment files in the Deployments section.
   - Default Virtual Image Store Sets this bucket as the default storage target when uploading Virtual Images from the Virtual Images section, importing Images from Instance Actions, creating Images with the Image Builder and when creating new images from Migrations.
   - RETENTION POLICY
     - None Files in the Bucket will not be automatically deleted or backed up.
Backup Old Files

This option will backup files after a set amount of time and remove them from the bucket.

**DAYS OLD** Files older than the set number of days will be automatically backed up to the selected Backup Bucket.

**BACKUP BUCKET** Search for and then select the Bucket the files will be backed up to.

DELETE OLD FILES

This option will delete files from this bucket after a set amount of days.

**DAYS OLD** Files older than the set number of days will be automatically deleted from the Bucket.

6. Select **SAVE CHANGES**

The Bucket will be created and displayed in the Buckets tab.

• To browse, upload, download, or delete files from this Bucket, select the name of the Bucket.

• To edit the Bucket, select the edit icon or select the name of the Bucket and select **ACTIONS - EDIT**.

**Warning:** Repointing a bucket that is in use may cause loss of file references. Ensure data is mirrored first.

• To delete a Bucket, select the trash icon or select the name of the Bucket and select **DELETE**.

**Warning:** When deleting a Bucket, all Deployment Versions and Backups associated with the Bucket will be deleted.

Amazon S3 Buckets

To Add an Amazon S3 Storage Bucket:

1. Select the Infrastructure link in the navigation bar.
2. Select the Storage link in the sub navigation bar.
3. In the BUCKETS tab, Click the **+ ADD** button.
4. Select **Amazon S3** from the dropdown list
5. From the NEW BUCKET Wizard input the following:

   **NAME** Name of the Bucket in Morpheus.
   **ACCESS KEY** AWS IAM Access Key
   **SECRET KEY** AWS IAM Secret Key
   **BUCKET NAME** Enter existing S3 Bucket name, or to add a new Bucket enter a new name and select **Create Bucket**.
   **CREATE BUCKET** Enable if the Bucket entered in BUCKET NAME does not exist and needs to be created. If enabled, select an AWS Region to create the Bucket in.
   **ENDPOINT URL** Optional endpoint URL if pointing to an object store other than amazon that mimics the Amazon S3 APIs.
   **Default Backup Target** Sets this Bucket as the default backup target when creating Backups. If selected the option to update existing Backup configuration to use this Bucket will be presented.
**Archive Snapshots** Enabled to export VM snapshots to this Bucket when creating VMware Backups, after which the snapshot will be removed from the target hypervisor.

**Default Deployment Archive Target** Sets this bucket as the default storage target when uploading Deployment files in the Deployments section.

**Default Virtual Image Store** Sets this bucket as the default storage target when uploading Virtual Images from the Virtual Images section, importing Images from Instance Actions, creating Images with the Image Builder and when creating new images from Migrations.

**RETENTION POLICY**

None Files in the Bucket will not be automatically deleted or backed up.

**Backup Old Files**

This option will backup files after a set amount of time and remove them from the bucket.

**DAYS OLD** Files older than the set number of days will be automatically backed up to the selected Backup Bucket.

**BACKUP BUCKET** Search for and then select the Bucket the files will be backed up to.

**DELETE OLD FILES**

This option will delete files from this bucket after a set amount of days.

**DAYS OLD** Files older than the set number of days will be automatically deleted from the Bucket.

6. Select **SAVE CHANGES**

The Bucket will be created and displayed in the Buckets tab.

- To browse, upload, download, or delete files from this Bucket, select the name of the Bucket.
- To edit the Bucket, select the edit icon or select the name of the Bucket and select **ACTIONS - EDIT**.

**Warning:** Repointing a bucket that is in use may cause loss of file references. Ensure data is mirrored first.

- To delete a Bucket, select the trash icon or select the name of the Bucket and select **DELETE**.

**Warning:** When deleting a Bucket, all Deployment Versions and Backups associated with the Bucket will be deleted.

**Azure Buckets**

To Add an Azure Storage Bucket:

1. Select the Infrastructure link in the navigation bar.
2. Select the Storage link in the sub navigation bar.
3. In the BUCKETS tab, Click the **+ ADD** button.
4. Select **Azure** from the dropdown list
5. From the NEW BUCKET Wizard input the following:
   - **NAME** Name of the Bucket in Morpheus.
   - **STORAGE ACCOUNT** Name of the Storage Account in Azure for the Bucket
STORAGE KEY  Storage Key provided from Azure

SHARE NAME  Enter existing Azure Storage Share name, or to add a new Share enter a new name and select Create Bucket below.

CREATE BUCKET  Enable if the Share entered in SHARE NAME does not exist and needs to be created.

Default Backup Target  Sets this bucket as the default backup target when creating Backups. If selected the option to update existing Backup configuration to use this Bucket will be presented.

Archive Snapshots  Enabled to export VM snapshots to this Bucket when creating VMware Backups, after which the snapshot will be removed from the target hypervisor.

Default Deployment Archive Target  Sets this Bucket as the default storage target when uploading Deployment files in the Deployments section.

Default Virtual Image Store  Sets this bucket as the default storage target when uploading Virtual Images from the Virtual Images section, importing Images from Instance Actions, creating Images with the Image Builder and when creating new images from Migrations.

RETENTION POLICY

None  Files in the Bucket will not be automatically deleted or backed up.

Backup Old Files

This option will backup files after a set amount of time and remove them from the bucket.

DAYS OLD  Files older than the set number of days will be automatically backed up to the selected Backup Bucket.

BACKUP BUCKET  Search for and then select the Bucket the files will be backed up to.

DELETE OLD FILES

This option will delete files from this bucket after a set amount of days.

DAYS OLD  Files older than the set number of days will be automatically deleted from the Bucket.

6. Select SAVE CHANGES

The Bucket will be created and displayed in the Buckets tab.

- To browse, upload, download, or delete files from this Bucket, select the name of the Bucket.
- To edit the Bucket, select the edit icon or select the name of the Bucket and select ACTIONS - EDIT.

**Warning:** Repointing a bucket that is in use may cause loss of file references. Ensure data is mirrored first.

- To delete a Bucket, select the trash icon or select the name of the Bucket and select DELETE.

**Warning:** When deleting a Bucket, all Deployment Versions and Backups associated with the Bucket will be deleted.
Google Cloud Storage Buckets

**Note:** Google Cloud Storage Buckets are associated with an existing GCP Cloud integration. Ensure the GCP Cloud integration is pre-existing before attempting to create a new Google Cloud Storage Bucket. On the initial integration and subsequent cloud syncs, Google Cloud Storage Buckets are automatically onboarded and updated.

To add a Google Cloud Storage Bucket:

1. Select the Infrastructure link in the navigation bar
2. Select the Storage link in the sub-navigation bar
3. In the BUCKETS tab, Click the + ADD button
4. Select Google Cloud Storage from the dropdown list
5. From the NEW BUCKET Wizard input the following:
   - **NAME** A friendly name for the bucket in Morpheus
   - **STORAGE SERVICE** Select the GCP cloud integration this bucket should be created in
   - **PROJECT ID** Select the Project to create the group under, Projects are a GCP-specific concept and are logical grouping for your resources. Select any existing project associated with your selected GCP cloud integration
   - **BUCKET NAME** The name for the bucket resource on the GCP side
   - **LOCATION TYPE** Select Region, Dual-Region, or Multi-Region. Buckets with a Region location type will be stored in one GCP region, such as “us-east1 (South Carolina)”. Dual-Region and Multi-Region data is stored in two (or more, in the case of multi-region) GCP regions separated by a significant physical distance. Dual-Region and Multi-Region data is geo-redundant across the multiple selected regions
   - **LOCATION** A selected GCP region (or regions, in the case of dual and multi-location data) where the data will be stored
   - **STORAGE CLASS** Select Standard, Nearline, Coldline, or Archive. The appropriate storage class will depend on how frequently the bucket data is accessed and how long the type of data in the bucket is expected to be stored. More information on storage classes can be found in GCP Documentation
   - **ACTIVE** When marked, the bucket is available for use in Morpheus
   - **DEFAULT BACKUP TARGET** Sets the bucket as the default storage option when creating backups at provision time or in the Backups section of Morpheus
   - **DEFAULT DEPLOYMENT ARCHIVE TARGET** Sets this Bucket as the default storage target when uploading deployment files in the Deployments section
   - **DEFAULT VIRTUAL IMAGE STORE** Sets this bucket as the default storage target when uploading virtual images from the Virtual Images section, importing images from Instance actions, creating images with the Image Builder, and when creating new images from Migrations
   - **RETENTION POLICY** Select None and the files in this bucket will never be deleted or backed up by Morpheus. When selecting ‘Backup Old Files’, Morpheus will backup files into another selected bucket once they reach a certain number of days old. When selecting ‘Delete Old Files’, Morpheus will delete any files that reach a certain number of days old
Dell EMC ECS Buckets

**Note:** A Dell EMC ECS Storage Server must be configured in *Infrastructure - Storage - Servers* prior to adding a Dell EMC ECS Bucket.

To Add a Dell EMC ECS Storage Bucket:

1. Select the Infrastructure link in the navigation bar.
2. Select the Storage link in the sub navigation bar.
3. In the BUCKETS tab, Click the + ADD button.
4. Select *Dell EMC ECS Bucket* from the dropdown list
5. From the NEW BUCKET Wizard input the following:
   - **NAME** Name of the Bucket in Morpheus.
   - **STORAGE SERVICE** Select existing Dell EMC ECS Storage Server (configured in *Infrastructure - Storage - Servers*).
   - **BUCKET NAME** Enter a name for the new Dell EMC ECS bucket.
   - **USER** Dell EMC ECS User
   - **SECRET KEY** Dell EMC ECS Secret key
   - **NAMESPACE** Select Dell EMC ECS Namespace for the Bucket
   - **STORAGE GROUP** Select a Dell EMC ECS Storage Group
   - **Default Backup Target** Sets this bucket as the default backup target when creating Backups. If selected the option to update existing Backup configuration to use this Bucket will be presented.
   - **Archive Snapshots** Enabled to export VM snapshots to this Bucket when creating VMware Backups, after which the snapshot will be removed from the target hypervisor.
   - **Default Deployment Archive Target** Sets this Bucket as the default storage target when uploading Deployment files in the *Deployments* section.
   - **Default Virtual Image Store** Sets this bucket as the default storage target when uploading Virtual Images from the *Virtual Images* section, importing Images from Instance Actions, creating Images with the *Image Builder* and when creating new images from *Migrations*.

**RETENTION POLICY**

- **None** Files in the Bucket will not be automatically deleted or backed up.

**Backup Old Files**

This option will backup files after a set amount of time and remove them from the bucket.

- **DAYS OLD** Files older than the set number of days will be automatically backed up to the selected Backup Bucket.

**DELETE OLD FILES**

This option will delete files from this bucket after a set amount of days.

- **DAYS OLD** Files older than the set number of days will be automatically deleted from the Bucket.
6. Select *SAVE CHANGES*

The Bucket will be created and displayed in the Buckets tab.

- To browse, upload, download, or delete files from this Bucket, select the name of the Bucket.
- To edit the Bucket, select the edit icon or select the name of the Bucket and select *ACTIONS - EDIT*.

**Warning:** Repointing a bucket that is in use may cause loss of file references. Ensure data is mirrored first.

- To delete a Bucket, select the trash icon or select the name of the Bucket and select *DELETE*.

**Warning:** When deleting a Bucket, all Deployment Versions and Backups associated with the Bucket will be deleted.

---

**Openstack Swift Buckets**

To Add an Azure Storage Bucket:

1. Select the Infrastructure link in the navigation bar.
2. Select the Storage link in the sub navigation bar.
3. In the BUCKETS tab, Click the + ADD button.
4. Select *Openstack Swift* from the dropdown list.
5. From the NEW BUCKET Wizard input the following:
   - **NAME** Name of the Bucket in Morpheus.
   - **USERNAME** Openstack Swift Username
   - **API KEY** Openstack Swift API Key
   - **BUCKET NAME** Enter existing Openstack Swift Bucket name, or to add a new Bucket enter a new name and select *Create Bucket* below.
   - **IDENTITY URL** Openstack Swift Identity URL
   - **Create Bucket** Enable if the name entered in BUCKET NAME does not exist and needs to be created.
   - **Default Backup Target** Sets this bucket as the default backup target when creating Backups. If selected the option to update existing Backup configuration to use this Bucket will be presented.
   - **Archive Snapshots** Enabled to export VM snapshots to this Bucket when creating VMware Backups, after which the snapshot will be removed from the target hypervisor.
   - **Default Deployment Archive Target** Sets this Bucket as the default storage target when uploading Deployment files in the *Deployments* section.
   - **Default Virtual Image Store** Sets this bucket as the default storage target when uploading Virtual Images from the *Virtual Images* section, importing Images from Instance Actions, creating Images with the *Image Builder* and when creating new images from *Migrations*.

**RETENTION POLICY**

- **None** Files in the Bucket will not be automatically deleted or backed up.
- **Backup Old Files**

  *This option will backup files after a set amount of time and remove them from the bucket.*
Morpheus Documentation

**DAYS OLD** Files older than the set number of days will be automatically backed up to the selected Backup Bucket.

**BACKUP BUCKET** Search for and then select the Bucket the files will be backed up to.

**DELETE OLD FILES**

This option will delete files from this bucket after a set amount of days.

**DAYS OLD** Files older than the set number of days will be automatically deleted from the Bucket.

6. Select **SAVE CHANGES**

The Bucket will be created and displayed in the Buckets tab.

- To browse, upload, download, or delete files from this Bucket, select the name of the Bucket.
- To edit the Bucket, select the edit icon or select the name of the Bucket and select **ACTIONS - EDIT**.

**Warning:** Repointing a bucket that is in use may cause loss of file references. Ensure data is mirrored first.

- To delete a Bucket, select the trash icon or select the name of the Bucket and select **DELETE**.

**Warning:** When deleting a Bucket, all Deployment Versions and Backups associated with the Bucket will be deleted.

**Rackspace CDN Buckets**

To Add a Rackspace CDN Bucket:

1. Select the Infrastructure link in the navigation bar.
2. Select the Storage link in the sub navigation bar.
3. In the BUCKETS tab, Click the **+ ADD** button.
4. Select **Rackspace CDN** from the dropdown list.
5. From the NEW BUCKET Wizard input the following:
   - **NAME** Name of the Bucket in Morpheus.
   - **USERNAME** Rackspace CDN Username
   - **API KEY** Rackspace CDN API Key
   - **REGION** Enter Rackspace CDN Region
   - **BUCKET NAME** Enter existing Rackspace CDN Bucket name, or to add a new Bucket enter a new name and select **Create Bucket** below.
   - **Create Bucket** Enable if the name entered in BUCKET NAME does not exist and needs to be created.
   - **Default Backup Target** Sets this bucket as the default backup target when creating Backups. If selected the option to update existing Backup configuration to use this Bucket will be presented.
   - **Archive Snapshots** Enabled to export VM snapshots to this Bucket when creating VMware Backups, after which the snapshot will be removed from the target hypervisor.
   - **Default Deployment Archive Target** Sets this Bucket as the default storage target when uploading Deployment files in the Deployments section.
Default Virtual Image Store  Sets this bucket as the default storage target when uploading Virtual Images from the Virtual Images section, importing Images from Instance Actions, creating Images with the Image Builder and when creating new images from Migrations.

RETENTION POLICY

None  Files in the Bucket will not be automatically deleted or backed up.

Backup Old Files

This option will backup files after a set amount of time and remove them from the bucket.

DAYS OLD  Files older than the set number of days will be automatically backed up to the selected Backup Bucket.

BACKUP BUCKET  Search for and then select the Bucket the files will be backed up to.

DELETE OLD FILES

This option will delete files from this bucket after a set amount of days.

DAYS OLD  Files older than the set number of days will be automatically deleted from the Bucket.

6. Select SAVE CHANGES

The Bucket will be created and displayed in the Buckets tab.

- To browse, upload, download, or delete files from this Bucket, select the name of the Bucket.
- To edit the Bucket, select the edit icon or select the name of the Bucket and select ACTIONS - EDIT.

**Warning:** Repointing a bucket that is in use may cause loss of file references. Ensure data is mirrored first.

- To delete a Bucket, select the trash icon or select the name of the Bucket and select DELETE.

**Warning:** When deleting a Bucket, all Deployment Versions and Backups associated with the Bucket will be deleted.

5.7.3 File Shares

File Shares are for Backup, Archives, Deployment and Virtual Images storage targets. File Shares can be browsed and files and folders can be uploaded, downloaded or deleted from the File Shares section. Retention Policies can be set on Storage File Shares for files to be deleted or backed up to another File Share after a set amount of time.

**Supported File Share Types**

- CIFS (Samba Windows File Sharing)
- Dell EMC ECS Share
- Dell EMC Isilon Share
- Local Storage
- NFSv3
CIFS File Shares

To Add a CIFS File Share:

1. Select the Infrastructure link in the navigation bar.
2. Select the Storage link in the sub navigation bar.
3. In the FILE SHARES tab, Click the + ADD button.
4. Select CIFS (Samba Windows File Sharing) from the dropdown list
5. From the NEW FILE SHARE Wizard input the following:
   - **NAME**  Name of the File Share in Morpheus.
   - **HOST**  Enter host IP or resolvable hostname Example: 192.168.200.210
   - **USERNAME**  CIFS Share Username
   - **PASSWORD**  CIFS Share User Password
   - **SHARE PATH**  Enter CIFS Share Path Example: cifs
   - **Default Backup Target**  Sets this File Share as the default backup target when creating Backups. If selected the option to update existing Backup configuration to use this File Share will be presented.
   - **Archive Snapshots**  Enabled to export VM snapshots to this File Share when creating VMware Backups, after which the snapshot will be removed from the source Cloud.
   - **Default Deployment Archive Target**  Sets this File Share as the default storage target when uploading Deployment files in the Deployments section.
   - **Default Virtual Image Store**  Sets this File Share as the default storage target when uploading Virtual Images from the Virtual Images section, importing Images from Instance Actions, creating Images with the Image Builder and when creating new images from Migrations.
   - **RETENTION POLICY**  None Files in the File Share will not be automatically deleted or backed up.
   - **Backup Old Files**  This option will backup files after a set amount of time and remove them from the File Share.
     - **DAYS OLD**  Files older than the set number of days will be automatically backed up to the selected Backup File Share.
     - **BACKUP File Share**  Search for and select the File Share the files will be backed up to.
   - **DELETE OLD FILES**  This option will delete files from this File Share after a set amount of days.
     - **DAYS OLD**  Files older than the set number of days will be automatically deleted from the File Share.
6. Select SAVE CHANGES

The File Share will be created and displayed in the File Shares tab.

- To browse, upload, download, or delete files from this File Share, select the name of the File Share.
• To edit the File Share, select the edit icon or select the name of the File Share and select ACTIONS - EDIT.

**Warning:** Repointing a File Share that is in use may cause loss of file references. Ensure data is mirrored first.

• To delete a File Share, select the trash icon or select the name of the File Share and select DELETE.

**Warning:** When deleting a File Share, all Deployment Versions and Backups associated with the File Share will be deleted.

**Dell EMC ECS File Shares**

To Add a Dell EMC ECS File Share:

1. Select the Infrastructure link in the navigation bar.
2. Select the Storage link in the sub navigation bar.
3. In the FILE SHARES tab, Click the **ADD** button.
4. Select **Dell EMC ECS Share** from the dropdown list
5. From the NEW FILE SHARE Wizard input the following:
   - **NAME** Name of the File Share in Morpheus.
   - **STORAGE SERVICE** Select existing Dell EMC ECS Storage Server (configured in **Infrastructure - Storage - Servers**)
   - **SHARE PATH** Enter Dell EMC ECS Share Path Example: *ecs-file-share-1*
   - **USER** Dell EMC ECS User
   - **SECRET KEY** Dell EMC ECS Secret key
   - **Volume Size** Specify volume size for the File Share (in MB)
   - **Allowed IP’s** Specify IP Addresses to limit accessibility to the File Share
     - **Leave blank for open access** Click the + symbol to the right of the first ALLOWED IPS field to add multiple IP’s
   - **NAMESPACE** Select Dell EMC ECS Namespace (synced)
   - **STORAGE GROUP** Select Dell EMC ECS Storage Group (synced)
   - **Default Backup Target** Sets this File Share as the default backup target when creating Backups. If selected the option to update existing Backup configuration to use this File Share will be presented.
   - **Archive Snapshots** Enabled to export VM snapshots to this File Share when creating VMware Backups, after which the snapshot will be removed from the source Cloud.
   - **Default Deployment Archive Target** Sets this File Share as the default storage target when uploading Deployment files in the *Deployments* section.
**Default Virtual Image Store** Sets this File Share as the default storage target when uploading Virtual Images from the Virtual Images section, importing Images from Instance Actions, creating Images with the Image Builder and when creating new images from Migrations.

**RETENTION POLICY**

- **None** Files in the File Share will not be automatically deleted or backed up.

**Backup Old Files**

This option will backup files after a set amount if time and remove them from the File Share.

- **DAYS OLD** Files older than the set number of days will be automatically backed up to the selected Backup File Share.

**DELETE OLD FILES**

This option will delete files from this File Share after a set amount of days.

- **DAYS OLD** Files older than the set number of days will be automatically deleted from the File Share.

6. Select **SAVE CHANGES**

The File Share will be created and displayed in the File Shares tab.

- To browse, upload, download, or delete files from this File Share, select the name of the File Share.

- To edit the File Share, select the edit icon or select the name of the File Share and select **ACTIONS - EDIT**.

**Warning:** Repointing a File Share that is in use may cause loss of file references. Ensure data is mirrored first.

- To delete a File Share, select the trash icon or select the name of the File Share and select **DELETE**.

**Warning:** When deleting a File Share, all Deployment Versions and Backups associated with the File Share will be deleted.

---

**Dell EMC Isilon File Shares**

To Add a Dell EMC Isilon File Share:

1. Select the Infrastructure link in the navigation bar.
2. Select the Storage link in the sub navigation bar.
3. In the FILE SHARES tab, Click the **+ ADD** button.
4. Select **Dell EMC Isilon Share** from the dropdown list
5. From the NEW FILE SHARE Wizard input the following:
   - **NAME** Name of the File Share in Morpheus.
   - **STORAGE SERVICE** Select existing Dell EMC Isilon Storage Server (configured in **Infrastructure - Storage - Servers**)
   - **SHARE PATH**
Enter Dell EMC Isilon Share Path  Example: ecs-file-share-1

Volume Size  Specify volume size for the File Share (in MB)

Allowed IP’s

Specify IP Addresses to limit accessibility to the File Share

Leave blank for open access  Click the + symbol to the right of the first ALLOWED IPS field to add multiple IP’s

NAMESPACE  Select Dell EMC Isilon Namespace (synced)

STORAGE GROUP  Select Dell EMC Isilon Storage Group (synced)

Default Backup Target  Sets this File Share as the default backup target when creating Backups. If selected the option to update existing Backup configuration to use this File Share will be presented.

Archive Snapshots  Enabled to export VM snapshots to this File Share when creating VMware Backups, after which the snapshot will be removed from the source Cloud.

Default Deployment Archive Target  Sets this File Share as the default storage target when uploading Deployment files in the Deployments section.

Default Virtual Image Store  Sets this File Share as the default storage target when uploading Virtual Images from the Virtual Images section, importing Images from Instance Actions, creating Images with the Image Builder and when creating new images from Migrations.

RETENTION POLICY

None  Files in the File Share will not be automatically deleted or backed up.

Backup Old Files

This option will backup files after a set amount if time and remove them from the File Share.

DAYS OLD  Files older than the set number of days will be automatically backed up to the selected Backup File Share.

BACKUP File Share  Search for and select the File Share the files will be backed up to.

DELETE OLD FILES

This option will delete files from this File Share after a set amount of days.

DAYS OLD  Files older than the set number of days will be automatically deleted from the File Share.

6. Select SAVE CHANGES

The File Share will be created and displayed in the File Shares tab.

• To browse, upload, download, or delete files from this File Share, select the name of the File Share.

• To edit the File Share, select the edit icon or select the name of the File Share and select ACTIONS - EDIT.

Warning:  Repointing a File Share that is in use may cause loss of file references. Ensure data is mirrored first.

• To delete a File Share, select the trash icon or select the name of the File Share and select DELETE.
Warning: When deleting a File Share, all Deployment Versions and Backups associated with the File Share will be deleted.

Local Storage File Shares

Important: Local Storage refers to local to the Morpheus Appliance and the path must be owned by `morpheus-app`. Please be conscious of storage space. High Availability configurations require Local Storage File Shares paths to be shared storage paths between the front end Morpheus Appliances.

Note: To change the owner of a file path to be used as a Local Storage File Share, run `chown morpheus-app.morpheus-app /path` on the Morpheus Appliance.

Note: Morpheus will validate path and ownership of the File Share Path.

To Add a Local Storage File Share:

1. Select the Infrastructure link in the navigation bar.
2. Select the Storage link in the sub navigation bar.
3. In the FILE SHARES tab, Click the + ADD button.
4. Select Local Storage Share from the dropdown list
5. From the NEW FILE SHARE Wizard input the following:
   - **NAME**: Name of the File Share in Morpheus.
   - **STORAGE PATH**: Enter the File Share path on the local Morpheus Appliance. Example: `/var/opt/morpheus/morpheus-ui/vms/virtual-images`

   Important: High Availability configurations require Local Storage File Shares paths to be shared storage paths between the front end Morpheus Appliances.

Default Backup Target Sets this File Share as the default backup target when creating Backups. If selected the option to update existing Backup configuration to use this File Share will be presented.

Archive Snapshots Enabled to export VM snapshots to this File Share when creating VMware Backups, after which the snapshot will be removed from the source Cloud.

Default Deployment Archive Target Sets this File Share as the default storage target when uploading Deployment files in the Deployments section.

Default Virtual Image Store Sets this File Share as the default storage target when uploading Virtual Images from the Virtual Images section, importing Images from Instance Actions, creating Images with the Image Builder and when creating new images from Migrations.

RETENTION POLICY

None Files in the File Share will not be automatically deleted or backed up.
Morpheus Documentation

Backup Old Files
This option will backup files after a set amount of time and remove them from the File Share.

**DAYS OLD**  Files older than the set number of days will be automatically backed up to the selected Backup File Share.

**DELETE OLD FILES**  This option will delete files from this File Share after a set amount of days.

**DAYS OLD**  Files older than the set number of days will be automatically deleted from the File Share.

6. Select **SAVE CHANGES**

The File Share will be created and displayed in the File Shares tab.

- To browse, upload, download, or delete files from this File Share, select the name of the File Share.
- To edit the File Share, select the edit icon or select the name of the File Share and select **ACTIONS - EDIT**.

**Warning:** Repointing a File Share that is in use may cause loss of file references. Ensure data is mirrored first.

- To delete a File Share, select the trash icon or select the name of the File Share and select **DELETE**.

**Warning:** When deleting a File Share, all Deployment Versions and Backups associated with the File Share will be deleted.

NFSv3 File Shares

**Note:**  Configure access to the NFS folder on the NFS Provider prior to adding the NFSv3 File Share.

**Note:**  Upon save Morpheus will create a persistent mount owned by `morpheus-app.morpheus-app` on the Morpheus Appliance for the NFSv3 File Share. The Morpheus appliance will require access to the following ports in order to mount the share: 111, 54302, 20048, 2049, 46666, 42955, 875. With some storage solutions, you may need to enable insecure, unprivileged ports, or allow non-root on the export before Morpheus is able to successfully mount the share.

To Add a NFSv3 File Share:

1. Select the Infrastructure link in the navigation bar.
2. Select the Storage link in the sub navigation bar.
3. In the FILE SHARES tab, Click the + **ADD** button.
4. Select **NFSv3** from the dropdown list
5. From the NEW FILE SHARE Wizard input the following:
   - **NAME**  Name of the File Share in Morpheus.
HOST Enter the File Share path on the local Morpheus Appliance.

EXPORT FOLDER Enter the NFSv3 Folder

Default Backup Target Sets this File Share as the default backup target when creating Backups. If selected the option to update existing Backup configuration to use this File Share will be presented.

Archive Snapshots Enabled to export VM snapshots to this File Share when creating VMware Backups, after which the snapshot will be removed from the source Cloud.

Default Deployment Archive Target Sets this File Share as the default storage target when uploading Deployment files in the Deployments section.

Default Virtual Image Store Sets this File Share as the default storage target when uploading Virtual Images from the Virtual Images section, importing Images from Instance Actions, creating Images with the Image Builder and when creating new images from Migrations.

RETENTION POLICY

None Files in the File Share will not be automatically deleted or backed up.

Backup Old Files

This option will backup files after a set amount of time and remove them from the File Share.

DAYS OLD Files older than the set number of days will be automatically backed up to the selected Backup File Share.

BACKUP File Share Search for and select the File Share the files will be backed up to.

DELETE OLD FILES

This option will delete files from this File Share after a set amount of days.

DAYS OLD Files older than the set number of days will be automatically deleted from the File Share.

6. Select SAVE CHANGES

The File Share will be created and displayed in the File Shares tab.

- To browse, upload, download, or delete files from this File Share, select the name of the File Share.
- To edit the File Share, select the edit icon or select the name of the File Share and select ACTIONS - EDIT.

**Warning:** Repointing a File Share that is in use may cause loss of file references. Ensure data is mirrored first.

- To delete a File Share, select the trash icon or select the name of the File Share and select DELETE.

**Warning:** When deleting a File Share, all Deployment Versions and Backups associated with the File Share will be deleted.
5.7.4 Volumes

Volumes sync or created in Morpheus can be viewed in *Infrastructure- Storage - Volumes*. Volumes can be added for Storage Servers integrated with Morpheus in the *Infrastructure- Storage - Servers* section.

Volumes Types

The available Volume Types list and filterable by are:

- 3Par Volume
- Alibaba Cloud SSD
- Alibaba Efficiency Disk
- Alibaba Cloud Disk
- AWS gp2
- AWS io1
- AWS sc1
- AWS st1
- Azure Volume
- Azure Disk
- Bluemix Disk
- Bluemix SAN
- Bluemix SAN
- CD ROM
- DO Disk
- ECS Block Storage
- ECS Object Storage
- ECS Shared File System
- Floppy Disk
- Google Standard
- HP Enclosure Disk
- Oracle iSCSI
- Isilon NFS Volume
- Nutanix IDE
- Nutanix SATA
- Nutanix SCSI
- Open Telekom Volume
- Openstack Disk
- Openstack Volume
- Oracle Block Volume
• Oracle Disk
• Oracle Virtual Volume
• SCVMM Datastore
• Softlayer Disk
• Softlayer SAN
• Softlayer SAN
• Disk
• UpCloud Disk
• UpCloud MaxIOPS
• NULL
• NULL
• VMWare Datastore
• VMWare Disk

CREATE VOLUME

At least one Storage Server Integration from *Infrastructure- Storage - Servers* is required to create volumes from *Infrastructure- Storage - Volumes*.

3par

To Add a 3Par Volume:
1. Select the Infrastructure link in the navigation bar.
2. Select the Storage link in the sub navigation bar.
3. In the Volumes tab, Click the + ADD button.
4. Select 3Par from the dropdown list
5. From the CREATE VOLUME Wizard input the following:

**SELECT TYPE**

- **STORAGE SERVER**  Name of the 3par Storage Server added in *Infrastructure- Storage - Servers*
- **GROUP**  Select Storage Group
- **VOLUME TYPE**  3Par Volume
- Click NEXT  Select NEXT

**CONFIGURE**

- **NAME**  Name of the Volume
- **VOLUME SIZE**  Specify size of the Volume (in MB)

**PROVISION TYPE**

- **FULL**
- **TPVV**
• SNP
• PEER
• UNKNOWN
• TDVV

Click COMPLETE Select COMPLETE

Dell EMC ECS

To Add a Dell EMC ECS Volume:
1. Select the Infrastructure link in the navigation bar.
2. Select the Storage link in the sub navigation bar.
3. In the VolumeS tab, Click the + ADD button.
4. Select Dell EMC ECS from the dropdown list
5. From the CREATE VOLUME Wizard input the following:

SELECT TYPE

STORAGE SERVER Name of the DELL EMC ECS Storage Server added in Infrastructure- Storage - Servers
GROUP Select Storage Group
VOLUME TYPE ECS Block Storage ECS Object Storage ECS Shared File System

Click NEXT Select NEXT

CONFIGURE

NAME Name of the Volume

Click COMPLETE Select COMPLETE

Dell EMC Isilon

To Add a Dell EMC ECS Volume:
1. Select the Infrastructure link in the navigation bar.
2. Select the Storage link in the sub navigation bar.
3. In the VolumeS tab, Click the + ADD button.
4. Select Dell EMC Isilon from the dropdown list
5. From the CREATE VOLUME Wizard input the following:

SELECT TYPE

STORAGE SERVER Name of the Dell EMC Isilon Storage Server added in Infrastructure- Storage - Servers
GROUP Select Storage Group
VOLUME TYPE Isilon NFS Volume

Click NEXT Select NEXT
**CONFIGURE**

- **NAME** Name of the Volume
- **ALLOWED IP’s**
  - Specify IP Addresses to limit accessibility to the File Share
  - Leave blank for open access
  - Click the + symbol to the right of the first ALLOWED IPS field to add multiple IP’s
- **VOLUME SIZE** Specify size of the Volume (in MB)
- **Click COMPLETE** Select COMPLETE

### 5.7.5 Data Stores

Data Stores are logical divisions of underlying storage disk. Organizations may use them to divide and track cloud resources by team or department. When integrating certain Cloud types, Morpheus will onboard all existing data stores and administrators can then make them available to Groups or Tenants as needed. At provision time, when applicable based on Cloud and Layout, users can select the data store they wish to provision to.

Here within the Data Store view in the storage section, users can see a list of data stores for each Cloud. In the row for each Cloud, the storage type, associated Cloud, and permissions information are shown.

#### Create Data Stores

To a limited extent, data stores can be created from this view. Currently, data store creation is restricted to VMware data store creation on 3Par volumes. In order to create such a data store you would need to first have an integrated 3Par server. See the section on storage servers for more information on setting up this integration.

**Note:** For all other data store types, create the needed data store within the target Cloud and Morpheus will automatically sync in the data store on the next Cloud sync. You can force a Cloud sync from the Cloud Detail Page (Infrastructure > Clouds > Selected Cloud > Refresh Menu > Short).

- Navigate to Infrastructure > Storage > Data Stores
- Click +ADD
- Enter a Name, select a VMware Cloud, select a 3Par Volume, and select a Host Group
- Manage permissions in the Group Access and Tenant Permissions sections, if needed
- Click SAVE CHANGES

#### Manage Permissions

From this view, users can manage permissions for any data store synced from integrated Clouds. This includes setting which Groups have access to the data store, and which Tenants have access. To edit data store permissions:

- Navigate to Infrastructure > Storage > Data Stores
- Click ACTIONS > Edit
- **Groups:** Select “all” Groups or select specific Groups which should have access to the data store
• **Tenants:** Primary Tenant users can opt to make the data store available to all Tenants (public visibility) or to selected Tenants (private visibility with specific Tenants selected). Subtenant users will only be able to make data stores visible to their own Tenant.

• **Active:** When marked, the data store is active and available for provisioning.

• Click *SAVE CHANGES*

### 5.7.6 Servers

**Add Storage Server**

**Adding 3Par Storage Server**

1. Select the Infrastructure link in the navigation bar.
2. Select the Storage link in the sub navigation bar.
3. In the SERVERS tab, Click the + ADD button.
4. From the ADD STORAGE SERVER wizard input the following:
   - **NAME** Name of the Storage Server in Morpheus
   - **TYPE** Select 3Par
   - **URL** URL Of 3Par Server Example: `https://192.168.190.201:8008`
   - **USERNAME** Add your administrative user account.
   - **PASSWORD** Add your administrative password.
5. Select *SAVE CHANGES*

The 3Par Storage Server will be added and displayed in the Buckets tab. Buckets, Files Shares and Storage Groups will be synced in.

**Adding Dell EMC ECS Storage Server**

1. Select the Infrastructure link in the navigation bar.
2. Select the Storage link in the sub navigation bar.
3. In the SERVERS tab, Click the + ADD button.
4. From the ADD STORAGE SERVER wizard input the following:
   - **NAME** Name of the Storage Server in Morpheus
   - **TYPE** Select *Dell EMC ECS*
   - **URL**
     - **URL OF DELL EMC ECS Server** Example: `https://192.168.190.200:4443`
     - **Tip:** The port 4443 is the api port for ECS api. This may be different depending on your configuration
   - **USERNAME** Add your administrative user account.
   - **PASSWORD** Add your administrative password.
S3 SERVICE URL (Optional) Add your S3 service url Example: http://192.168.190.220:9020

Note: S3 SERVICE URL is not required if you are not planning on using ECS S3.

5. Select SAVE CHANGES
The Dell EMC ECS Storage Server will be added and displayed in the Buckets tab. Buckets, Files Shares and Storage Groups will be synced in.

Adding Dell EMC Isilon Storage Server

1. Select the Infrastructure link in the navigation bar.
2. Select the Storage link in the sub navigation bar.
3. In the SERVERS tab, Click the + ADD button.
4. From the ADD STORAGE SERVER wizard input the following:
   NAME Name of the Storage Server in Morpheus
   TYPE Select Dell EMC Isilon
   URL URL Of Dell EMC Isilon Server Example : https://192.168.190.202:8080
   USERNAME Add your administrative user account.
   PASSWORD Add your administrative password.
   PROVISION USER Select Provision User
   PROVISION GROUP Select Provision Group
   ROOT PATH Enter Root Path Example : \

5. Select SAVE CHANGES
The Dell EMC Isilon Storage Server will be added and displayed in the Buckets tab. Buckets, Files Shares and Storage Groups will be synced in.

5.8 Key Pairs & Certificates

5.8.1 Key Pairs
The key pairs section enables the following actions: Add and Delete key pairs. Key pairs are commonly used by Morpheus for accessing instances via SSH. Morpheus stores key pairs to simplify administration and access across both private and public clouds.

Morpheus only accepts key pairs in PEM format (for example, a private key beginning with -----BEGIN RSA PRIVATE KEY------). If you have a key in another format, such as OpenSSH, convert the key:

```bash
#No passphrase
ssh-keygen -m pem -f /path/to/key

#With passphrase
ssh-keygen -p -P "old passphrase" -N "new passphrase" -m pem -f path/to/key
```
5.8.2 Add Key Pair

To Add Key Pair:

1. Navigate to Infrastructure > Keys & Certs
2. On the Key Pairs tab, click + ADD
3. From the Add Key Pair wizard input the following as needed:
   - Name
   - Public Key
   - Private Key
   - Passphrase

Note: Certain features do not require storage of the private key.

5.8.3 Delete Key Pair

To Delete Key Pair:

1. Navigate to Infrastructure > Keys & Certs
2. On the Key Pairs tab, select the trash can icon at the end of any row
3. Acknowledge that you wish to delete the selected key pair

5.8.4 SSL Certificates

SSL certificates authenticate the identity of web servers and encrypt the data being transmitted. Morpheus stores SSL certificates to simplify administration and application of SSL certificates to Morpheus-managed resources.

5.8.5 Add SSL Certificate

1. Navigate to Infrastructure > Keys & Certs
2. On the SSL Certificates tab, click + ADD
3. From the Add SSL Certificate wizard input the following as needed:
   - Name
   - Domain Name
   - Key File
   - Cert File
   - Root Cert
5.8.6 Delete SSL Certificate

To Delete SSL Certificate:

1. Navigate to Infrastructure > Keys & Certs
2. On the SSL Certificates tab, select the trash can icon at the end of any row
3. Acknowledge that you wish to delete the selected SSL Certificate

5.8.7 Trust Integrations

Some organizations may use outside technologies to manage their key and certificates. Morpheus allows users to integrate with Venafi for trust management. Trust management integrations can be managed from the Integrations tab on the Infrastructure > Keys & Certs page. Additionally, they can be managed in Administration > Integrations.

Currently, Morpheus supports trust integration Venafi. For more detailed information on integrating Venafi with Morpheus, take a look at our integration guide.

5.9 Boot

5.9.1 Overview

Morpheus includes a built in PXE Server to enable easy and rapid bare metal provisioning.

5.9.2 Prerequisites

- DHCP server with following config added to dhcpd.conf

```plaintext
allow booting;
allow bootp;
option option-128 code 128 = string;
option option-129 code 129 = text;
next-server morpheus-appliance-ip;
filename "pxelinux.0";
```

**Note:** Replace `morpheus-appliance-ip` in the dhcpd.conf file with your Morpheus appliance IP address.

- Internal Appliance URL (PXE) set in Administration - Settings. For PXE-Boot your appliance needs to be routable directly with minimal NAT masquerading. This allows one to override the default appliance url endpoint for use by the PXE Server. If this is unset, the default appliance url will be used instead.

- Mac or IP addresses of PXE target mapped in {morpheus} Infrastructure > Boot - Mapping

- Target host configured for Network boot in BIOS

**Note:** On the Morpheus Appliance, PXE is enabled by default and port 69 is forwarded to the Internal PXE port 6969. These settings are configurable in the pxe: section of `/opt/morpheus/conf/application.yml`. 

428 Chapter 5. Infrastructure
5.9.3 Mapping

Add Mapping

1. Select the Mapping tab then click the Add Mapping button.
2. From the New Mapping Wizard input the following information:
   - **Match Pattern**: Mac address separated by ‘:’ or an ip address filter
   - **Description (optional)**: Description of the new mapping.
   - **Active**: Flag to denote the mapping as active or disabled.
   - **Operating System**: List of operating systems for the mapping.
   - **Boot Image**: Lists available PXE boot images.
   - **Answer File**: Lists available answer files.
   - **Cloud**: Lists the available clouds.
   - **Server Mode**: List of server modes: unmanaged, Managed, Bare metal host, Container host, VM host, and Container & VM host.
3. Save

Once the mapping is added, and the target host is powered on, the {morpheus} PXE menu will load and PXE boot will start.

Edit Mapping

1. Click the edit icon on the row of the mapping you wish to edit.
2. Modify information as needed.
3. Click the Save Changes button to save.

Delete Mapping

1. Click the delete icon on the row of the mapping you wish to delete.

5.9.4 Boot Menus

System-seeded Boot Menus are displayed and user-created Boot Menus can be edited and deleted. User-created Boot Menus are edited or deleted by clicking on the pencil or trash can icon in the appropriate row.

Adding a Boot Menu

To begin, click + ADD. Available fields include:

- **NAME**: Name of the Boot Menu
- **DESCRIPTION**: Description of the Boot Menu
- **TYPE**: Select between bios, uefi, ipxe and grub
- **ENABLED**: Determines if the Boot Menu is active
- **DEFAULT MENU
- **ROOT MENU
• MENU NAME
• BOOT IMAGE
• ANSWER FILE
• MENU CONTENT
• SUB MENUS

Click SAVE CHANGES

5.9.5 Answer Files

Answer files are like lists of answers for questions that you know the setup program is going to ask but the user is not prepared to answer. They contain one or more sections, and each section contains one or more properties in the form name=value. Morpheus provides Answer Files for ESXi, CentOS, Ubuntu and XenServer, and user can add their own.

Add Answer Files

1. Click the Infrastructure link in the navigation bar.
2. Click the Boot link in the sub navigation bar
3. Select the Answer Files tab then click the Add Answer File button.
4. From the New Answer File Wizard input the following information
   - Name  Name of the answer file.
   - Description(optional)  Description of the new answer file.
   - Active  Flag to denote the mapping as active or disabled.
   - Script Name  Name of the new answer file.
   - Script  The script for the new answer file.
5. Save

Edit Answer File

1. Click the Infrastructure link in the navigation bar.
2. Click the Boot link in the sub navigation bar
3. Select the Answer Files tab
4. Click the edit icon on the row of the answer file you wish to edit.
5. Modify information as needed.
6. Save Changes
Delete Answer File

1. Click the Infrastructure link in the navigation bar.
2. Click the Boot link in the sub navigation bar
3. Select the Answer Files tab.
4. Click the delete icon on the row of the answer file you wish to delete.

5.9.6 Images

Morpheus provides Images for ESXi, CentOS, Ubuntu and XenServer, and user can add their own Images.

Add Images

1. Click the Infrastructure link in the navigation bar.
2. Click the Boot link in the sub navigation bar
3. Select the Images tab then click the Add Image button.
4. From the Upload Virtual Image Wizard input the following information
   - **Name**: Name of the Image.
   - **Operating System**: List of available operating systems.
   - **Storage Provider**: List of available storage providers.
   - **Image Path**: Path of the image.
   - **Visibility**: Private or Public
   - **Account**: List of accounts to allow permission to this image.
5. Save Changes

Edit Image

1. Click the Infrastructure link in the navigation bar.
2. Click the Boot link in the sub navigation bar
3. Select the Images tab
4. Click the actions drop down and select edit.
5. Modify information as needed.
6. Click the Save Changes button to save.
Convert Image

1. Click the Infrastructure link in the navigation bar.
2. Click the Boot link in the sub navigation bar.
3. Select the Images tab
4. Click the Actions drop and select Convert.

Download Image

1. Click the Infrastructure link in the navigation bar.
2. Click the Boot link in the sub navigation bar.
3. Select the Images tab
4. Click the Actions drop and select Download.

Remove Image

1. Click the Infrastructure link in the navigation bar.
2. Click the Boot link in the sub navigation bar.
3. Select the Image tab.
4. Click the Actions drop and select Remove.
Morpheus built-in Backup solution provides VM, Container, Host, Database, File, Directory, Volume and Storage Provider Backup, Snapshot and Replication capabilities. Backups can be automatically configured during provisioning or manually created at any time. Backup Jobs with custom Execution Schedules and retention counts can be created and used across all environments in conjunction with configured Storage Providers. Backups can be restored over current Instances or as new Instances, and downloaded or deleted from Morpheus.

Morpheus also integrates with external services to automate availability with other providers.

### 6.1 Initial Backups Setup

Global Backup settings, Storage Providers and Execution Schedules should be configured prior to creating backups.

#### 6.1.1 Global Backups Settings

Morpheus Backups can be enabled under Administration > Settings > Backups.

- **Scheduled Backups** When enabled, configured Backups will automatically run on the set Schedule. If disabled, backups need to be manually run.
- **Create Backups** When enabled, Morpheus will automatically configure backup jobs for Instances.
- **Backup Appliance** When enabled, a Backup will be created to backup the Morpheus appliance database. Select the Backup text link to edit Appliance Backup Settings and view existing Appliance Backups.
- **Default Backup Storage Provider** Storage Providers can be configured and managed in the Infrastructure > Storage section.
- **Default Backup Schedule** Schedules can be configured and managed in the Library > Automation > Power Scheduling.
- **Backup Retention Count** Default maximum number of successful backups to retain.
6.1.2 Backup Schedules

Backup Execution Schedules can be configured and managed in Library > Automation > Execute Scheduling. An execution schedule stores only the interval at which some execution should be run. To create a new backup job with this schedule, navigate to Backups > Backups and click “+ADD”. In the final step of creating the backup job we are able to select any of our created execution schedules. The Default Backup Schedule set in Administration > Settings > Backups will be selected when creating a backup job and not specifying an execution schedule.

6.2 Configuring Backups during Provisioning

When Backups are enabled, Backup options are presenting in the Automation tab of the Provisioning wizard.

**Note:** The Backup options presented in the Automation tab can be disabled using a “Create Backup” policy. See Policies

**BACKUP TYPE** Select the type for the Backup. Backup Types displayed will be filtered by available options per selected Instance Layout.

**BACKUP NAME** Defaults to Instance name

**BACKUP TARGET** Select Storage Provider target for the Backup (when applicable).

**BACKUP JOB TYPE** Create New, Clone, or Add to existing Job

**JOB Name** Defaults to Instance name

**RETENTION COUNT** Maximum number of successful backups to retain.

**BACKUP SCHEDULE** Select the schedule the Backup Job will be executed.

Backup Types displayed will be filtered by available options per selected Instance Layout. Backup Job Types include:

- File Backup
- Directory Backup
- MySQL
- MongoDB
- LVM Snapshot
- LVM Image
- LVM Migration
- Windows Migration
- Postgres
- Tar Directory Backup
- Amazon VM Snapshot
- VMWare VM Snapshot
- Fusion VM Snapshot
- Xen VM Snapshot
- SqlServer
- Veeam VMWare VM Backup
6.3 Summary

The Backups Summary section shows the following metrics:

- Number of Configured Backups trend
- Backup Success Rate
- Number of Completed Backups
- Number of Failed Backups
- Total Size of Backups (MB) trend
- Upcoming and In Progress Backups

If a User’s Role permission for Backups is set to User, the user will only see metrics for backups they own.
6.4 Backups

In the Backups > Backups section, currently configured Backups can be viewed and managed, and new Instance, Host and Provider backups be configured.

Note: Role permissions for Backups determine which backups will be accessible per user.

6.4.1 Manage an existing Backup

1. Select the Backups link in the navigation bar.
2. Select the Backups link in the sub navigation bar.
3. Select the name of the Backup to view the Backups detail page.

6.4.2 Create Instance Backup

To create instance backup

1. Select the Backups link in the navigation bar.
2. Select the Backups link in the sub navigation bar.
3. Click the Add Backup button.
4. From the Create Backup Wizard select the radio button Instance, then click Next.
5. Input the following:
   - Name Name of the backup job being created.
   - Instance Select an instance to backup from the dropdown.
6. Click Next.
7. Depending on the instance type selected in the previous step, enter additional details such as:
   - Database Name
   - Username
   - Password
   - Container
   - etc..
8. Click the Next button.
10. Click Complete to save.

Note: On VMware Cloud types, Morpheus will merge and consolidate the snapshots held against a VM before exporting the OVF to the storage location or share. This is so Morpheus has a full and consistent copy of the VM state.
6.5 Managing Backups

6.5.1 Overview

Backups are automatically configured and performed on each new Morpheus-provisioned Instance. Users can edit the frequency of backups. Administrators can define destination targets where backups are stored and perform all user-based tasks.

6.5.2 To View Backups:

Select the Backups link in the navigation bar.

**Note:** If backups are disabled, they are still created upon instance provisioning and can be executed manually. However, backups will not be executed on a schedule automatically. Scheduled backups must be enabled by an administrator to run automatically. To review how to enable/disable backups see here.

Backup View

Review information about configuration such as: schedule, target details, total amount and successfully run backups, total and average size of backups from the Backup Page.

To Display Backup

1. Select the Backups link in the navigation bar.
2. Select the Backups link in the sub navigation bar.
3. Clicking the backup name to review its details.

Create Instance Backup

To create instance backup

1. Select the Backups link in the navigation bar.
2. Select the Backups link in the sub navigation bar.
3. Click the Add Backup button.
4. From the Create Backup Wizard select the radio button Instance, then click Next.
5. Input the following:
   - **Name** Name of the backup job being created.
   - **Instance** Select an instance to backup from the dropdown.
6. Click Next.
7. Depending on the instance type selected in the previous step, enter additional details such as:
   - Database Name
   - Username
   - Password
8. Click the Next button.


10. Click Complete to save.
7.1 Overview

Morpheus provides great monitoring features out of the box. Anything provisioned within Morpheus automatically gets a check created in the monitoring service. These checks are organized hierarchically in “Groups” and “Apps”. This makes it easy to gain a perspective as to what a customer or full stack facing impact is in the event of a particularly instance failure. This also takes into account redundancy layers when it comes to calculating the applications overall uptime percentage.

There are also several integrations built into the monitoring subsystem of Morpheus including App Dynamics, New Relic, and even Service Now integration.

7.1.1 Logs

Overview

The logging architecture backing Morpheus uses the latest and greatest technologies and standards to be able to service large amounts of log traffic as well as facilitate easy viewing. Utilizing elasticsearch behind the scenes and buffered log transmission protocols Morpheus provides a highly efficient and highly scalable solution for capturing log data from anything provisioned via the system. By utilizing common formats (syslog) it is also very easy to forward logs to external third party log services.

Configuration

Logging configuration can be setup in the Administration > Settings > Logs section. There are useful settings here, including customizing the retention policy (7 days by default). This could be expanded to years for PCI compliance purposes or other requirements an organization might have.

Note: When increasing the retention policy of the logging system, it may be necessary to scale out the elasticsearch cluster. Please refer to the relevant information with regards to scaling elasticsearch and advanced installation options for externalizing the elasticsearch cluster.

The Log administration section also provides options for setting custom syslog forward rules. These rules are applied on each individual host therefore keeping the Morpheus appliance itself out of the data plane. For information on different syslog formatting rules please refer to the [http://www.rsyslog.com/sending-messages-to-a-remote-syslog-server/][1] documentation.
Usage

Morpheus automatically sets up and configures logging for all of the standard catalog items provisioned through morpheus. This includes both Docker containers as well as virtual machines. Simply view instance-specific logs in instance detail via the “Logs” tab.

There are several filtering capabilities built into the logging UI with more being added continually. Easily toggle log level filters from the dropdown or change the date range filter using the handy date filter component. A chart is also displayed above logs representing the log counts by level over the selected time range (default last 24 hours). A handy pattern search is also available with some rather capable features based on Lucene search syntax.

Tip: It may be useful to review the Lucene search query syntax for powerful use cases: https://lucene.apache.org/core/2_9_4/queryparsersyntax.html[[]Syntax Guide]

There are several other places logs can be viewed. Not only can they be viewed across an application in app detail but also across all instances in the account. The main level Logs section provides an ability to query all logs produced by the system. It is also possible to view host-specific logs on a docker host by viewing the host detail page via Infrastructure.

Note: New features are on the roadmap for the main logs section including saved searches, and handy charting dashboards for garnering insights out of log data.

Exporting Logs

Log Settings

There are three main log areas in Morpheus

• Agent Logs
• Morpheus Server Logs
• Activity / Audit Logs

Agent Logs

When Instances are deployed through Morpheus, the installed Agent captures application logs and sends them back to the Morpheus server.

In most cases, the built-in Morpheus logging features are sufficient for tracking and reviewing Agent logs. However, if needed, Morpheus supports integration with advanced logging systems. See the log integration section above for more information.
Morpheus Server Logs

The main Morpheus server log is in /var/log/morpheus/morpheus-ui and the latest log file is named current. This log is archived every 24hrs. There are a number of other log files for the individual infrastructure components as well.

If you wish to export these to an external syslog platform, do the following:

1. Once you have configured your syslog destination (edit rsyslog.conf), create a morpheus-syslog.conf file in the /etc/rsyslog.d directory and add the following entries

```groovy
module(load="imfile" PollingInterval="10")
input(type="imfile" File="/var/log/morpheus/morpheus-ui/current" Tag="morpheus-ui" ReadMode="2" Severity="info" StateFile="morpheus-ui")
input(type="imfile" File="/var/log/morpheus/check-server/current" Tag="check-server" ReadMode="2" Severity="info" StateFile="check-server")
input(type="imfile" File="/var/log/morpheus/guacd/current" Tag="guacd" ReadMode="2" Severity="info" StateFile="guacd")
input(type="imfile" File="/var/log/morpheus/elasticsearch/current" Tag="elasticsearch" ReadMode="2" Severity="info" StateFile="elasticsearch")
input(type="imfile" File="/var/log/morpheus/mysql/current" Tag="mysql" ReadMode="2" Severity="info" StateFile="mysql")
input(type="imfile" File="/var/log/morpheus/nginx/current" Tag="nginx" ReadMode="2" Severity="info" StateFile="nginx")
input(type="imfile" File="/var/log/morpheus/rabbitmq/current" Tag="rabbitmq" ReadMode="2" Severity="info" StateFile="rabbitmq")
```

2. Restart rsyslog

The logfiles will now be forwarded to the destination you have defined.

This configuration is valid for an ‘all-in-one’ Morpheus server. If the infrastructure components are running on separate servers /clusters, you will need to create the relevant redirects for the logs on those boxes.

Activity Log

The final log type that may require export is the Morpheus Activity log. This tracks system changes made by users, for example create and delete instances etc.

1. To set up CEF/SIEM auditing export, you should edit the following file: logback.groovy located at /opt/morpheus/conf/logback.groovy.

2. Copy the below configuration to the bottom of the logback.groovy configuration file, save and then exit.

```groovy
appender("AUDIT", RollingFileAppender) {
    file = "/var/log/morpheus/morpheus-ui/audit.log"
    rollingPolicy(TimeBasedRollingPolicy) {
        fileNamePattern = "/var/log/morpheus/morpheus-ui/audit_%d{yyyy-MM-dd}.%i.log"
        timeBasedFileNamingAndTriggeringPolicy(SizeAndTimeBasedFNATP) {
            maxFileSize = "50MB"
        }
        maxHistory = 30
    }
    encoder(PatternLayoutEncoder) {
        pattern = "[%d] [%thread] %-5level %logger{15} - %maskedMsg %n"
    }
}
logger("com.morpheus.AuditLogService", INFO, ['AUDIT'], false)
```
3. Once you have done this, you need to restart the Morpheus Application server. To do this, do the following:

```
morpheus-ctl stop morpheus-ui
```

**Note:** Please be aware this will stop the web interface for Morpheus.

4. Once the service has stopped enter the following at the shell prompt to restart (if the service does not stop, replace stop with graceful-kill and retry)

```
morpheus-ctl start morpheus-ui
```

5. To know when the UI is up and running you can run the following command

```
morpheus-ctl tail morpheus-ui
```

Once you see the ASCI art show up you will be able to log back into the User Interface. A new audit file will have been created called audit.log and will found in the default Morpheus log path which is `/var/log/morpheus/morpheus-ui/`

Instead of writing the output to a log file, you could create an Appender definition for your SIEM audit database product

**morpheus-ssl nginx logs**

**Note:** Morpheus does not put a logrotate in for Morpheus-ssl access logs

svlogd will only rotate the current file, nginx is setup to write the access logs to separate files and not stdout.

Implementation of a log rotate is left up to up to end users for files outside of the services. This is done in case end users have a log management solution.

Below is what a suggested configuration looks like for the file `/etc/logrotate.d/morpheus-nginx`:

```
/var/log/morpheus/nginx/morpheus-access.log {  
daily  
rotate 14  
compress  
delaycompress  
missingok  
notifempty  
create 644 morpheus-app morpheus-app  
postrotate  
  [ ! -f /var/run/morpheus/nginx/nginx.pid ] || kill -USR1  
  `cat /var/run/morpheus/nginx/nginx.pid`  
endscript }
```
7.1.2 Apps

App monitors are very useful for seeing an aggregation of failures or impact based on a set of checks and groups. App monitors typically correlate to Apps provisioned from Morpheus Blueprints but can also be manually created and organized. They can be great for visualizing the customer impact a failure might have or even keeping up on a screen in a NOC. To create an App monitor:

**Name**  A friendly name for the new app monitor in Morpheus

**Description**  An optional description value to identify the app monitor

**Max Severity**  The maximum severity incident a failed app may create. This setting overrides check and group max severity settings

**Affects Availability**  When checked, this failed app impacts system-wide availability calculations

**App Checks**  Use the typeahead field to select as many checks as needed to complete the app monitor. Checks are created in Monitoring > Checks and must exist prior to creating the app monitor

7.1.3 Checks

The Monitoring system is composed of individual checks. A check is created for every container or vm that is provisioned through Morpheus. One interesting thing about these checks is they are type aware. There are several different built in check types that are selected based on the service or instance type that is being provisioned. These range from database type checks to web checks and message checks. They are highly configurable and also feature fallback check types for those more generic use cases.

Checks can be customized to run custom queries, check queue sizes, or even adjust severity levels and check intervals. All of these things can be controlled from the Checks sub tab within Monitoring.

**Health**

A check can have 3 health states. They are Failed, Warning (Recovering), and Healthy. When a check test fails the system automatically reattempts the check after 30 seconds to eliminate false positives. This will convert the check into a Failed state and raise the appropriate severity incident depending on the grouping of the check. When a check recovers it automatically goes into a Warning state. This will remain in the warning state until 10 successful check runs have completed.

**Options**

All check types have several core options and some of these default options can be configured in Admin > Monitoring. This includes the default check interval time. By default a check is run every 5 minutes. This can however be changed to run as frequently as once every minute.

- **Max Severity:** The maximum severity level impact for a created incident that can occur if the check fails (defaults to Critical).
- **Check Interval:** The frequency with which a check is run (default 5 minutes).
- **Affects Availability:** Whether or not this check impacts overall system availability calculations.
SSH Tunneling

In many cases when it comes to monitoring databases, and services they may not be fronted on the public ip’s for external monitoring. To reach these safely, and securely Morpheus provides an SSH Tunneling mechanism for its check servers. This allows the check to be confirmed via an ssh port tunnel securely using a keypair.

Check Servers

On a base installation of Morpheus a single check server is installed on the appliance. This is used for running any custom user checks. This service connects to the provided rabbitmq services and can be moved off or even scaled horizontally onto sets of check servers. All other checks that are related to provisioned containers or VMs are executed by the installed agent on the guest OS or Docker host.

Check types

Web Check

A web check is useful to identify if a url is reachable and the text to match check criteria confirms if the website is loading with the expected values. The text to match character should be within the first few lines of the page source.

Use case:

Adding a check to make sure morpheus demo environment is functioning. The below check will login to the morpheus UI and look for a text Morpheus on the dashboard page.

Values to be added in Check:

- Name: “<enter name>”
- Type: Web Check
- Interval: 5 mins (Select an interval)
- Max severity: Critical
- Check the box for affects availability
- Web Url: https://demo.morpheusdata.com/operations/dashboard (Note: this page will load only if my login is successful. Enter the login details in Username and password fields)
- Request Method: GET
- Basic Authentication: * User: <username> * Password: <password>
- Text to Match: “Morpheus” (Login to the url and on the page of dashboard, right click and select view page source. In the first few lines, look for a text that you want this check to verify)
- Save Changes
**Push API Check**

This check can be used to send an API call to morpheus from a platform to check if the push api is working. A push Check is not polled regularly by the standard monitoring system. Instead it is expected that an external API push updates as to the status of the check timed closely with the configured check interval setting. This is used to throttle the push from performing too many status updates.

**Note:** If a check is not heard from within the check intervals, It’s status will be updated to error and an incident will be raised as if it failed.

**Use Case:**

Send an API call from an app to make sure the API is not cluttered and can send checks in a 2 mins interval.

**Values to be added to the check:**

- Name: “<enter name>”
- Type: “Push API Check”
- Interval: 5 mins (Select an interval)
- Max severity: Critical
- Check the box for affects availability
- Copy the curl command are schedule to send this via your API. For testing we used postman to send the api call at an interval of 4 mins.
- Save Changes

**MySQL Check**

This check is used to run a query on a host running mysql.

**Use Case:**

Query localhost running mysql to query a table to check if there is any status as requested. If the status has a count of 1 then the check would pass else mark it as critical.

**Values to be added to the check:**

- Name: “<enter name>”
- Type: “MySQL Check”
- Interval: 5 mins (Select an interval)
- Check the box for affects availability
- Host: 127.0.0.1
- Port: 3306
- DB Name: morpheus
- User: <db user name>
- Password: <password>
- Query: “select count(*) as count from request_reference where status = ‘requested’;”
• Operator: Equal
• Check results: 1
• Save Changes

7.1.4 Monitoring Groups

Group monitors can only contain checks and can be edited or created in Monitoring > Groups. Besides simply adding and removing checks to a group there are a few other useful options that can be customized in a group:

Name  A friendly name for the group monitor in Morpheus
Min Checks This specifies the minimum number of checks within the group that must be happy to keep the group from becoming unhealthy
Max Severity The maximum severity incident a failed check may create. This setting overrides a check’s max severity setting
Affects Availability If checked, a failing group monitor impacts system-wide availability calculations
Checks Use the typeahead field to select pre-existing checks for the group monitor. If check(s) need to be created, this can be done in Monitoring > Checks

Note: Some useful information can also be seen on the detail page of a check. For example, the average response time of all checks within the group, or an aggregated check history can be viewed.

7.1.5 Incidents

Incident management is very important in any IT Operations environment. The ability to notify the appropriate people of an outage that requires immediate attention is critical to reducing recovery time and even preventing potential customer facing impacts. Because of this, Morpheus provides incident management features as well as external integrations out of the box.

Incidents can be found in the Monitoring > Incidents section. When a check fails, an incident is automatically raised. These can vary in severity based on the user configured check severities as well as the group hierarchy (representative of redundancy).

Incidents are also grouped. If an application is impacted and multiple checks fail for that application they automatically get grouped together in one Incident that can fluctuate or escalate in severity as time progresses. These incidents can be muted so as not to affect availability and they can also be resolved manually with an option to detail resolution information.

There are also integrations and API’s for integrating with existing corporate workflows when it comes to incident management.
7.1.6 Contacts

To configure user notifications, a contact must first be created in Monitoring > Contacts. These contacts can be one of a few types:

- **Contact**: Used for either Email or SMS
- **Web Hook**: Used for posting a notification to a web endpoint or Alert Ops
- **Slack Hook**: Used for posting notifications to a Slack channel (ex. https://slack.com/[\{}{Slack}\])
- **VictorOps**: Provides a web post format consistent with the required notification format for Victor Ops.

Most of these options provide convenient examples and information when configuring the contact. Once they are configured, contacts can freely be used to build *Alert Rules*.

7.1.7 Alert Rules

Alert Rules provide a powerful means to configure who gets notified in various scenarios. These scenarios include targeting specific checks, groups, or apps, and adding the appropriate recipients to be notified during a situation in which those filters are impacted.

- **Min Duration**: This setting delays notification to the recipients by the entered number of minutes required for the incident to be opened.

- **Min Severity**: Some executives might want to be notified of an outage but only if the severity impact goes above a certain level. This is very useful for scoping escalations.

To add recipients to a rule just start typing their name in the Recipients section towards the button of the edit form. An auto-complete list will start populating with contact names. Once one is selected a delivery method can be selected as well as whether or not they should be notified of any escalation changes and/or closed incidents. The delivery methods available depend on the type of contact information configured for your contact. If needed, contacts can be created or edited in Monitoring > Contacts.

**Tip:** A recipient can be in multiple alert rules and can even be configured to be notified via different methods depending on the rule. A useful example might be to alert someone via email for lower severity incidents but SMS for critical severity levels.
8.1 Cypher

8.1.1 Overview

Cypher at its core is a secure Key/Value store. But what makes cypher useful is the ability to securely store or generate credentials to connect to your instances. Not only are these credentials encrypted but by using a cypher you don’t have to burn in connection credentials between instances into your apps.

Cypher keys can be revoked, either through lease timeouts or manually. So even if somebody were to gain access to your keys you could revoke access to the keys and generate new ones for your applications.

Keys can have different behaviors depending on the specified mountpoint.

8.1.2 Mountpoints

- **password** Generates a secure password of specified character length in the key pattern (or 15) with symbols, numbers, upper case, and lower case letters (i.e. password/15/mypass generates a 15 character password).

- **tfvars** This is a module to store a tfvars file for terraform app blueprints.

- **secret** This is the standard secret module that stores a key/value in encrypted form.

- **uuid** Returns a new UUID by key name when requested and stores the generated UUID by key name for a given lease timeout period.

- **key** Generates a Base 64 encoded AES Key of specified bit length in the key pattern (i.e. key/128/mykey generates a 128-bit key)
  
  - Key lease times are entered in seconds and default to 32 days (2764800 s).
    
    - Quick Time Reference:
    - Day: 86400
    - Week: 604800
    - Month (30 days): 2592000
    - Year: 31536000
8.1.3 Creating Cypher Keys

1. Navigate to Services - Cypher and select “+ ADD KEY”
2. Configure one of the following types of Keys:

8.1.4 Password

A Cypher password generates a secure password of specified character length in the key pattern (or 15) with symbols, numbers, upper case, and lower case letters (i.e. password/15/mypass generates a 15 character password).

**Key** Pattern “password/character_length/key”

Example: password/10/mypassword

**Value** Leave the Value filed blank for a password, as it will be generated.

**Lease** Enter lease time in seconds (ex. 604800 for one week)

Save changes and the password will be generated and available for use.

If your user role has Cypher: Decrypt permissions, a “DECRYPT” button will be available in the Cypher section to view the generated password.

To delete the password key, select Actions > Remove and confirm.

8.1.5 Secret

A Cypher secret is the standard secret module that stores a key/value in encrypted form.

**Key** Pattern “secret/key”

- EXAMPLE: secret/mysecret

**Value** Add the secret value to be encrypted

**Lease** Enter lease time in seconds (ex. 604800 for one week)

Save changes and the secret will be encrypted and available for use.

If your Morpheus user role has Cypher: Decrypt permissions, a “DECRYPT” button will be available in the Cypher section to view the secret.

To delete the secret, select Actions > Remove and confirm.

8.1.6 UUID

A Cypher UUID Returns a new UUID by key name when requested and stores the generated UUID by key name for a given lease timeout period.

**Key** Pattern “uuid/key”

- Example: uuid/myuuid

**Value** Leave the Value filed blank for UUID, as it will be generated.

**Lease** Enter lease time in seconds (ex. 604800 for one week)
Save changes and the UUID will be generate and available for use.

If your user role has Cypher: Decrypt permissions, a “DECRYPT” button will be available in the Cypher section to view the generate UUID.

To delete the UUID, select Actions > Remove and confirm.

### 8.1.7 Key

A Cypher Key generates a Base 64 encoded AES Key of specified bit length in the key pattern (i.e. key/128/mykey generates a 128-bit key).

**Key** Pattern “key/bit_length/key”

- Example: key/256/mykey

**Value** Leave the Value filed blank for key, as it will be generated.

**Lease** Enter lease time in seconds (ex. 604800 for one week)

Save changes and the AES Key will be generate and available for use.

If your user role has Cypher: Decrypt permissions, a “DECRYPT” button will be available in the Cypher section to view the generate AES Key.

To delete the UUID, select Actions > Remove and confirm.

### 8.1.8 Using Cypher Keys in Scripts

To use a cypher Key in a script, use the following syntax:

```
<%=cypher.read('var_name')%>
```

Example: `PASSWORD=<%=cypher.read('secret/myuserpassword')%>`

**Note:** You can reference the original owner of a workflow so that keys can be used in a sub-tenant. Example `PASSWORD=<%=cypher.read('secret/myuserpassword')%>` could be changed to `PASSWORD=<%=cypher.read('secret/myuserpassword', true)%>` within a library or a workflow and the true means OWNER true. This will keep that key in the master tenants cypher store.

### 8.2 Archives

#### 8.2.1 Overview

Archives provides a way to store your files and make them available for download by your Scripts and Users. Archives are organized by buckets. Each bucket has a unique name that is used to identify it in URLs and Scripts.
8.2.2 Storage Provider

Archive buckets are assigned a Storage Provider (Object Store). This is where the bucket will write its files. A Storage Provider can be configured to use the local appliance file system (Local), an Amazon S3 bucket, etc.

Every archive bucket generates and uses a random File Path to store its files under. This ensures two different archive buckets will not contend for the same backend storage location.

8.2.3 Permissions

Visibility

Visibility determines whether your files are secure or not.

Private  This secures your files. Only authorized users of the Owner and Tenants account may view the bucket and download its files. This is the default.

Public  This makes your files available to the public. Anyone, including anonymous users/scripts can download these files without any authentication.

**Warning:** Be careful not to store sensitive files in a Public archive.

Users of the Owner account may fully manage the files in a bucket.

Tenants

Users of the Owner account may fully manage the files in a bucket. Users of the Tenant account(s) will have read-only access. They may browse and download files in the bucket.

Both Owner and Tenants must have the Services: Archives permission to access a Private bucket. READ level access allows browsing and downloading files in the bucket.

FULL access allows full management of the bucket and its files. This includes modifying files and links, bucket settings and deleting it.

8.2.4 Files

To add a file to a bucket, click on the bucket name, and then click the + ADD FILE button. Once added, click on the file name to access the links, history and script section for the file.

8.2.5 Links

You can create a Link to download a Private file without any authentication. Links may be configured to expire after a period of time.
8.2.6 Scripts

Morpheus automatically generates syntax for creating a link to a file in your Scripts. When the Script is generated, it will create a temporary link to download the file and return the URL of that link. This link is made available to the public. It is accessible to any user or script that can reach the appliance. Downloading the file only requires knowing the URL, which includes a secret token parameter. You can specify the number of seconds before the link expires. The default value is 1200 (20 minutes).

8.3 Image Builder

The Morpheus Image Builder tool creates vmdk, qcow2, vhd and raw Images from scratch. The Image Builder creates a blank VM in VMware, attaches an os iso, executes a boot script on the VM at startup via VNC which calls a preseed script which runs the unattended os installation and configuration. Morpheus then executes an ova export of the completed vmdk to target Storage provider, and converts the image to all other specified formats. The new Virtual Image records are automatically added to Morpheus and the Images are then available for use.

8.3.1 Requirements

- **DHCP must be enabled on the network specified for the VM in Morpheus, and network settings configured for DHCP in Morpheus**
  The blank VM must get network configuration via DHCP upon boot. Static IP assignment is not possible.

- **Hypervisor Console must be enabled on the Target Cloud**
  Morpheus utilizes VNC to pass the boot script to the VM.

- **VM must be able to reach and resolve the Morpheus appliance url over 443**
  The boot script calls to the Morpheus appliance to get the preseed script.

- **Valid Linux iso set for the Virtual Image. Windows is not supported.**
  The iso can exist in the target cloud or uploaded to Morpheus

  **Note:** cloud-init enabled must be disabled on the iso Virtual Image settings.

- **Access to target ESXi host(s) over 443 and ESXi hostname dns resolution**
  - Same requirement as Hypervisor Console and Image upload/download to/from vCenter.

- Valid Boot Script

- Valid Pre-seed script

- Valid Storage Provider configure for ova export of generated image.

8.3.2 Sample Scripts

Sample Boot Script

```
<wait5><tab> text ks=<%=preseedUrl%><enter>
```

**Note:** `<%=preseedUrl%>` is a Morpheus variable that will populate with the Morpheus appliance url.
Morpheus Documentation

Sample Preseed Script

```plaintext
# CentOS 7.x kickstart file - ks.cfg
#
# For more information on kickstart syntax and commands, refer to the
# CentOS Installation Guide:
# --Installation_Guide/sect-kickstart-syntax.html
#
# For testing, you can fire up a local http server temporarily.
# cd to the directory where this ks.cfg file resides and run the following:
# $ python -m SimpleHTTPServer
# You don't have to restart the server every time you make changes. Python
# will reload the file from disk every time. As long as you save your changes
# they will be reflected in the next HTTP download. Then to test with
# a PXE boot server, enter the following on the PXE boot prompt:
# $ > linux text ks=http://<your_ip>:8000/ks.cfg

# Required settings
lang en_US.UTF-8
keyboard us
rootpw password
authconfig --enableshadow --enablemd5
timezone UTC

# Optional settings
install
cdrom
user --name=cloud-user --plaintext --password password
unsupported_hardware
network --bootproto=dhcp
firewall --disabled
selinux --permissive
bootloader --location=mbr --append="biosdevname=0 net.ifnames=0"
text
skipx
zerombr
clearpart --all --initlabel
autopart --type=plain
firstboot --disabled
reboot

%packages --nobase --ignoremissing --excludedocs
openssh-clients
# Prerequisites for installing VMware Tools guest additions.
# Put in kickstart to ensure first version installed is from install disk,
# not latest from a mirror.
kernel-headers
kernel-devel
gcc
make
perl
curl
wget
bzip2
dkms
patch
```

(continues on next page)
net-tools
git
# Core selinux dependencies installed on 7.x, no need to specify
# Other stuff
sudo
nfs-utils
open-vm-tools
-fprintd-pam
-intltool
-biosdevname

# unnecessary firmware
-aic94xx-firmware
-atmel-firmware
-b43-openfwwf
-bfa-firmware
-ipw*-firmware
-irqbalance
-ivtv-firmware
-iwl*-firmware
-libertas-usb8388-firmware
-ql*-firmware
-rt61pci-firmware
-rt73usb-firmware
-xorg-x11-drv-ati-firmware
-zd1211-firmware
%end

%post
# configure vagrant user in sudoers
echo "%cloud-user ALL=(ALL) NOPASSWD: ALL" >> /etc/sudoers.d/cloud-user
chmod 0440 /etc/sudoers.d/cloud-user
cp /etc/sudoers /etc/sudoers.orig
sed -i "s/^\(.*requiretty\)$/#\1/" /etc/sudoers
# keep proxy settings through sudo
echo 'Defaults env_keep += "HTTP_PROXY HTTPS_PROXY FTP_PROXY RSYNC_PROXY NO_PROXY"' >> /etc/sudoers
%end

8.4 VDI Pools

The VDI Pools section of Morpheus Tools provides a management area for defining VDI Pools and VDI Apps that a user can consume within the Virtual Desktop Persona.

Pools can be either persistent or non-persistent and have various controls pertaining to idle pools and minimum or maximum sizes. The idea here is to make sure a server is always quickly available to accommodate user demand.

Morpheus leverages its Instance Types concept for provisioning servers within the VDI Pool. All the options available during Instance provisioning is available for setting the base server configuration. This includes Workflows, domain joins, tagging, image selection and more.

A timeout setting can also be applied to release pool allocations from a user once they have disconnected their session. For non-persistent pools, a good recommendation is ten minutes whereas, for a persistent pool, a sensible recommendation would be around one hour.

Pool behavior changes depending on the pool type. In a non-persistent pool, when a timeout period expires, the VM is
destroyed and a new one is allocated for use. This functionality will change based on the cloud technology in a future update allowing for potential recycling of the VMs. In a Persistent pool, when the lease timeout expires, the Instance will shutdown until the user requests it again in the future. It is important to note that lease timeouts auto-extend for as long as the user is logged into or browsing any area of the Morpheus application. Once the user closes their browser or logs out of their session, the timeouts will no longer auto-extend.

8.4.1 Configuring Access to VDI Pools

Access to the Virtual Desktop Persona and individual VDI pools is handled through the user Role and, where applicable, Tenant Role. When creating a new Role, access is restricted to the Virtual Desktop Persona and all VDI pools by default. To grant access:

1. Navigate to the Role (Administration > Roles > Selected Role)
2. Access the Personas tab
3. Toggle the Virtual Desktop permission to “Full” or “None”
4. Access the VDI Pool Access tab
5. Toggle access to selected VDI pools to “Full” or “None”, you can also toggle permission on all pools to “Full” or “None” with the Global Access selection
6. Role changes are saved automatically, there is no need to manually save

Additionally, users should have a Linux and/or Windows username and password configured in their user profiles in order for virtual desktop login to be as seamless as possible. User profiles are accessed by clicking on the user’s name in the upper-right corner of the application windows and clicking USER SETTINGS. The section to enter Windows and Linux account credentials is in the right column of the page.

8.4.2 Creating VDI Templates

Note: The following guide focuses on VMware and Windows but is applicable to most cloud environments. Morpheus also supports Linux virtual desktops.

1. Create a thin-provisioned VM in the VMware vCenter console. It’s recommended you allocate at least 50 GB of storage, at least 2 vCPU and at least 8 GB RAM on the template. Smaller VMs can be deployed from this template later.
2. Install a Windows operating system, there is no need to supply a license during deployment.
3. Supply the initial username and password
4. Install any updates, applications or optimizations. See the next section for recommended optimizations for the most performant virtual desktop experience
5. Shutdown the VM and convert to a template. Optionally, you can also use the Linked Clones (VMware) process which is described in a later section
Suggested Optimizations

Reducing display and input delays is key to providing the best virtual desktop experience for the user. Consider the following optimizations for VDI desktops and servers:

- Disable desktop wallpapers
- Implement Roaming Profiles
- Enforce WDDM remote display driver
- Re-enable local Administrator
- Delete the initial created user profile
- Clean up any unneeded installer packages

Additionally, there are a number of OS optimization tools available on the Internet which are specific to VDI use cases.

Linked Clones

Linked Clones are a feature of VMware which references snapshots of a VM to deploy from. This adds the advantage of quicker clone times and the ability to more easily share small modifications to a file system. Morpheus supports Linked Clones but recommends them for VDI workloads only.

Note: Linked Clones are not templates but rather powered down VMs.

1. Locate the VM you desire to have the Linked Clone in Morpheus. If it’s not currently managed by Morpheus, navigate to the appropriate Cloud (Infrastructure > Clouds), find the VM on the “VMs” tab, and click “Convert to Managed” from the ACTIONS menu

2. In the CONVERT TO INSTANCE modal, select “No Agent Install” in the AGENT field

3. If snapshots are already on the VM, these will now be synced by Morpheus. If you have not yet created a snapshot, do so in the vCenter console (and refresh the Cloud integration in Morpheus afterward) or from the ACTIONS menu in Morpheus itself. Be sure to take a snapshot of a powered-off VM and give the snapshot a name that will be identifiable for administrators

4. From the Instance detail page in Morpheus, navigate to the Backups tab to find the snapshot

5. Select “More” and create the Linked Clone

6. The Linked Clone will now appear in the Morpheus Virtual Image repository (Library > Virtual Images), ready to use with your custom Layouts

Note: You should modify the Virtual Image to “Force Guest Customization” unless you sysprep your VM at shutdown time
8.4.3 Creating or Editing a VDI Pool

VDI pools are configured from the Tools menu (VDI Pools selection). The following information is displayed in the VDI pools list view, bear in mind some fields may be hidden depending on how you’ve configured your VDI pools list view (gear icon):

- **TYPE:** An icon indicating the machine type associated with the pool. Morpheus includes many logos out of the box and also allows users to set their own custom icons
- **NAME:** The friendly name given to the VDI pool
- **PERSISTENT:** A check mark will appear when the VDI pool is configured for persistent virtual desktops
- **ENABLED:** A check mark will appear when the VDI pool is enabled and visible to users whose Role permissions allow them access
- **POOL USAGE:** A graph representing the usage of the VDI pool. The total length of the bar represents the maximum pool size based on the configuration. Green segments represent available virtual desktops, blue segments represent reserved virtual desktops, yellow segments represent virtual desktops which are being prepared, and gray segments represent additional pool capacity which could be made available depending on how many virtual desktops are currently reserved and how many idle machines you’ve configured the pool to keep available
- **DESCRIPTION:** A description of the virtual desktop type, if provided

Create a VDI pool by selecting `+ ADD` from the VDI Pools tab or edit an existing one by clicking on the pencil icon from the appropriate row. Configure the following, fields containing a vertical blue bar along the left edge are required:

- **NAME:** A friendly name for the VDI pool in Morpheus
- **DESCRIPTION:** A description of the virtual desktop type
- **MIN IDLE:** The minimum number of virtual desktops that should remain idle and ready
- **INITIAL POOL SIZE:** The number of virtual desktops that will be prepared when the pool is created or enabled
- **MAX IDLE:** The maximum number of virtual desktops that remain idle and ready. Machines will be shut down as necessary when this number is exceeded due to users vacating their machines
- **MAX SIZE:** The total number of virtual desktops this pool can have. Additional users will not be able to access machines once this number is reached
- **LEASE TIMEOUT (MINUTES):** The user lease time on a virtual desktop they’ve reserved. The lease will continue to auto-renew itself as long as the user is logged into Morpheus. Once the user has logged out and the lease timeout period has expired, the machine will be released as appropriate based on your configuration
- **PERSISTENT:** Pools with persistent virtual desktops will reserve a machine for each user in order to preserve settings, installed applications, work files and more. Machines in persistent pools will be shut down rather than destroyed when they are no longer in use.

- **RECYCLABLE:** When enabled, the VDI Instance will revert back to a snapshot and become available once again after the user has logged out and the VDI session has expired. This behavior will not apply to VDI pools which are also configured to be persistent because in that configuration the Instance is merely stopped and saved for the user’s next session. This feature is currently only available for Cloud types which support snapshot management (VMware, Nutanix, and vCD).

- **ALLOW COPY** Enables or disables the ability for the VDI user to copy contents from the VDI instance to the local clipboard.

- **ALLOW PRINTER** When enabled, users local system printers can be targeted from the VDI Instance.

- **ALLOW HYPervisor CONSOLE:** When checked, native cloud console will be enabled (if available) rather than using Morpheus-native RDP/SSH capability.

- **AUTO CREATE LOCAL USER UPON RESERVATION:** When marked, the user configured in Morpheus user settings will be created when the machine is initially accessed. If unchecked or if there is no user configured in Morpheus user settings, ensure the machine is joining a domain or there is a known user on the machine image in order to allow access.

- **ENABLED:** When marked, the initial pool size will begin to deploy once the VDI pool is saved. The icon for this desktop environment will also be presented to Virtual Desktop Persona users.

- **CONFIGURE:** Click this button to configure the deployment configuration each system will use. The wizard is identical to the Instance provisioning wizard meaning all available Instance Types, Workflows, and more are available to virtual desktop machine creation. Consult the steps above to see an example VDI image prep walkthrough.

- **LOGO:** Upload or select a logo to represent the virtual desktop type to users.

- **VDI APPS:** Optionally select one or more frequently-used applications the user can launch directly. Users will also have the option to launch into the desktop.

- **VDI GATEWAY** Select a configure VDI Gateway for VDI sessions to be redirected to. VDI sessions will be redirected to the gateway when a gateway is specified.

**Guest Console SSH Tunnel (optional)** A Jump Host can be configured for VDI session connections. Morpheus will tunnel through the Jump Host when connecting Guest Console sessions for VDI. This is not applicable for Hypervisor Console connections.

- **GUEST CONSOLE JUMP HOST** Jump Host IP address or hostname used to connect to the Jump Host for Guest Console sessions to VDI Instances.

- **GUEST CONSOLE JUMP USERNAME** Jump Host Username used to connect to the Jump Host for Guest Console sessions to VDI Instances.

- **GUEST CONSOLE JUMP PORT** Jump Host Port used to connect to the Jump Host for Guest Console sessions to VDI Instances.

- **GUEST CONSOLE JUMP PASSWORD** Jump Host Password used to connect to the Jump Host for Guest Console sessions to VDI Instances (optional if key specified).

- **GUEST CONSOLE KEYPAIR** Jump Host SSH Key used to connect to the Jump Host for Guest Console sessions to VDI Instances (optional if password specified).

**Note:** A Guest Console Keypair included here must be a local keypair, not a synced keypair.
8.4.4 Creating or Editing a VDI Apps

VDI Apps allow users to launch directly into commonly-used apps rather than the OS desktop. Currently, VDI Apps only work with RDP Windows Instances, taking advantage of native Windows Remote Application functionality. Natively-hosted remote desktop applications can only be presented from Windows 10 Enterprise and Education. Other versions of Windows 10 can present remote applications using the procedure below:

1. Open the Windows Registry Editor

2. Locate the following entry:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\TSAppAllowList

3. Navigate to fDisabledAllowList and set its value to “1” in the right-hand pane

4. Add a new key under TSAppAllowList and name it “Applications”

5. Add a new key under “Applications” using any name you’d like

6. Within this new key, create two new string values, one called “Name” and one called “Path”

7. The string value for “Name” should describe the application (ex. “Notepad”)

8. The string value for “Path” should be the absolute path to the executable for that application (ex. “C:\Windows\System32\notepad.exe”)

VDI Apps are created by selecting + ADD from the VDI Apps tab or edit an existing one by clicking on the pencil icon from the appropriate row. Configure the following, fields containing a vertical blue bar along the left edge are required:

- **NAME**: A friendly name for the VDI App in Morpheus

- **DESCRIPTION**: A description of the virtual app type

- **LAUNCH PREFIX**: A reference to the remote app registry prepended with two pipes ( || ). For example, we might create a registry “Chrome” for a Chrome browser VDI App and the associated launch prefix would be “||Chrome”

- **LOGO**: Upload or select a logo to represent the virtual app type to users
8.4.5 VDI Gateways

The Morpheus Worker is a lightweight distributed worker daemon as well as a scalable VDI Gateway. Currently, the features center around VDI Gateway but will expand to support full plugin workloads as well as agent relay capabilities.

Adding VDI Gateways to Morpheus

VDI Gateways can be linked to a Morpheus appliance and then used in VDI Pool configurations. VDI sessions will be redirected to configured gateways instead of the Morpheus appliance when a VDI Gateway is specified for a VDI Pool.

Note: A VDI Gateway is a separate VM or container instance used to route users to VDI Instances. The Morpheus VDI Gateway section is for configuring a connection to a VDI Gateway, not creating the gateway instance itself.

- **NAME** Specify a name for the VDI Gateway in Morpheus. Note that the VDI Gateway Name is not used when connecting to the gateway
- **DESCRIPTION** Specify a description for the VDI Gateway in Morpheus. (optional)
- **GATEWAY URL** The url of the VDI Gateway. This url is used to connect to the gateway, and should match the worker url of the VDI Gateway.

Upon creation, the VDI Gateway record will produce an API KEY. This API KEY needs to be specified in the morpheus-worker.rb file on the API Gateway itself under worker['apikey'] = '$API_KEY'

VDI Gateway VM Install

A VDI Gateway VM is installed and configured similarly to a Morpheus appliance via rpm or deb package.

Note: VDI Gateway Package URLs are available at https://morpheushub.com in the downloads section.

Requirements

<table>
<thead>
<tr>
<th>Table 1: Supported VDI Gateway Operating Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OS</strong></td>
</tr>
<tr>
<td>Amazon Linux</td>
</tr>
<tr>
<td>CentOS</td>
</tr>
<tr>
<td>Debian</td>
</tr>
<tr>
<td>RHEL</td>
</tr>
<tr>
<td>SUSE SLES</td>
</tr>
<tr>
<td>Ubuntu</td>
</tr>
</tbody>
</table>

- **Memory**: 4 GB RAM minimum recommended for default installations supporting up to 20 concurrent sessions. Add 50 MB RAM per additional concurrent session
- **Storage**: 10 GB storage minimum recommended. Storage is required for VDI Gateway Packages and log files
- **CPU**: 4-core minimum recommended
- **Network connectivity to and from Morpheus appliance and from users to the VDI Gateway over TCP 443 (HTTPS)
- Superuser privileges via the sudo command for the user installing the Morpheus VDI Gateway package
• Access to base **yum** or **apt** repos. Access to Optional RPM repos may be required for RPM distros

1. Download the target distro & version package for installation in a directory of your choosing. The package can be removed after successful installation.

```bash
wget https://downloads.morpheusdata.com/path/to/morpheus-worker-$version.distro
```

2. Validate the package checksum matches source checksums. For example:

```bash
sha256sum morpheus-worker-$version.distro
```

3. Next install the package using your selected distribution’s package installation command and your preferred opts. Example, for RPM:

```bash
rpm:
sudo rpm -ihv morpheus-worker-$version.$distro
Preparing... ################################# [100%]
Updating / installing...
  1:morpheus-worker-5.3.1-1.$distro ################################# [100%]
Thank you for installing Morpheus Worker!
Configure and start the Worker by running the following command:
sudo morpheus-worker-ctl reconfigure
```

4. Configure the gateway by editing `/etc/morpheus/morpheus-worker.rb` and updating the following:

```ruby
worker_url 'https://gateway_worker_url' # This is the gateway URL the |morpheus| appliance can resolve and reach on 443
worker['appliance_url'] = 'https://morpheus_appliance_url' # The resolvable URL or IP address of |morpheus| appliance which the gateway can reach on port 443
worker['apikey'] = 'API KEY FOR THIS GATEWAY' # VDI Gateway API Key generated from |morpheus| Appliance VDI Pools > VDI Gateways configuraiton
```

**Note:** By default the worker_url uses the machine’s hostname, ie `https://your_machine_name`. The default worker_url value can be changed by editing `/etc/morpheus/morpheus-worker.rb` and changing the value of worker_url. Additional appliance configuration options are available below.

5. After all configuration options have been set, run `sudo morpheus-worker-ctl reconfigure` to install and configure the worker, nginx and guacd services:

```bash
sudo morpheus-worker-ctl reconfigure
```

The worker reconfigure process will install and configure the worker, nginx and guacd services and dependencies.

**Tip:** If the reconfigure process fails due to a missing dependency, add the repo that the missing dependency can be found in and run

**Note:** Configuration options can be updated after the initial reconfigure by editing `/etc/morpheus/morpheus-worker.rb` and running `sudo morpheus-worker-ctl reconfigure` again.
6. Once the installation is complete the morpheus worker service will automatically start and open a web socket with the specified Morpheus appliance. To monitor the startup process, run `morpheus-worker-ctl tail` to tail the logs of the worker, nginx and guacd services. Individual services can be tailed by specifying the service, for example `morpheus-worker-ctl tail worker`.

**VDI Gateway Docker Install**

To Use VDI Gateway within a Docker container, a few pieces of information are needed.

Firstly, in Morpheus, go to **Tools > VDI Pools > VDI Gateways** and create a new VDI Gateway Record. Be sure to set the HTTPS URL as Morpheus will need to be able to redirect the user’s browser to that page. An API Key will be generated. Make note of this as you will need it later.

Now Simply run with:

```
docker run -d -p 8443:8443 -e MORPHEUS_SELF_SIGNED=true -e MORPHEUS_KEY={[apiKey]} -e MORPHEUS_URL=https://my.morpheusAppliance.url morpheusdata/morpheus-worker:latest
```

This will setup an HTTPS self-signed exposed port on 8443 for the vdi gateway. It is highly recommended to use valid certificates on your VDI Gateways. It could be terminated at the VIP or a p12 SSL File can be used and configured for the container.

If the docker entrypoint detects a file at `/etc/certs/cert.p12`, SSL Will be enabled on port 8443 instead. be sure to set environment variables `MORPHEUS_SSL_ALIAS` and `MORPHEUS_SSL_PASSWORD` when using p12 files.

If you wish to run in HTTP mode and SSL terminate at the VIP, you can run the container like so:

```
docker run -d -p 8080:8080 -e MORPHEUS_SELF_SIGNED=true -e MORPHEUS_KEY={[apiKey]} -e MORPHEUS_URL=https://my.morpheus.url morpheusdata/morpheus-worker:latest
```

**VDI Gateway Helm Chart Installation**

First, configure the Helm repository:

```
helm repo add morpheusdata https://gomorpheus.github.io/helm-charts-morpheus/
```

Next, install the Morpheus worker using `helm install`. You can specify each parameter using `--set key=value[,key=value]` arguments as in the following example:

```
helm install morpheus-worker --set replicaCount="1" morpheusdata/morpheus-worker
```

Alternatively, you can create a values YAML file and pass an argument as in the following example:

```
helm install -f values.yaml morpheus-worker morpheusdata/morpheus-worker
```

Upgrading the workers node(s) is as simple as refreshing the repo and using `helm upgrade`:

```
helm repo update
helm upgrade -f values.yaml morpheus-worker morpheusdata/morpheus-worker
```

To uninstall, use one of the following:

```
helm uninstall morpheus-worker
```

or
Note: `helm delete` removes all the Kubernetes components associated with the chart and deletes the release.

The following table lists the configurable parameters of the Sentry chart and their default values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>image.repository</td>
<td>Image repository</td>
<td>morpheusdata/morpheus-worker</td>
</tr>
<tr>
<td>image.tag</td>
<td>Image tag. Possible values listed here.</td>
<td>5.3.1-4</td>
</tr>
<tr>
<td>image.pullPolicy</td>
<td>Image pull policy</td>
<td>IfNotPresent</td>
</tr>
<tr>
<td>env.MORPHEUS_KEY</td>
<td>API Key for Morpheus Worker</td>
<td></td>
</tr>
<tr>
<td>env.MORPHEUS_URL</td>
<td>Morpheus FQDN with protocol</td>
<td></td>
</tr>
<tr>
<td>env.MORPHEUS_SELF_SIGNED</td>
<td>Is Morpheus using a Self Signed Certificate</td>
<td>false</td>
</tr>
<tr>
<td>service.type</td>
<td>Kubernetes service type for the GUI</td>
<td>ClusterIP</td>
</tr>
<tr>
<td>service.port</td>
<td>Kubernetes port where the GUI is exposed</td>
<td>8989</td>
</tr>
<tr>
<td>livenessProbe.initialDelaySeconds</td>
<td>Initial delay (seconds) for liveness monitoring</td>
<td>5</td>
</tr>
<tr>
<td>livenessProbe.timeoutSeconds</td>
<td>Timeout (seconds) before health check considered unhealthy</td>
<td>5</td>
</tr>
<tr>
<td>livenessProbe.periodSeconds</td>
<td>Poll interval (seconds) between health checks</td>
<td>10</td>
</tr>
<tr>
<td>livenessProbe.failureThreshold</td>
<td>Number of failed polls before restarting service</td>
<td>3</td>
</tr>
<tr>
<td>replicaCount</td>
<td>Number of Replicas if AutoScaling False</td>
<td>1</td>
</tr>
<tr>
<td>autoscaling.enabled</td>
<td>Enable AutoScaling</td>
<td>false</td>
</tr>
<tr>
<td>autoscaling.minReplicas</td>
<td>Minimum number of Replicas</td>
<td>1</td>
</tr>
<tr>
<td>autoscaling.maxReplicas</td>
<td>Maximum number of Replicas</td>
<td>100</td>
</tr>
<tr>
<td>autoscaling.targetCPUUtilizationPercentage</td>
<td>CPU Threshold for AutoScaling</td>
<td>80</td>
</tr>
<tr>
<td>autoscaling.targetMemoryUtilizationPercentage</td>
<td>Memory Threshold for AutoScaling</td>
<td></td>
</tr>
<tr>
<td>ingress.enabled</td>
<td>Enables Ingress</td>
<td>false</td>
</tr>
<tr>
<td>ingress.annotations</td>
<td>Ingress annotations</td>
<td>{}</td>
</tr>
<tr>
<td>ingress.path</td>
<td>Ingress path</td>
<td>/</td>
</tr>
<tr>
<td>ingress.hosts</td>
<td>Ingress accepted hostnames</td>
<td>chart-example.local</td>
</tr>
<tr>
<td>ingress.tls</td>
<td>Ingress TLS configuration</td>
<td>[]</td>
</tr>
<tr>
<td>resources</td>
<td>CPU/Memory resource requests/limits</td>
<td>[]</td>
</tr>
<tr>
<td>nodeSelector</td>
<td>Node labels for pod assignment</td>
<td>()</td>
</tr>
<tr>
<td>tolerations</td>
<td>Toleration labels for pod assignment</td>
<td>[]</td>
</tr>
<tr>
<td>affinity</td>
<td>Affinity settings for pod assignment</td>
<td>[]</td>
</tr>
</tbody>
</table>
There are several administrative integrations built into Morpheus that make it great to work with within any organization ranging from small to large. Especially, with its built in white label support and multitenancy capabilities, managed service providers have a wide range of capabilities when it comes to managing customer accounts and users.

9.1 Tenants

9.1.1 Overview

A Tenant in Morpheus is an isolated environment with unique users and workloads. The Master Tenant is the default Tenant in Morpheus, created upon installation. All other Tenants outside of the Master Tenants are Subtenants.

- The Master Tenant is the default Tenant created during the installation of Morpheus
- All Tenants created after installation are Subtenants. Only one Master Tenant can exist
- The Master Tenant creates and controls all Subtenants.
- Tenants are isolated environments with unique users, workloads, and Groups
- The Master Tenant can share or assign its resources to Subtenants
- Subtenants cannot share their resources with other Tenants
- Subtenants cannot see resources from other Subtenants
- Subtenants can only access Master Tenant resources that have been set to Public visibility or specifically assigned to the Subtenant

9.1.2 Roles

There are two Role types in Morpheus, Tenant Roles and User Roles. Understanding these Role types is key to effectively administering Role permissions in Morpheus. These two Role types are discussed in greater detail in this section.
Tenant Roles

Tenant Roles set the maximum permission levels for Users in the Tenant. User Role permissions will not exceed the permissions of the Tenant Role.

- Tenant Roles set the maximum permissions for a Tenant
- User Roles in a Tenant cannot exceed the permissions of the Tenant Role
- A Tenant Role can be assigned to one or multiple Tenants
- Tenant Roles determine Cloud access for the Subtenant such that all Clouds in the Master Tenant which have visibility set to Public will show as options in the Tenant Role Cloud Access tab
- Only Master Tenant Clouds given access in the Tenant Role will be accessible in the Subtenant

**Important:** Tenant Roles cap permissions on all Subtenant User Roles. User Roles can be created in the Subtenant with lesser permissions than the Tenant Role allows. Tenant Roles are designed for a Master Tenant Admin to set max permissions for the Subtenant, and a Subtenant Admin to configure User Roles inside the Subtenant.

User Roles

User Roles determine feature, Group, and Instance Type access for all Users. In a multi-Tenant environment, there are two types of User Roles: Single-Tenant User Roles and Multi-Tenant User Roles.

- **Single-Tenant User Roles:** These exist solely in the Tenant they are created in. All Roles created in a Subtenant will be Single-Tenant User Roles
- **Multi-Tenant User Roles:** The Master Tenant can create Multi-Tenant User Roles. These Roles are automatically seeded into Subtenants and can be assigned to Subtenant Users. Changes to Multi-Tenant User Roles made in the Master Tenant are propagated to all Subtenants. However, once a Multi-Tenant User Role is edited inside a Subtenant, it is no longer linked to the Multi-Tenant User Role and becomes its own unique Role. It will no longer receive propagated changes.

**Note:** Multi-Tenant User Roles are intended to make Subtenant User Role creation easier, so Master Tenant Users do not have to re-create the same base Subtenant Users Roles for every Subtenant. Multi-Tenant User Roles are not a single Role across Tenants, but more like a template that creates new Subtenant User Roles that can then be managed in the Sub Tenant.

9.1.3 Tenants

The Tenants page displays a list of all Tenants. This page enables users to Create, Edit, and Delete Tenants. The list of Tenants displays the Tenant Name, Role, Total Instances, Total Users, and the Created Date.

Click the Tenant Name to drill into the Tenant View where you can again Edit or Delete the Tenant, as well as Create Users, Edit Users, and Delete Users users belonging to the Tenant.
**Create Tenants**

To Create Tenants:
1. Select the Administration link in the navigation bar.
2. Select the Tenants link in the sub navigation bar.
3. Click the Create Tenant button.
4. From the New Tenant wizard input:
   - Name
   - Description (optional)
   - Subdomain
   - Base Role
   - Currency
5. Within the Advanced Options section, track customer data related to the Tenant if needed:
   - Account Number
   - Account Name
   - Customer Number
6. Click the *Save Changes*

**Edit Tenant**

To edit a Tenant:
1. Select the Administration link in the navigation bar.
2. Select the Tenants link in the sub navigation bar.
3. Click the Edit pencil icon on the row of the Tenant to edit.
4. Edit the Edit Tenant settings.

**Disabling Tenant**

When disabling a tenant, they are not able to login and cannot be impersonated by another tenant. However all of their information will still remain in Morpheus and they may still receive notifications and alerts.

To disable a Tenant:
1. Select the Administration link in the navigation bar.
2. Select the Tenants link in the sub navigation bar.
3. Click the Edit pencil icon on the row of the Tenant to edit.
4. Uncheck the *Enabled* box.
Delete Tenant

To delete a Tenant:
1. Select the Administration link in the navigation bar.
2. Select the Tenants link in the sub navigation bar.
3. Click the Delete trashcan icon on the row of the Tenant to delete.
4. Confirm

9.1.4 Tenant Users

The Tenant View displays a list of users belonging to the Tenant and their Name, Username, Email, and Role.

From this page: Create, Edit, and Delete users within the Tenant.

**Important:** In versions 3.1.1 and 2.12.5 and later, a Multi-Tenant User Role must be created prior to adding Subtenant Users or the User will not save. In previous versions a default Multi-Tenant Role was seeded. Due to customer requests, the seeded role was removed and a Multi-Tenant Role must be created by the Master Tenant for Subtenant Users.

Create Tenant User

To create a Tenant User:
1. Select the Administration link in the navigation bar.
2. Select the Tenants link in the sub navigation bar.
3. Click the Tenant Name on the row of the Tenant where the user will be added.
4. Click **ADD USER**
5. From the New User wizard, input the fields below:
   - First Name
   - Last Name
   - Username
   - Email address
   - Role (to be inherited by the user)
   - Password
   - Any default Windows or Linux credentials

Click **SAVE CHANGES**

**Important:** In versions 3.1.1 and 2.12.5 and later, a Multi-Tenant User Role must be created prior to adding Subtenant Users or the User will not save. In previous versions a default Multi-Tenant Role was seeded. Due to customer requests, the seeded role was removed and a Multi-Tenant Role must be created by the Master Tenant for Subtenant Users.
Edit a Tenant User

To edit a User:

1. Select the Administration link in the navigation bar.
2. Select the Tenants link in the sub navigation bar.
3. Click the specific Tenant name from the row of available Tenants.
4. Click the Edit pencil icon for your selected Tenant.
5. Edit User information

Note: Name, Username, Passwords and e-mail addresses cannot be edited on Users created from Identity Source Integrations.

Click SAVE CHANGES

Delete Tenant User

To delete a Tenant User:

1. Select the Administration link in the navigation bar.
2. Select the Tenants link in the sub navigation bar.
3. Click the Tenant Name from the row for the Tenant containing the user.
4. Click the Delete trashcan icon of the row of the user to delete.
5. Confirm

Subtenant User Login

Subtenant Users can have the same Username as the User on the Master Tenant or any other Tenant. Subtenant Users will now have to login using the subdomain prefix.

Important: Subtenant users will no longer be able to login from the main login page without specifying their subdomain.

Example: I have a username subuser that belongs to a tenant with the subdomain subaccount. When logging in from the main login url, I would now need to enter in: subaccount\subuser

9.1.5 Configuring Tenants and Resources for Multi-Tenancy

A very common scenario for Managed Service Providers is the need to provide access to resources on a customer by customer basis. Several administrative features are available in Morpheus to ensure customer resources are properly scoped and isolated. With its built multi-tenancy capabilities and white label support, managed service providers have a wide range of capabilities when it comes to managing customer Tenants and users.
Tenants

There are essentially two types of Tenants in Morpheus

- Master Tenant
- Sub Tenants

During the initial setup of a Morpheus Appliance, the Master Tenant is created. All Tenants created in addition to this Master Tenant are sub-Tenants. There can only be one Master Tenant, and sub-Tenants cannot become the Master Tenant. The delineation between the Master Tenant and sub-Tenants is important to understand for properly scoping resources across Tenants.

Creating Tenants

The Master Tenant is created during the initial appliance setup. Additional sub-Tenants can be created in the Administration > Tenants section.

The Tenants page displays a list of all Tenants. This page enables users to Create, Edit, and Delete Tenants. The list of Tenants displays the Tenant Name, Role, Total Instances, Total Users, Status (active or inactive) and the Created Date. Click the Tenant Name to drill into the Tenant View where you can edit or delete the Tenant, as well as create, edit and delete users belonging to the Tenant.

**Note:** At least one Tenant in addition to the Master Tenant is required to scope resources across Tenants.

To create a new sub-Tenant

1. Select the Administration link in the navigation bar.
2. Select the Tenants link in the sub navigation bar.
3. Click the +Create Tenant button.
4. From the New Tenant wizard input * Name (Required) * Description * Base Role * Currency (for pricing)

The Base Role defines a role set from which all roles created within the Tenant will inherit.

**Note:** In prior versions, we could set Limits when creating a Subtenant. These could restrict the amount of storage, memory, and CPUs that can be collectively provisioned by all users in the Tenant. In more recent versions, this functionality has been rolled into Policies (Administration > Policies). When creating a Policy, we are able to specify a Tenant to which the Policy should apply.

Click the Save Changes button.
Viewing Tenants

To View an individual Tenant page, select the Tenant name from the main Tenants section.

From inside the Tenant view, we can edit or delete the Tenant, as well as click into any of the Tenant’s users.
Tenant Users

To create a new user within the Tenant:

Click the **CREATE USER** button, then from the New User wizard input the fields below:

- First Name
- Last Name
- Username
- Email
- Role
- Password
- Confirm Password

Click **Save Changes**.

**Note:** Users are specific to each Tenant. Users created in the Master Tenant or other sub-Tenants will only have access to the Tenant they are created in.

Impersonate Tenant User

Morpheus allows admin users in the Master Tenant to impersonate any user in the Subtenants to see the application as if they are that user. To impersonate a user, you must be logged in as a user with the “Impersonate User” feature enabled in the assigned role.

From inside a Tenant detail page (containing the list of that Tenant’s users), and in the specific user’s ACTIONS drop down, select “Impersonate”.

This will log you in as that user in their respective Tenant. To log out of the impersonate users Tenant, select the username in the header, and then select “Quit Impersonating”
Resources

In the Master Tenant, resources can be configured with private or public visibility:

- **Private Visibility**: Only available to the assigned Tenant.
- **Public Visibility (option available in Master Tenant only)**: Available across all Tenants

Resources in the Master Tenant can also be assigned directly to Subtenants. When a resource is assigned to a Subtenant, it is only available for that Subtenant, and its visibility is automatically set to private. Public visibility is not an option for any resource assigned to or created in a Subtenant.

From the Master Tenant, the following resources can be configured for public visibility across all Tenants, or assigned to individual sub-Tenants

- Clouds
- Hosts
- Virtual Machines
- Networks
- Datastores
- Resource Pools
- Folders
- Virtual Images
- Library Instance Types
- Pricing
- Policies
- Workflows
- Roles

**Note:** Virtual Image Blueprints can be made available to multiple select Tenants when set to private.
Cloud Visibility & Assignment

To set the visibility of a Cloud to Public (shared across all Tenants) or Private (only available to the assigned Tenant):

1. Navigate to Infrastructure > Clouds
2. Select either the pencil/edit icon on the end of the cloud row, or click the name of the cloud and select “Edit” in the cloud page.
3. From the “Visibility” drop down, select either “Public” or “Private”
4. Select Save Changes in the footer of the Edit Cloud modal.

When a cloud is set to Public visibility, it is available to be added to Subtenants. All Subtenants created after a Master Tenant cloud is set to public will automatically have clouds with public visibility added, and a group will be created for each available cloud matching the cloud name in the new Subtenant(s).

For Tenants created prior to a Master Tenant cloud being set to public visibility, the Subtenant will have the option to add that cloud but it will not automatically be added.

While the cloud will be available for Subtenants, the resources available in that cloud to the Subtenant(s) depends on the visibility or assignment of the individual resources.

Note: A Subtenant user must have sufficient role permissions and cloud access to add publicly available clouds. Master Tenant clouds settings cannot be edited from Subtenants.
Assign a Cloud to an Tenant

**Important:** When assigning a Cloud to a Tenant, all resources for that Cloud will only be available to the assigned Tenant. If a cloud is created in the Master Tenant and assigned to a sub-Tenant, it will no longer be available for use by the Master Tenant or any other sub-Tenants, although it can be assigned back to the Master Tenant, or to another sub-Tenant.

It may be preferable for service providers to share or assign their cloud resources, such as specific hosts, networks, resources pools and datastores, across sub-Tenants, rather than an entire cloud.

To assign a cloud from the Master Tenant to a Sub-Tenant

1. Navigate to Infrastructure, Clouds
2. Select either the pencil/edit icon on the end of the cloud row, or click the name of the cloud and select “Edit” in the cloud page.
3. From the “Tenant” drop down, select the Tenant to assign the cloud to. The visibility will automatically be set to “Private” when a cloud is assigned to a sub-Tenant.
4. Select Save Changes in the footer of the Edit Cloud modal.

When a cloud is assigned to a sub-Tenant, or assigned to the Master Tenant with private visibility, that cloud and all of its resources are only available to the assigned Tenant. The Master Tenant still maintains control and visibility, and can edit the cloud settings or re-assign the cloud.
Individual Resource Visibility & Assignment

Similar to clouds, individual resources from the Master Tenant can be set to public and available to sub-Tenants, or assigned to sub-Tenants.

By default, any host, virtual machine, bare metal server, network, resource pool, datastore or blueprint added, created or inventoried by an Tenant is assigned to that Tenant. If these resources are in the Master Tenant, they can be assigned to sub Tenants. Assigning one of these resources will make it unavailable to the Master Tenant, but it will still be visible and editable by the Master Tenant. This allows Master Tenant resources to be isolated for use by sub-Tenants while still under the control of the Master Tenant.

Resources assigned to sub-Tenants from the Master Tenant will be visible and available for use by that sub-Tenant, however they cannot be edited or re-assigned by the sub-tenant.

Set the Visibility of a Host, Virtual Machine or Bare metal Server to Public or Private

1. From the Master Tenant, navigate to Infrastructure, Hosts
2. Select either the Hosts, Virtual Machines or Bare Metal tab
3. Click the name of the resource
4. Select Edit in the resource page to bring up the config modal
5. From the “Visibility” drop down, select either “Public” or “Private”
6. Select Save Changes

Assigning a Host, Virtual Machine, or Bare Metal server to an Tenant

1. From the Master Tenant, navigate to Infrastructure, Hosts
2. Select either the Hosts, Virtual Machines or Bare Metal tab
3. Click the name of the resource
4. From the “Actions” dropdown in the the resource page, select Assign Tenant
5. In the Assign Tenant modal, select the Tenant to assign the resource to.
6. Select **Execute** in the modal

The resource will now be assigned and available for use by the assigned Tenant. If assigned to a sub-Tenant, the Master Tenant will maintain visibility and control.

**Set the Visibility of a Network to Public or Private**

1. From the Master Tenant, navigate to Infrastructure, Network
2. Select either the pencil/edit icon in the network row, or click the name of the network and select “Edit” in the network page.
3. From the “Visibility” drop down, select either “Public” or “Private”
4. Select **Save Changes** in the modal
Assign a Network to an Tenant

1. From the Master Tenant, navigate to Infrastructure, Network
2. Select either the pencil/edit icon in the network row, or click the name of the network and select “Edit” in the network page.
3. From the “Tenant” drop down, select an Tenant to assign the network to.
4. Select Save Changes in the lower the modal
The Network will now be assigned and available for use by the assigned Tenant. If assigned to a sub-Tenant, the Master Tenant will maintain visibility and control.

Set the Visibility or assign a datastore to an Tenant

1. From the Master Tenant, navigate to Infrastructure, Storage
2. Select the “Data Stores” tab
3. Select Edit from the “Actions” dropdown in the datastores row
4. From the “Visibility” drop down, select either “Public” or “Private”
5. From the “Tenant” drop down, select the Tenant to assign the datastore to.

**Note:** If assigned to a sub-tenant, the visibility will be automatically set to private.

6. Select *Save Changes* in the modal
Set the Visibility or assign a Virtual Image to an Tenant

1. From the Master Tenant, navigate to Provisioning, Virtual Images
2. Select Edit from the “Actions” dropdown in the Virtual Images row
3. From the “Visibility” drop down, select either “Public” or “Private”. Public will share the
4. From the “Tenant” field, start typing the name of the Tenant to assign the Virtual Image to. Matching Tenants
   will populate, then select the Tenant to add.

   **Note:** Virtual Images can be set to Private, but accessible to more that one Tenant

#. Repeat step 4 for all Tenants requiring access to the virtual image. .. To remove access for an Tenant, click the “x”
next to the Tenant name#. Select *Save Changes* in the modal
The Virtual Image will now be available for use by the assigned Tenants.

9.2 Identity Sources

Administration > Tenants > (Selected Tenant) > Identity Sources Administration > Users > Identity Sources

9.2.1 Overview

Morpheus can integrate with many of the most common identity source technologies, such as Active Directory, Okta, and many others. These can be configured via the Identity Sources button on any Tenant detail page (Administration > Tenants > Selected Tenant) or on the Users list page (Administration > Users). These integrations map roles within these sign-on tools to equivalent roles in Morpheus so at first log in users are assigned the appropriate role.

9.2.2 Active Directory

Overview

Active Directory is Microsoft’s primary authentication service widely used in Enterprise organizations and even via Microsoft’s cloud services. While Active Directory also supports LDAP protocol support (which Morpheus can integrate with as well), the main Active Directory integration can also be utilized. It is even possible to map Active Directory groups to equivalent Roles within Morpheus. Morpheus will connect over port 389 for non-secure LDAP and port 636 for secure LDAP.
Adding an Active Directory Integration

1. Navigate to Administration > Tenants
2. Select a Tenant
3. Select IDENTITY SOURCES
4. Select + IDENTITY SOURCE
5. Choose “Active Directory”
6. Populate the following:
   - **Name**: Unique name for authentication type.
   - **AD Server**: Hostname or IP address of AD Server.
   - **Domain**: Domain name of AD Domain.
   - **Binding Username**: Service account username for bind user.
   - **Binding Password**: Password for bind service account.
   - **Required Group**: The AD group users must be in to have access (optional)
   - **Default Role**: The default role a user is assigned if no group is listed under AD user that maps under Role Mappings section.
   - **Service Account Holder**: This is the admin account type in Morpheus and an AD group can be created and populated to a user that this role should be assigned. Roles are assigned dynamically based on group membership.

**ENABLE ROLE MAPPING PERMISSION** When selected, Tenant users with appropriate rights to view and edit Roles will have the ability to set role mapping for the Identity Source integration. This allows the Tenant user to edit only the role mappings without viewing or potentially editing the Identity Source configuration.

**MANUAL ROLE ASSIGNMENT** When selected, administrators can manually edit Roles for users created through this identity source integration from the user detail page (Administration > Users > Selected user).

**Note:** For more on Identity Source role mapping permissions, see the associated guide in our KnowledgeBase.

1. Select SAVE CHANGES.

Now allowed AD users can login to Morpheus via their Active Directory credentials and a User will be automatically generated to Morpheus with matching metadata and mapped Role permissions.

**Note:** Only the username is required with password, not the username@domain.

**Note:** Sub-tenant Morpheus API authentication for Active Directory generated users is not currently supported.
9.2.3 Azure Active Directory SSO (SAML)

Azure Active Directory Single Sign-on can be added as a Identity Source in Morpheus using the SAML Identity Source Type. The Azure AD SSO configuration is slightly different than other SAML providers, and this guide will assist in adding a Azure AD SSO Identity Source.

Create a Azure AD SAML Integration

Azure requires inputting the **Identifier (Entity ID)** and **Reply URL (Assertion Consumer Service URL)** in the Azure SSO configuration before it provides the Endpoints and Certificate necessary to add the Integration into Morpheus. In order to get the **Identifier (Entity ID)** and **Reply URL (Assertion Consumer Service URL)** to input into Azure SSO config, we need to create a base SAML Integration in Morpheus first.

To add a base SAML integration:

1. Navigate to Administration > Tenants
2. Select a tenant.
3. Select IDENTITY SOURCES in the Tenant detail page
4. Select + ADD IDENTITY SOURCE.
5. Select SAML SSO from the TYPE field
6. Add a Name, optional Description and any value in the LOGIN REDIRECT URL field. Since we do not have the LOGIN REDIRECT URL from Azure yet, type any text such as test into the LOGIN REDIRECT URL field so the Identity Source Integration can be saved and the **Identifier (Entity ID)** and **Reply URL (Assertion Consumer Service URL)** generated. We will edit the Integration with the proper LOGIN REDIRECT URL after configuring SSO in Azure.
7. Select SAVE CHANGES.

Upon save, the **Entity ID** (Identifier (Entity ID)) and **SP ACS URL** (Reply URL (Assertion Consumer Service URL)) will be provide in the Identity Source list view. Copy these for use in Azure SSO config.

Configure Azure SSO

This guide assumes an Azure AD Application has already been created in Azure with a subscription level high enough to configure SSO in the application. Please refer to Azure documentation if this has not already been configured.

1. Next, in the Azure Active Directory Application details page, select Single sign-on, then enter the following:
   - **Single Sign-on Mode dropdown** Select SAML-based Sign-on
   - **Identifier (Entity ID)** Enter the Entity ID URL from the Morpheus Identity Source Integration above.
   - **Reply URL (Assertion Consumer Service URL)** Enter the SP ACS URL from the Morpheus Identity Source Integration above.
2. Save and click the Test SAML Settings button. Azure will confirm connection with Morpheus
3. In Azure’s User Attributes & Claims settings (step 2), select Add a group claim with value user. groups [SecurityGroup] User Attributes & Claims config
### Morpheus Documentation

<table>
<thead>
<tr>
<th>Claim name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unique User Identifier (Name ID)</td>
<td>user.userprincipalname [nameid-format:emailAddress]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Claim name and Namespace URL</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://schemas.microsoft.com/ws/2008/06/identity/claims/groups">http://schemas.microsoft.com/ws/2008/06/identity/claims/groups</a></td>
<td>user.groups [SecurityGroup]</td>
</tr>
<tr>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress</a></td>
<td>user.mail</td>
</tr>
<tr>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname</a></td>
<td>user.givenname</td>
</tr>
<tr>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name</a></td>
<td>user.userprincipalname</td>
</tr>
<tr>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname</a></td>
<td>user.surname</td>
</tr>
</tbody>
</table>

4. Copy or keep available for reference the Claim Names/Namespace URLs for entering Role Attribute Values in the Morpheus Identity Source Integration.

5. In Azure SSO config, if one has not been generated, select **Create new certificate** to generate a new SAML Signing Certificate.

6. Enter a valid email address to receive certificate expiration notifications (these are not Morpheus-generated email).

7. In Azure SSO config, select `Configure {AD App Name}`

8. In the **Configure sign-on** pane, copy the following:
   - **SAML Single Sign-On Service URL** This will be used for the LOGIN REDIRECT URL in the Morpheus Identity Source Integration settings
   - **Sign-Out URL** This will be used for the LOGOUT REDIRECT URL in the Morpheus Identity Source Integration settings
   - **Click on the SAML XML Metadata link, open the xml file, and copy the key between the `<X509Certificate>` and `</X509Certificate>` elements.** This will be used for the Public Key value in the SAML RESPONSE section of the Morpheus Identity Source Integration settings

   ```xml
   MIICCAIBAwIBAgIQQgA9d2jIwMAYDVQQDEy...t56a+2wIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQCSjf2IOG6O3wdOmkfJ/...
   ```

9. Save the SSO config in Azure AD app and return to Morpheus.

484 Chapter 9. Administration
Edit the existing Azure AD SAML Integration

Now that we have the required information, we can finalize the Azure AD SAML Integration in Morpheus

1. Edit the existing Azure AD SAML Integration created in the first step and populate the following:

   - **LOGIN REDIRECT URL** Add the SAML Single Sign-On Service URL copied from Azure SSO config.
   - **LOGOUT REDIRECT URL** Add the Sign-Out URL copied from Azure SSO config.
   - **SAML RESPONSE** Set to “Validate Assertion Signature”, then in the “Public Key” field enter the Public Key value we discussed in the last section
   - **GIVEN NAME ATTRIBUTE NAME** (May have to click “show” to see hidden SAML Assertion Attribute Names fields) Enter the `givenname` Namespace url from Azure SSO config: `http://schemas.xmlsoap.org/ws/2005/05/identity/claims`
   - **SURNAME ATTRIBUTE NAME** Enter the `emailaddress` Namespace url from Azure SSO config: `http://schemas.xmlsoap.org/ws/2005/05/identity/claims`
   - **EMAIL ATTRIBUTE NAME** (May need to scroll down within the SAML Assertion Attribute Names section see this field) Enter the `surname` Namespace url from Azure SSO config: `http://schemas.xmlsoap.org/ws/2005/05/identity/claims`

Configure Role Mappings

Role mappings will map Azure AD Groups to Morpheus Roles. Azure AD users will be assigned Roles in Morpheus upon signing in based on their Group Membership in Azure AD.

**Important:** Use an Azure Groups Object ID, not Group name, when entering Role Mappings. Example: 7626a4a2-b388-4d9b-a228-72ce9a33bd4b

- **DEFAULT ROLE** Role a Azure AD user will be assigned by default upon signing in to Morpheus using this Identity Source.

- **REQUIRED AZURE AD GROUP OBJECT ID** Object ID of Azure AD Group a user must be a member of to be authorized to sign in to Morpheus. Users not belonging to this Group will not be authorized to login to Morpheus. This field is optional, and if left blank, any user from the Azure AD App will be able to sign in to Morpheus and will be assigned the Default Role if no Role Mappings match AD Group membership.

- **GROUP ASSERTION ATTRIBUTE NAME** Enter `http://schemas.microsoft.com/ws/2008/06/identity/claims/groups` for Azure AD SSO

**Additional Role Mappings** The existing Roles in Morpheus will be listed. To map a Morpheus Role to an Azure AD Group, enter the Object ID of the desired Azure AD Group in the `Role Attribute Value` field for the corresponding Morpheus Role.

**Important:** Use an Azure Groups Object ID, not Group name, when entering Role Mappings. Example: 7626a4a2-b388-4d9b-a228-72ce9a33bd4b

**ENABLE ROLE MAPPING PERMISSION** When selected, Tenant users with appropriate rights to view and edit Roles will have the ability to set role mapping for the Identity Source integration. This allows the Tenant user to edit only the role mappings without viewing or potentially editing the Identity Source configuration.

**MANUAL ROLE ASSIGNMENT** When selected, administrators can manually edit Roles for users created through this identity source integration from the user detail page (Administration > Users > Selected user).
Note: For more on Identity Source role mapping permissions, see the associated guide in our KnowledgeBase.

Once populated, select SAVE CHANGES and the SAML identity source integration will be added. The Identity Source can be edited anytime to deactivate or change Role Mappings or other values.

Note: If Role mappings are edited after Azure AD SSO users have signed into Morpheus, currently logged in users will need to log out of Morpheus for the new Role mappings to take effect, when applicable.

Azure Group Lookups

When a user in azure ad has more that 150 group attributes, Azure does not include the group claims in the SAML response, and Morpheus is required to query Microsoft Graph to obtain the users group attribute values. When there are users that are members of more that 150 groups, populate the Azure Group Lookups section in order for those users to be able to use the Azure AD SAML SSO integration, otherwise no groups will be obtained and proper role mappings cannot occur.

AZURE TENANT ID Add Azure AD Tenant ID if user group membership will exceed 150. See Copy Directory (tenant) and Application (client) IDs for information on obtaining an Azure AD Tenant ID

AZURE APP ID Add Azure AD Application (Client) ID if user group membership will exceed 150. See Copy Directory (tenant) and Application (client) IDs for information on obtaining an Azure AD Application (Client) ID

AZURE APP SECRET Add Azure Application (Client) Secret if user group membership will exceed 150. See Generate a Client Secret for information on creating an Azure Application (Client) Secret

ROLE LINK ATTRIBUTE NAME default: http://schemas.microsoft.com/claims/groups.link. This is not normally changed.

Signing In to Morpheus

When there is an active SAML/Azure AD SSO Identity Source Integration, a new button will appear on the Morpheus login page with the name of the Identity Source Integration as the button title. Example: MORPHEUS SSO. Another button titled “USERNAME AND PASSWORD” is also added for Morpheus account authentication outside of an Identity Source.

• SAML/Azure AD SSO users can log into Morpheus by clicking the SAML button This will redirect the User to Azure AD app sign in url. If they are currently signed into Azure and authorized, the user will be instantly signed into Morpheus.
• Local Morpheus users can select “USERNAME AND PASSWORD” to sign in with their local credentials as before.

**Note:** If no local users other than the System Admin have been created, “USERNAME AND PASSWORD” option will not be displayed, only the SAML option.

### 9.2.4 Okta

**Overview**

Morpheus allows users to integrate an Okta deployment for user management and authentication. In Morpheus, identity sources are added on a per-Tenant basis and Morpheus allows you to map Okta user groups to Morpheus user groups. User accounts are automatically created with matching metadata and role permissions when users are authenticated.

**Adding an Okta Integration**

1. Navigate to Administration > Tenants
2. Select a Tenant
3. Select **IDENTITY SOURCES**
4. Select **+ IDENTITY SOURCE**
5. Choose **TYPE:** “Okta”
6. Populate the following, then select **SAVE CHANGES:**
   - **Name** Unique name for authentication type
   - **Description** A description for your new Okta Identity Source
   - **Okta URL** Your Okta URL
   - **Administrator API Token** Your Okta Administrator API Token
   - **Required Group** The Okta group that users must be in to have access (optional)
   - **Default Role** The default role a user is assigned if no group is listed under an Okta user that maps within the Morpheus Role Mappings section
   - **ENABLE ROLE MAPPING PERMISSION** When selected, Tenant users with appropriate rights to view and edit Roles will have the ability to set role mapping for the Identity Source integration. This allows the Tenant user to edit only the role mappings without viewing or potentially editing the Identity Source configuration.
   - **MANUAL ROLE ASSIGNMENT** When selected, administrators can manually edit Roles for users created through this identity source integration from the user detail page (Administration > Users > Selected user).

**Note:** For more on Identity Source role mapping permissions, see the associated guide in our KnowledgeBase.

Now, allowed Okta users can log into Morpheus via their Okta credentials and a user will be automatically generated within Morpheus with matching metadata and mapped Role permissions.
Note: If you’ve created multi-tenant roles, these will also appear here and can be mapped to Okta user groups allowing you to map users to equivalent user groups in Morpheus.

9.2.5 OneLogin

Adding OneLogin Identity Source Integration

1. Navigate to Administration > Tenants
2. Select the Tenant to add the Identity Source Integration
3. Select IDENTITY SOURCES
4. Select + IDENTITY SOURCE
5. Enter the following:
   - **TYPE** OneLogin
   - **NAME** Name of the Identity Source Integration in Morpheus
   - **DESCRIPTION** Optional Description of the Identity Source
   - **ONELOGIN SUBDOMAIN** example: morpheus-dev

   Warning: Please verify the subdomain carefully. An invalid subdomain will cause authentication attempts by OneLogin users to fail.

   **ONELOGIN REGION** Specify US or EU region
   **API CLIENT SECRET** OneLogin API Client Secret from the Settings - API section in OneLogin portal
   **API CLIENT ID** OneLogin API Client ID from the Settings - API section in OneLogin portal
   **REQUIRED ROLE** Enter a role if OneLogin users logging into morpheus must have at least this OneLogin role to gain access to Morpheus.
   **DEFAULT ROLE** The default Morpheus Role applied to users created from OneLogin Integration if no other role mapping is specified below
   **ROLE MAPPINGS** Existing Morpheus Roles will be listed with fields to enter OneLogin Roles to map to. Users with OneLogin roles matching the role mappings will be assigned the appropriate Role(s) in Morpheus when signing in.
   **ENABLE ROLE MAPPING PERMISSION** When selected, Tenant users with appropriate rights to view and edit Roles will have the ability to set role mapping for the Identity Source integration. This allows the Tenant user to edit only the role mappings without viewing or potentially editing the Identity Source configuration.
   **MANUAL ROLE ASSIGNMENT** When selected, administrators can manually edit Roles for users created through this identity source integration from the user detail page (Administration > Users > Selected user).

Note: For more on Identity Source role mapping permissions, see the associated guide in our KnowledgeBase.
1. Select *SAVE CHANGES* and the OneLogin Integration will be added.

Users can now login to Morpheus with OneLogin credentials. The first Login will create a user in Morpheus matching the Username, email and Password from OneLogin. If a **REQUIRED ROLE** is specified in the Identity Source settings, only users with that Role in OneLogin will be able to login to Morpheus.

**Important:** OneLogin users will not authenticate in Morpheus if there is an existing Morpheus User with matching username or email address.

### 9.2.6 SAML Integration

**Overview**

The Morpheus SAML identity source integration allows customers to add user SSO to Morpheus, authenticated by external login SAML providers.

Adding a SAML Integration

To add a SAML integration:

1. Navigate to Administration > Tenants
2. Select a tenant.
3. Select IDENTITY SOURCES in the Tenant detail page
4. Select *ADD IDENTITY SOURCE*.
5. Select SAML (external login) from the TYPE field
6. Add a Name and optional Description for the SAML integration

There are 3 sections with fields that need to be populated depending on the desired configuration:

- SAML Configuration
- Role Mappings
- User Attribute Names

**SAML Configuration**

**LOGIN REDIRECT URL**  This is the SAML endpoint Morpheus will redirect to when a user signs into Morpheus via SAML.

**LOGOUT POST URL**  The url morpheus will post to when a SAML user log out of Morpheus to log out of the SAML provider as well.

**SIGNING PUBLIC KEY**  Add the X.509 Certificate public key from the SAML provider.
Role Mappings

**DEFAULT ROLE**  Role a saml user will be assigned by default when no role is mapped

**ROLE ATTRIBUTE NAME**  The name of the attribute filed that will map to morpheus roles, such a MemberOf

**REQUIRED ROLE ATTRIBUTE VALUE**  Role attribute value that a user must be assigned/a member of to be authorized, such as group or role in the SAML SP.

**ENABLE ROLE MAPPING PERMISSION**  When selected, Tenant users with appropriate rights to view and edit Roles will have the ability to set role mapping for the Identity Source integration. This allows the Tenant user to edit only the role mappings without viewing or potentially editing the Identity Source configuration.

**MANUAL ROLE ASSIGNMENT**  When selected, administrators can manually edit Roles for users created through this identity source integration from the user detail page (Administration > Users > Selected user).

**Note:** For more on Identity Source role mapping permissions, see the associated guide in our KnowledgeBase.

The rest of the Role Mapping Fields will be the existing Roles in morpheus with a Role Attribute Value field.

User Attribute Names

**GIVEN NAME ATTRIBUTE NAME**  SAML SP field value to map to Morpheus user First Name

**SURNAME ATTRIBUTE NAME**  SAML SP field value to map to Morpheus user Last Name

**EMAIL ATTRIBUTE NAME**  SAML SP field value to map to Morpheus user email address
EDIT IDENTITY SOURCE

Identity Source

**TYPE**  SAML [Beta]

**ACTIVE**  Yes

**NAME**  SAML

**DESCRIPTION**  onelogin SAML

SAML Configuration

**LOGIN REDIRECT URL**  
https://morpheusdata-dev.onelogin.com/trust/saml2/http-

- [ ] Do not include SAMLRequest parameter

**LOGOUT POST URL**  
https://morpheusdata-dev.onelogin.com/trust/saml2/http-

**SIGNING PUBLIC KEY**  
MIIEFzCCAvqgAwIBAgIuQayYdMuOBTGcaIoARanhrJwttQwDVYJKwZIzjzIhvzNAQEF

Role Mappings

**DEFAULT ROLE**  System Admin

**ROLE ATTRIBUTE NAME**  MemberOf

**REQUIRED ROLE ATTRIBUTE VALUE**  dev

**LEGACY ACCOUNT ADMIN**  Role Attribute Value

User Attribute Names

**GIVEN NAME ATTRIBUTE NAME**  firstName

**SURNAME ATTRIBUTE NAME**  lastName

**EMAIL ATTRIBUTE NAME**  

[DEACTIVATE]  [DELETE]  [SAVE CHANGES]
Once populated, select SAVE CHANGES and the SAML identity source integration will be added.

In the Identity Sources section, important information for configuration of the SAML integration is provided. Use the SP ENTITY ID and SP ACS URL for configuration on the external login SAML provider side.

- **SP ENTITY ID**
- **SP ACS URL**
- **IDP LOGIN REDIRECT URL**
- **IDP LOGOUT POST URL**
- **SP METADATA**

Sample Metadata code output:

```xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<EntityDescriptor entityID="https://someip.com/saml/CDWPjmZt" xmlns="urn:oasis:names:tc:SAML:2.0:metadata">
  <SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</NameIDFormat>
    <AssertionConsumerService index="0" isDefault="true" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://someip.com/externalLogin/callback/CDWPjmZt"/></SPSSODescriptor>
</EntityDescriptor>
```

**Note:** Different SAML providers will have different field names and requirements. A onelogin SAML Test Connector (IdP w/attr) was used for the example integration this article.

**Onelogin SAML SSO**

For Onelogin SAML integration, the following fields are mapped:

- **LOGIN REDIRECT URL** : SAML 2.0 Endpoint (HTTP)
- **LOGOUT POST URL** : SLO Endpoint (HTTP)
- **SIGNING PUBLIC KEY** : X.509 Certificate
- **SP ENTITY ID** : ACS (Consumer) URL Validator
- **SP ACS URL** : ACS (Consumer) URL
### 9.3 Plans & Pricing

#### 9.3.1 Overview

Plans & Pricing is where Plans, Prices Sets and Prices are managed. Prices are added to Prices Sets, and Price Sets are added to Plans. Plans include Service Plans, Load Balancer Price Plans, Virtual Image Prices Plans and Snapshot Price Plans. Price sets can be agnostic and available for any Plan, or specific to a Region Code, Cloud or a specific Resource Pool. Prices are configured per Price Type and can be added to Price Set configurations that support the Price Type. Master Tenant Prices can apply to all Tenants or be assigned to a single Tenant.

A set of Service Plans are seeded by Morpheus for private cloud provision types as well as some public clouds. Additional Plans and Prices are synced in for other public clouds when the corresponding cloud types are added to an appliance. Users can create new Service Plans or edit the system seeded Service Plans for Private Cloud types. Service Plans configurations cannot be created or edited for Public Cloud provision types.

#### 9.3.2 Plans

Plans types include Service Plans and Price Plans. Service Plans determine the memory, storage and cores configuration during provisioning and reconfigure.

**Service Plans**

A set of Service Plans are seeded by Morpheus for private cloud provision types as well as some public clouds. Additional Plans and Prices are synced in for other public clouds when the corresponding cloud types are added to an appliance. Users can create new Service Plans or edit the system seeded Service Plans for Private Cloud types. Service Plans configurations cannot be created or edited for Public Cloud provision types.

**Service Plan Configuration**

- **NAME** The name of the Service Plan in Morpheus
- **ACTIVE** Inactive Service Plans are not available for selection during provisioning or reconfigure, and new discovered records will not be associated with deactivated Plans. Resources attached to active Plans will continue to be associated if the Plan is deactivated
- **CODE** A unique identifier for use in Morpheus API and CLI
- **DISPLAY ORDER** Configures the order in which plans are displayed relative to other plans associated with the same provision type
- **PROVISION TYPE** Determines the resource Provision Type the Service Plan is available for when provisioning, reconfigures and discovery association.
- **REGION CODE** (optional) Limits availability of the Service Plan to Clouds with the specified Region Code
- **STORAGE** The default value of the Root volume (in MB or GB)
  - **CUSTOMIZE ROOT VOLUME** Allows the Root Volume size value to be customized during provisioning or reconfigure. Custom Range limits apply.
  - **CUSTOMIZE EXTRA VOLUMES** Allows the size of additional Volumes to be customized during provisioning or reconfigure. Custom Range limits apply.
  - **ADD VOLUMES** Allows additional volumes to be added during provisioning or reconfigure.
MEMORY  The amount of memory included with the plan (in MB or GB), when the CUSTOM MEMORY box is marked users can select a memory amount within the custom range configured below. CUSTOM MEMORY: Allows the Memory value to be customized during provisioning or reconfigure. Custom Range limits apply.

CORE COUNT  The number of virtual CPU cores associated with the plan, when the CUSTOM CORES box is marked users can select a number of cores within the custom range configured below. CUSTOM CORES: Allows the CORE COUNT value to be customized during provisioning or reconfigure. Custom Range limits apply.

CORES PER SOCKET  Determines core distribution across sockets. CORES PER SOCKET cannot be larger than CORE COUNT, and CORE COUNT must be divisible by CORES PER SOCKET. For example 4 CORES with 2 CORES PER SOCKET means 2 sockets would have 2 cores each assigned. 4 CORES with 1 CORE PER SOCKET would have 4 sockets with 1 core each assigned, and 4 CORES with 4 CORES PER SOCKET would have 1 socket with 4 cores assigned.

CUSTOM RANGES

- STORAGE  Min and Max allowed values allowed when CUSTOMIZE ROOT VOLUME or CUSTOMIZE EXTRA VOLUMES is enabled. Units inherited from the Plans STORAGE: GB/MB setting.
- MEMORY  Min and Max allowed values allowed when CUSTOM MEMORY is enabled. Units inherited from the Plans MEMORY GB/MB setting.
- CORES  Min and Max allowed values allowed when CUSTOM CORES is enabled.

PRICE SETS  In the Price Sets tab, associate Price Sets with the Plan. See Add Price Set(s) to Plan

Tip: Custom Range storage and memory values units (GB/MB) are inherited from the :STORAGE:: and :MEMORY:: GB/MB settings in the same Plan. For example, if :STORAGE: is configured for for 40 GB, a custom range for Storage would also be in GB.

Create Service Plan

Morpheus offers a few distinct types of service plans, each with different data fields to track and valid price types which can be associated. Price Sets can be added to the plan at the time it’s created so often it makes sense to create the Prices and associate them with Price Sets before creating the plan. Additional instructions for creating Prices and Price Sets are in the next section. With the Price Sets ready, continue with the instructions below to create Price Plans of various types.

1. Navigate to |AdmPla| (/admin/service-plans)
2. Click the + ADD dropdown and select a Price Plan type
3. Configure details on the Service Plan on the General tab, the data tracked will depend on the Plan type selected.
4. On the Price Sets tab, associate all relevant Price Sets with the Plan. See Service Plan Configuration
5. Click SAVE CHANGES
Add Price Set(s) to Plan

1. Select a Price Unit to list available Price Sets within that Price Unit. Available Price Sets are filtered to show only those which are relevant for the Plan type you’ve selected
2. Select a Price Set from the list and click + ADD
3. Add additional Price Sets if desired (multiple Price Sets can be associated with a Plan)
4. Added Price sets can be remove from a Plan by clicking the icon
5. Once all Price Sets have been added, select SAVE CHANGES

Tip: +ADD must be selected after selecting a Price Set or it will not be added to a Plan

Service Plan Permissions

Group and Tenant Access permissions determine availability of a Service Plan.

- Group Access determines what Groups the Service Plan will be available in for Provisioning and Reconfigure.
- Group Access settings only apply to the Tenant they are configured in, as Groups are not multi-tenant.
- For multi-tenant environments, the Master Tenant can set Tenant Permissions to determine if the Service Plan is available to all Tenants (public visibility) or assign the Service Plan to one or multiple Tenants.

Removing Plans

Plans can be removed by selecting ACTIONS: on a Plan and then selecting :Remove: from the Actions menu. Removing a Plan makes it no longer visible, however it does not hard delete the Plan as the record must remain for existing associations usage and price tracking. Synced Plans should be deactivated rather than removed.

Load Balancer Price Plans


Load Balancer Price Plan Configuration:

- **NAME** The name of the Load Balancer Price Plan in Morpheus
- **ACTIVE** When Active, Prices in Price Sets added to the Price Plan will apply to associated resources per Price and Price Set configuration.
- **CODE** A unique identifier for use in Morpheus API and CLI
- **LOAD BALANCER TYPE** Select from the available Load Balancer Types to associate the Price Plan with
- **PRICE SETS** In the Price Sets tab, associate Price Sets with the Plan. See Add Price Set(s) to Plan
Virtual Image Price Plans

Virtual Image Price Plans configure pricing for Virtual Images. Pricing is associated per Price and Price Set configurations, but in general applies to Images with location records in the Price Plans specified :CLOUD TYPE:. Virtual Image Prices Plans are for setting pricing for Virtual Image storage, not for adding pricing to resources that use Virtual Images associated with Virtual Image Price Plans. Virtual Image Price Plans do not apply to uploaded Virtual Images that have not been copied to a location in the specified :CLOUD TYPE: yet.

Virtual Image Price Plan Configuration:

- **NAME** The name of the Virtual Image Price Plan in Morpheus
- **ACTIVE** When Active, Prices in Price Sets added to the Price Plan will apply to associated resources per Price and Price Set configuration.
- **CODE:** A unique identifier for use in Morpheus API and CLI
- **CLOUD TYPE** Virtual Image Pricing applies to Virtual Images with location records in the specified :CLOUD TYPE:
- **PRICE SETS** In the Price Sets tab, associate Price Sets with the Plan. See Add Price Set(s) to Plan

Snapshot Price Plans

Snapshot Price Plan Configuration:

- **NAME** The name of the Snapshot Price Plan in Morpheus
- **ACTIVE** When Active, Prices in Price Sets added to the Price Plan will apply to associated resources per Price and Price Set configuration.
- **CODE:** A unique identifier for use in Morpheus API and CLI
- **CLOUD TYPE** Snapshot Pricing applies to Snapshots that exist in the specified :CLOUD TYPE:
- **PRICE SETS** In the Price Sets tab, associate Price Sets with the Plan. See Add Price Set(s) to Plan

9.3.3 Price Sets

Price Sets combine Prices and then attach to Plans. Prices must be created prior to creating Price Sets, but it is recommended to review the Price Set Type options prior to creating Prices.

- **Price Unit** Select the Price Unit to use for the Price Set.
  - Minute
  - Hour
  - Day
  - Month
  - Year
  - Two Year
  - Three Year
  - Four Year
  - Five Year
Note: Only Prices configured with matching Price Units can be used in a Price Set. “Month” is equivalent to 30 days by default. For AWS, month is 30.5 days. For Azure, month is 30.4 days.

Type Price Set types determine which Prices are available to make up the set. This selection will filter the values returned in the Prices field at the bottom of the modal.

Note: It’s helpful to make note of the Prices options below before creating Price Sets.

• **Everything**: ‘Everything’ price sets require one or more ‘Everything’ price types and may include ‘Platform’ or ‘Software’ price types
• **Compute + Storage**: ‘Compute + Storage’ price sets require at least one of each ‘Memory’, CPU’, and ‘Disk Only’ price types and may include ‘Platform’ or ‘Software’ price types
• **Component**: ‘Component’ price sets require at least one of each ‘Memory’, ‘Cores’, ‘CPU’, and ‘Storage’ price types and may include ‘Platform’ or ‘Software’ price types
• **Load Balancer**: ‘Load Balancer’ price sets require at least one ‘Load Balancer’ price type and may include ‘Load Balancer Virtual Server’ price types. Load Balancer price sets are the only type which can be associated with Load Balancer Price Plans
• **Virtual Image**: ‘Virtual Image’ price sets require at least one ‘Storage’ price type. Virtual Image price sets are the only type which can be associated with Virtual Image Price plans
• **Snapshot**: ‘Snapshot’ price sets require at least one ‘Storage’ price type and may only include ‘Storage’ price types. Snapshot price sets are the only type which can be associated with Snapshot Price plans

**Apply Price Changes to Usage** If marked, when saving a Price Set (new Price Set or saving changes to an existing one), usage records will be restarted for servers affected by the pricing change.

**Prices** Search for and select Prices to be added to the Price Set. One of each Price Type required for the Price Set Type selected must be added for the Price Set to save.

### 9.3.4 Prices

**Price Types**

• Everything: One price for all resources Storage, CPU, Memory, and Disks
• Memory + CPU
• Memory Only (per MB)
• Cores Only (per core)
• Disk Only (per GB)
• Platform
• Software
• Datastore (per GB)
• Load Balancer
• Load Balancer Virtual Server

**Price Units**

• Minute
• Hour
• Day
• Month
• Year
• Two Year
• Three Year
• Four Year
• Five Year

Currency
• AUD
• BRL
• CAD
• CHF
• CLF
• CLP
• DKK
• EUR
• GBP
• IDR
• ILS
• MAD
• MXN
• NOK
• NZD
• ROL
• SEK
• TRL
• USD
• USN
• XAF
• XCD
• XOF
• XPF
• ZAR (South African Rand)

Cost  The base cost of the resource(s). The Price will match the Cost unless a Price Adjustment is added.

Price Adjustment
• **None**: Default, no markup added and Price will match Cost
• **Fixed Markup**: A fixed amount added to the Cost. Price will equal Cost + Markup.
• **Percentage Markup**: Adds a percentage markup to Cost. Price equals Cost + \((\text{Cost} \times \text{Markup \%})\)
• **Custom Price**: Sets a Price independent from the Cost. If the Cost changes, a Custom Price will not.

**Price** A computed value of the final price including the cost plus any applicable markup.

**Apply Price Changes to Usage** If marked, when saving a Price Set (new Price Set or saving changes to an existing one), usage records will be restarted for servers affected by the pricing change.

### 9.4 Roles

#### 9.4.1 Overview

Within Morpheus is a wide array of role based access control capabilities. These roles can be managed within the Admin > Roles section of the Morpheus UI as well as through the API or CLI. They are designed to be robust enough to fit within a wide array of enterprise and managed service provider scenarios so they can be a bit hard to grasp at first, but should make sense once a few simple concepts are explained. There are two types of roles within Morpheus called Tenant and User based roles. Both sets of roles allow restrictions to be imposed on a user at the feature access level. Entire sections within the appliance UI can be hidden based on the specified access levels for features within Morpheus. Features have different access scopes that can be selected from and can range depending on the specific feature. The most common scope set involves none, read, and full. Instance Type access is also common among both role types which allow the administrator to restrict which service catalog items they are allowed to provision within Morpheus.

There are several handy tricks for creating new roles within Morpheus and users can be assigned more than one role. When a user is assigned more than one role, permissions are granted by the role with the highest level of scope access. This allows roles to be built with small subsets of features and combined to grant different individuals relevant permission control.

**Note**: Feature access control not only applies to the Morpheus UI but also applies to the public developer API. It is sometimes necessary to logout and back in for changes to a user's feature access level to be respected.

#### 9.4.2 Role Types

**Tenant Roles**

A Tenant based role (formerly called an Account based role) is used to ensure access control enforcement across an entire tenant with many sub-users. This allows the subtenant to manage their own set of internal user based roles without worrying master tenant involvement in setting them up. The master tenant is the only tenant able to create and manage these types of roles. When editing a Tenant, a singular tenant role can be assigned to the account. Users within the tenant can be assigned roles but those user based roles will never be able to supersede the level of access granted by the tenant role. This allows a super administrator the ability to restrict access at the department or organization level without having to worry about per user access control within said tenant.

Tenant roles also have an additional section not in User based roles related to Cloud Access. Cloud Access allows the master tenant the ability to assign cloud integration resources to specific subtenants or groups of subtenants. An example would be granting access to a specific VMware cluster only to a subset of tenants using the tenant based role control.
User Roles

User roles can be created by any tenant given permission at the tenant role level. These allow tenants to manage their own sets of users and their levels of access. They also allow tenants to control which users have access to specific “Groups” for provisioning into within Morpheus. Groups are not cross tenant and therefore need to be controlled within the individual tenant in Morpheus.

Master tenants are able to create a special type of user role called a multi-tenant user role. A multi-tenant user role is copied / duplicated down to all subtenants within Morpheus. These can be viewed as pre-canned role templates available to new tenants when their account is first created. Any changes made to the main role are propagated down to the subtenants version of the shared role so long as the subtenant has not previously adjusted/changed that role. The moment a subtenant makes adjustments to the shared role within their account, it is unlinked from the parent role and treated entirely independently.

Another note about user roles is that when a user role is copied down to a subtenant, the permission scopes cannot supersede the tenants assigned tenant role. If they do they are automatically downgraded when propagated to the specific tenant. Any changes made to the tenant role will automatically ensure roles within the tenant are downgraded appropriately.

Multi-Tenant User Role Lock

As discussed above, multi-tenanted user roles are made available within all subtenants as ‘canned’ user role sets. Master tenant administrators can prevent changes to these ‘canned’ user roles by marking the box labeled ‘MULTIENTANT LOCKED’ when creating or editing the role. In addition to preventing subtenant administrators from modifying permissions of these roles within their subtenancy, this option also ensures master tenant administrators can propagate new changes to that role. Modification of the role by the subtenant (if allowed) breaks the link back to the master tenant and the copy of the role within the subtenant will become its own unlinked role.

Note: Multi-tenant role lock applies only to permission sets on the ‘FEATURE ACCESS’ tab. Permissions in the ‘GROUP ACCESS’, ‘INSTANCE TYPE ACCESS’, and ‘BLUEPRINT ACCESS’ tabs are not locked. Similarly, changes made to the role on these tabs in the master tenant are not synced down.

9.4.3 Roles and Identity Sources

It is very common for large Enterprises to have an existing identity source that they would like to plug in to Morpheus for authentication. This includes services like LDAP, Active Directory, OKTA, Jump Cloud, One Login, and SAML. When using these services it becomes important to configure a role mapping between the Morpheus role assignments to the equivalent identity source groups/roles the user belongs to. This is configurable within the identity source management UI. Sections are provided allowing things like LDAP groups to be directly mapped to specific roles within Morpheus. If a user matches more than one LDAP/role group then both sets of roles are applied to the user automatically. Configuring Identity Sources is done in Tenant management or user management in Administration > Tenants or Administration > Users, and has to be configured on a per-tenant basis. Additionally, administrators may opt to lock users to their mapped role in Morpheus or keep the roles unlocked to manually administer roles in one-off scenarios.
9.4.4 Role Permissions

Note: Permission options for sub-tenant user roles will only list options permitted by the Tenant role applied to the sub-tenant. Sub-Tenant user roles permissions cannot exceed permissions set by the overriding Tenant Role.

User Role Permission Sections

Features Controls User access level for UI sections and features in Morpheus. The complete feature permissions grid is included below.

Groups Controls User access level for Groups. Groups are not a Multi-Tenant construct, only Groups created in the current Tenant will be visible.

Instance Types Controls User access level for Instance Types. Only Instance Types created in the current Tenant or those created in the Master Tenant and shared with the current Tenant will be available.

Blueprints Controls User access level for Blueprints during App provisioning. Only Blueprints created in the current Tenant or those created in the Master Tenant and shared with the current Tenant will be available.

Report Types Controls User access for each report type in the Reports section (Operations > Reports). The user must also have Operations: Reports access granted under the Feature permissions tab.

Personas Controls User access to Morpheus Personas, at the time of this writing Users may be given access to the Standard (full Morpheus experience) or Service Catalog Personas

Catalog Item Types Controls User access to Catalog Item types within the Service Catalog Persona. Only Catalog Items created in the current Tenant or those created in the Master Tenant and shared with the current Tenant will be available.

VDI Pools Controls User access to VDI Pools which are currently configured (Tools > VDI Pools) via the Virtual Desktops Persona view

Tenant Role Permission Sections

Features Controls Tenant access level for sections and features in Morpheus. The complete feature permissions grid is included below.

Clouds Controls Tenant access level for Clouds. This list includes Clouds integrated from the Master Tenant and shared publicly. Tenants given this Tenant Role will have either Full, Read, or None access levels to a given Cloud. See the section below for more information on Cloud Access levels.

Instance Types Controls Tenant access level for Instance Types. Only Instance Types created in the current Tenant or those created in the Master Tenant and shared with the current Tenant will be available.

Blueprints Controls Tenant access level for Blueprints during App provisioning. Only Blueprints created in the current Tenant or those created in the Master Tenant and shared with the current Tenant will be available.

Report Types Controls Tenant access for each report type in the Reports section (Operations > Reports). The Tenant must also have Operations: Reports access granted under the Feature permissions tab.

Personas Controls Tenant access to Morpheus Personas, at the time of this writing Users may be given access to the Standard (full Morpheus experience) or Service Catalog Personas

Catalog Item Types Controls Tenant access to Catalog Item types within the Service Catalog Persona. Only Catalog Items created in the current Tenant or those created in the Master Tenant and shared with the current Tenant will be available.
VDI Pools  Controls Tenant access to VDI Pools which are currently configured (Tools > VDI Pools) via the Virtual Desktops Persona view

Cloud Access Levels

When creating or editing a Tenant Role, Master Tenant administrators can choose which publicly-visible Clouds to share with Tenants having the current Role. Access can be completely restricted or administrators can choose between Read and Full access.

Read Access

Master Tenant administrators can opt to give other Tenants read-level access to any integrated Clouds through the Tenant Role. A read-only Cloud allows the Master Tenant to assign resources for viewing by Subtenant users but not allow them to perform any actions or provision new Instances.

With read-level access, Subtenant users will have access to the Cloud detail page (Infrastructure > Clouds). From the Summary subtab on the Cloud detail page, high-level information on Cloud resources are shown regardless of specific resources that have been shared with the Subtenant. Other metrics, such as costing, resource percentages (CPU, Memory, and Storage), VM counts and host counts will only be populated when servers in the Cloud have been assigned to the Tenant.

Full Access

With full access, Subtenant users also have access to the Cloud detail page (Infrastructure > Clouds > Specific Cloud) and see the same level of detail as Subtenants with read-only rights. However, with full access, Subtenant users can also perform many actions including the addition of Clusters, Hosts, and VMs, changing networks, and more. This cloud will also be selectable as a provisioning target for Subtenant users when deploying Instances or Apps.

Feature Access Permissions

Feature Access settings control permissions for sections and objects in Morpheus. Permission options include:

- **None**  Hidden or inaccessible for user
- **Read**   User can view but cannot edit or create
- **Full**   User has full access
- **User**  User can access Objects they have created or own.
- **Group** User can access Objects assigned to or shared with Groups the User has access to.
- **Remote Console: Provisioned**  Remote Console tab will only appear after instance is successfully provisioned.
- **Remote Console: Auto Login**  RDP and SSH only, controls if user is auto-logged in to Remote Console or presented with login prompt.

Role Mappings  Gives User Access to Role Mappings config in /admin/roles for configuring Identity Source Role Mappings without providing Access to other Identity Source configuration settings.

<table>
<thead>
<tr>
<th>Permission Name</th>
<th>Permission Options</th>
<th>Feature Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin: Appliance Settings</td>
<td>None, Full</td>
<td>Allows or disallows access to the Appliance</td>
</tr>
<tr>
<td>Permission Name</td>
<td>Permission Options</td>
<td>Feature Access</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>--------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Admin: Backup Settings</td>
<td>None, Full</td>
<td>Allows or disallows access to Administration &gt; Backup Settings.</td>
</tr>
<tr>
<td>Admin: Environment Settings</td>
<td>None, Full</td>
<td>Allows or disallows access to the Environments tab.</td>
</tr>
<tr>
<td>Admin: Guidance Settings</td>
<td>None, Full</td>
<td>Allows or disallows access to the Guidance Settings tab.</td>
</tr>
<tr>
<td>Admin: Health</td>
<td>None, Read</td>
<td>Determines access to the Administration &gt; Health tab.</td>
</tr>
<tr>
<td>Admin: Identity Source</td>
<td>None, Role Mappings, Full</td>
<td>Allows or disallows access to create, edit, or delete Identity Mappings.</td>
</tr>
<tr>
<td>Admin: Integrations</td>
<td>None, Read, Full</td>
<td>Allows or disallows access to the Integrations tab.</td>
</tr>
<tr>
<td>Admin: License Settings</td>
<td>None, Full</td>
<td>Allows or disallows access to the Licenses tab.</td>
</tr>
<tr>
<td>Admin: Log Settings</td>
<td>None, Full</td>
<td>Allows or disallows access to the Log Settings tab.</td>
</tr>
<tr>
<td>Admin: Message of the day</td>
<td>None, Full</td>
<td>Allows or disallows access to the Message of the Day tab.</td>
</tr>
<tr>
<td>Admin: Monitoring Settings</td>
<td>None, Full</td>
<td>Allows or disallows access to the Monitoring Settings tab.</td>
</tr>
<tr>
<td>Admin: Packages</td>
<td>None, Full</td>
<td>Allows or disallows access to the Packages tab.</td>
</tr>
<tr>
<td>Admin: Plugins</td>
<td>None, Full</td>
<td>Allows or disallows access to the Plugins tab.</td>
</tr>
<tr>
<td>Admin: Policies</td>
<td>None, Read, Full</td>
<td>This setting determines the level of access to Policies.</td>
</tr>
<tr>
<td>Admin: Provisioning Settings</td>
<td>None, Read, Full</td>
<td>Allows or disallows access to the Provisioning Settings tab.</td>
</tr>
<tr>
<td>Admin: Roles</td>
<td>None, Read, Full</td>
<td>This setting determines access to the Roles tab.</td>
</tr>
<tr>
<td>Admin: Service Plans</td>
<td>None, Read, Full</td>
<td>This setting determines access to Administration &gt; Service Plans tab.</td>
</tr>
<tr>
<td>Admin: Tenant</td>
<td>None, Read, Full</td>
<td>This setting determines access to Administration &gt; Tenant tab.</td>
</tr>
<tr>
<td>Admin: Tenant - Impersonate Users</td>
<td>None, Full</td>
<td>This setting allows or disallows access to impersonate users.</td>
</tr>
<tr>
<td>Admin: Users</td>
<td>None, Read, Full</td>
<td>This setting determines access to the Users tab.</td>
</tr>
<tr>
<td>Admin: Whitelabel Settings</td>
<td>None, Full</td>
<td>Allows or disallows access to the Whitelabel Settings tab.</td>
</tr>
<tr>
<td>API: Billing</td>
<td>None, Read, Full</td>
<td>Allows or disallows access to invoices and payments.</td>
</tr>
<tr>
<td>API: Execution Request</td>
<td>None, Full</td>
<td>Allows or disallows access to an API endpoint.</td>
</tr>
<tr>
<td>Backups</td>
<td>None, View, Read, User, Full</td>
<td>Determines access to the Backups section of the UI.</td>
</tr>
<tr>
<td>Backups: Integrations</td>
<td>None, Read, Full</td>
<td>Determines access to the Backups &gt; Integrations tab.</td>
</tr>
<tr>
<td>Infrastructure: Boot</td>
<td>None, Read, Full</td>
<td>Determines access to the Integrations &gt; Boot tab.</td>
</tr>
<tr>
<td>Infrastructure: Certificates</td>
<td>None, Read, Full</td>
<td>Determines access to the SSL Certificates tab.</td>
</tr>
<tr>
<td>Infrastructure: Clouds</td>
<td>None, Read, Full</td>
<td>Determines access to the Infrastructure &gt; Clouds tab.</td>
</tr>
<tr>
<td>Infrastructure: Clusters</td>
<td>None, Read, Group, Full</td>
<td>Determines access to the Infrastructure &gt; Clusters tab.</td>
</tr>
<tr>
<td>Infrastructure: Groups</td>
<td>None, Read, Full</td>
<td>Determines access to the Infrastructure &gt; Groups tab.</td>
</tr>
<tr>
<td>Infrastructure: Hosts</td>
<td>None, Read, Full</td>
<td>Determines access to the Infrastructure &gt; Hosts tab.</td>
</tr>
<tr>
<td>Infrastructure: Keypairs</td>
<td>None, Read, Full</td>
<td>Determines access to the Key Pairs tab on the UI.</td>
</tr>
<tr>
<td>Infrastructure: Load Balancers</td>
<td>None, Read, Full</td>
<td>Determines access to the Infrastructure &gt; Load Balancers tab.</td>
</tr>
<tr>
<td>Infrastructure: Network Domains</td>
<td>None, Read, Full</td>
<td>Determines access to the Domains tab on the UI.</td>
</tr>
<tr>
<td>Infrastructure: Network Firewalls</td>
<td>None, Read, Full</td>
<td>Determines access to the Firewall tab on the UI.</td>
</tr>
<tr>
<td>Infrastructure: Network Integration</td>
<td>None, Read, Full</td>
<td>Determines access to the Integrations tab on the UI.</td>
</tr>
<tr>
<td>Infrastructure: Network IP Pools</td>
<td>None, Read, Full</td>
<td>Determines access to the IP Pools tab on the UI.</td>
</tr>
<tr>
<td>Infrastructure: Network Proxies</td>
<td>None, Read, Full</td>
<td>Determines access to the Proxies tab on the UI.</td>
</tr>
<tr>
<td>Infrastructure: Network Router DHCP Pool</td>
<td>None, Read, Full</td>
<td>Determines access to the DHCP Pool tab on the UI.</td>
</tr>
<tr>
<td>Infrastructure: Network Router Firewalls</td>
<td>None, Read, Full</td>
<td>Determines access to Firewalls tabs on the UI.</td>
</tr>
<tr>
<td>Infrastructure: Network Router Interfaces</td>
<td>None, Read, Full</td>
<td>Determines access to Interfaces tabs on the UI.</td>
</tr>
<tr>
<td>Infrastructure: Network Router NAT</td>
<td>None, Read, Full</td>
<td>Determines access to the NAT tab on the UI.</td>
</tr>
<tr>
<td>Infrastructure: Network Router Redistribution</td>
<td>None, Read, Full</td>
<td>Determines access to Route Redistribution tab on the UI.</td>
</tr>
<tr>
<td>Infrastructure: Network Router Routes</td>
<td>None, Read, Full</td>
<td>Determines access to Routing tabs on the UI.</td>
</tr>
<tr>
<td>Infrastructure: Network Routers</td>
<td>None, Read, Group, Full</td>
<td>Determines access to the Routers tab on the UI.</td>
</tr>
<tr>
<td>Infrastructure: Networks</td>
<td>None, Read, Group, Full</td>
<td>Determines access to the Infrastructure &gt; Networks tab.</td>
</tr>
<tr>
<td>Infrastructure: Policies</td>
<td>None, Read, Full</td>
<td>Determines access to the Policies tabs on the UI.</td>
</tr>
<tr>
<td>Infrastructure: Security Groups</td>
<td>None, Read, Full</td>
<td>Determines access to the Security Groups tab on the UI.</td>
</tr>
<tr>
<td>Infrastructure: State</td>
<td>None, Read, Full</td>
<td>Determines access to the power state toggle on the UI.</td>
</tr>
<tr>
<td>Permission Name</td>
<td>Permission Options</td>
<td>Feature Access</td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>----------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Infrastructure: Storage</td>
<td>None, Read, Full</td>
<td>Determines access to the Infrastructure &gt; Storage tab.</td>
</tr>
<tr>
<td>Infrastructure: Storage Browser</td>
<td>None, Read, Full</td>
<td>Determines file browsing access to buckets and file shares.</td>
</tr>
<tr>
<td>Infrastructure: Trust Integrations</td>
<td>None, Read, Full</td>
<td>Determines access to the Integrations tab of the Trust Integrations page.</td>
</tr>
<tr>
<td>Integrations: Ansible</td>
<td>None, Full</td>
<td>Determines access to Ansible integrations on the Integrations tab.</td>
</tr>
<tr>
<td>Logs</td>
<td>None, Read, User, Full</td>
<td>Determines level of access to the Logs section on the Alarms tab.</td>
</tr>
<tr>
<td>Monitoring</td>
<td>None, Read, User, Full</td>
<td>Determines level of access to the Monitoring tab.</td>
</tr>
<tr>
<td>Operations: Activity</td>
<td>None, Read</td>
<td>Determines access to the Activity and History tab.</td>
</tr>
<tr>
<td>Operations: Alarms</td>
<td>None, Read, Full</td>
<td>Determines access to the Alarms tab in the Alarms tab.</td>
</tr>
<tr>
<td>Operations: Analytics</td>
<td>None, Read, Full</td>
<td>Determines access to the Operations &gt; Analytics tab.</td>
</tr>
<tr>
<td>Operations: Approvals</td>
<td>None, Read, Full</td>
<td>Determines access to the Operations &gt; Approvals tab.</td>
</tr>
<tr>
<td>Operations: Budgets</td>
<td>None, Read, Full</td>
<td>Determines access to the Operations &gt; Budgets tab.</td>
</tr>
<tr>
<td>Operations: Dashboards</td>
<td>None, Read, Full</td>
<td>Determines access to the Operations &gt; Dashboards tab.</td>
</tr>
<tr>
<td>Operations: Guidance</td>
<td>None, Read, Full</td>
<td>Determines access to the Operations &gt; Guidance tab.</td>
</tr>
<tr>
<td>Operations: Invoices</td>
<td>None, Read, Full</td>
<td>Determines access to the Operations &gt; Invoices tab.</td>
</tr>
<tr>
<td>Operations: Reports</td>
<td>None, Read, Full</td>
<td>Determines access to the Operations &gt; Reports tab.</td>
</tr>
<tr>
<td>Operations: Usage</td>
<td>None, Read, Full</td>
<td>Determines access to the Operations &gt; Usage tab.</td>
</tr>
<tr>
<td>Operations: Wiki</td>
<td>None, Read, Full</td>
<td>Determines access to the Operations &gt; Wiki page.</td>
</tr>
<tr>
<td>Projects</td>
<td>None, Read, Full</td>
<td>Determines access to Projects through Morpheus.</td>
</tr>
<tr>
<td>Provisioning Administrator</td>
<td>None, Full</td>
<td>When editing an Instance (Provisioning &gt; Instances), this permission is required.</td>
</tr>
<tr>
<td>Provisioning: Advanced Node Type Options</td>
<td>None, Full</td>
<td>This allows or disallows access to the “Extra Options” tab.</td>
</tr>
<tr>
<td>Provisioning: Allow Force Delete</td>
<td>None, Full</td>
<td>This allows or disallows access to the “Force Delete” tab.</td>
</tr>
<tr>
<td>Provisioning: Apps</td>
<td>None, Read, User, Full</td>
<td>Determines access to the Provisioning &gt; Apps tab.</td>
</tr>
<tr>
<td>Provisioning: Automation Integrations</td>
<td>None, Read, Full</td>
<td>Determines access to the Integrations tab on the Automation page.</td>
</tr>
<tr>
<td>Provisioning: Blueprints</td>
<td>None, Read, Full</td>
<td>Determines access to the Library &gt; Blueprints page.</td>
</tr>
<tr>
<td>Provisioning: Blueprints - ARM</td>
<td>None, Provision, Full</td>
<td>Determines access to ARM-type Blueprints page.</td>
</tr>
<tr>
<td>Provisioning: Blueprints - CloudFormation</td>
<td>None, Provision, Full</td>
<td>Determines access to CloudFormation-type Blueprints page.</td>
</tr>
<tr>
<td>Provisioning: Blueprints - Helm</td>
<td>None, Provision, Full</td>
<td>Determines access to Helm-type Blueprints page.</td>
</tr>
<tr>
<td>Provisioning: Blueprints - Kubernetes</td>
<td>None, Provision, Full</td>
<td>Determines access to Kubernetes-type Blueprints page.</td>
</tr>
<tr>
<td>Provisioning: Blueprint - Terraform</td>
<td>None, Provision, Full</td>
<td>Determines access to Terraform-type Blueprints page.</td>
</tr>
<tr>
<td>Provisioning: Clone Instance</td>
<td>None, Full</td>
<td>Determines access to the Clone Instance selection tab.</td>
</tr>
<tr>
<td>Provisioning: Code Integrations</td>
<td>None, Read, Full</td>
<td>Determines access to the Integrations tab on the Automation page.</td>
</tr>
<tr>
<td>Provisioning: Code Deployments</td>
<td>None, Read, Full</td>
<td>Determines access to the Deployments tab on the Automation page.</td>
</tr>
<tr>
<td>Provisioning: Code Repositories</td>
<td>None, List Files, Read, Full</td>
<td>Determines access to the Deployments tab on the Automation page.</td>
</tr>
<tr>
<td>Provisioning: Code Repositories</td>
<td>None, List Files, Read, Full</td>
<td>Determines access to the Deployments tab on the Automation page.</td>
</tr>
<tr>
<td>Provisioning: Code Repositories</td>
<td>None, List Files, Read, Full</td>
<td>Determines access to the Deployments tab on the Automation page.</td>
</tr>
<tr>
<td>Provisioning: Execute Script</td>
<td>None, Full</td>
<td>Determines access to the Run Script and App tab.</td>
</tr>
<tr>
<td>Provisioning: Execute Task</td>
<td>None, Full</td>
<td>Determines access to the Run Task tab.</td>
</tr>
<tr>
<td>Provisioning: Execute Workflow</td>
<td>None, Full</td>
<td>Determines access to the Run Workflow tab.</td>
</tr>
<tr>
<td>Provisioning: Import Image</td>
<td>None, Full</td>
<td>Determines access to the Import as Image tab.</td>
</tr>
<tr>
<td>Provisioning: Instances</td>
<td>None, Read, User, Full</td>
<td>Determines access to the Provisioning &gt; Instances tab.</td>
</tr>
<tr>
<td>Provisioning: Job Executions</td>
<td>None, Read</td>
<td>Determines access to the Job Executions tab.</td>
</tr>
<tr>
<td>Provisioning: Jobs</td>
<td>None, Read, Full</td>
<td>Determines access to the Jobs tab on the Provisioning tab.</td>
</tr>
<tr>
<td>Provisioning: Library</td>
<td>None, Read, Full</td>
<td>Determines access to the Library page, including the Tasks tab.</td>
</tr>
<tr>
<td>Provisioning: Scheduling - Execute</td>
<td>None, Read, Full</td>
<td>Determines access to the Execute Scheduling tab.</td>
</tr>
<tr>
<td>Provisioning: Scheduling - Power</td>
<td>None, Read, Full</td>
<td>Determines access to the Power Scheduling tab.</td>
</tr>
<tr>
<td>Provisioning: Service Mesh</td>
<td>None, Read, User, Full</td>
<td>Determines access to the Provisioning &gt; Service Mesh tab.</td>
</tr>
<tr>
<td>Provisioning: Tasks</td>
<td>None, Read, Full</td>
<td>Determines access to the Tasks, Workflows, and Incidents tabs.</td>
</tr>
<tr>
<td>Provisioning: Tasks - Script Engines</td>
<td>None, Full</td>
<td>Determines access to the Tasks tab of the Library page.</td>
</tr>
<tr>
<td>Provisioning: Thresholds</td>
<td>None, Read, Full</td>
<td>Determines access to the Scale Thresholds tab.</td>
</tr>
<tr>
<td>Provisioning: Virtual Images</td>
<td>None, Read, Full</td>
<td>Determines access to the Library &gt; Virtual Images tab.</td>
</tr>
<tr>
<td>Remote Console</td>
<td>None, Provisioned, Full</td>
<td>Determines access to the console on a Host detail.</td>
</tr>
<tr>
<td>Permission Name</td>
<td>Permission Options</td>
<td>Feature Access</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>Remote Console: Auto Login</td>
<td>No, Yes</td>
<td>Determines access to the Security Packages tab</td>
</tr>
<tr>
<td>Security: Scanning</td>
<td>None, Read, Full</td>
<td>Determines access to the Catalog page of the Tenant Role</td>
</tr>
<tr>
<td>Service Catalog: Catalog</td>
<td>None, Full</td>
<td>Determines access to the Inventory page of the Tenant Role</td>
</tr>
<tr>
<td>Service Catalog: Dashboard</td>
<td>None, Read</td>
<td>Determines access to the Dashboard page of the Tenant Role</td>
</tr>
<tr>
<td>Service Catalog: Inventory</td>
<td>None, Full</td>
<td>Determines access to the Catalog page of the Tenant Role</td>
</tr>
<tr>
<td>Snapshots</td>
<td>None, Read, Full</td>
<td>Determines access to the “Create Snapshot” page</td>
</tr>
<tr>
<td>Tools: Archives</td>
<td>None, Read, Full</td>
<td>Determines access to the Tools &gt; Archives page</td>
</tr>
<tr>
<td>Tools: Cypher</td>
<td>None, Read, User, Full, Full Decrypt</td>
<td>Determines access to the Tools &gt; Cypher page</td>
</tr>
<tr>
<td>Tools: Image Builder</td>
<td>None, Read, Full</td>
<td>Determines access to the Tools &gt; Image Builder page</td>
</tr>
<tr>
<td>Tools: Kubernetes</td>
<td>None, Read, User, Full</td>
<td>Allows for the management of Kubernetes clusters</td>
</tr>
<tr>
<td>Tools: Migrations</td>
<td>None, Read, Full</td>
<td>Determines access to the Tools &gt; Migrations page</td>
</tr>
<tr>
<td>Tools: Self Service</td>
<td>None, Read, Full</td>
<td>Determines access to the Tools &gt; Self Service page</td>
</tr>
<tr>
<td>None - No Permissions</td>
<td>None</td>
<td>When all permissions are set to None, the following behavior can be expected: This allows only access to the User Settings page displayed, which is accessed by clicking on the user's name in the upper-right corner of the application window.</td>
</tr>
</tbody>
</table>

### 9.4.5 Creating Roles

**User Roles**

User Roles can be single or multitenant. A Multitenant User Role is automatically copied into all existing subtenants as well as placed into a subtenant when created. Useful for providing a set of predefined roles a customer can use. The Multitenant Locked option prevent subtenant from modifying FEATURE ACCESS settings in the Role. Note Group, Instance Type and Blueprint Access settings will still be editable as Groups are unique per Tenant, and Instance and Blueprints can be a mix of unique and shared items.

**Important:** Multitenant Roles still need to be configured/managed be each subtenant, as Groups are unique per Tenant, and Instance and Blueprints can be a mix of unique and shared items.

**Note:** User Roles cannot exceed Tenant Role permissions. If a Multitenant User Role has higher permissions than the Tenant Role assigned to a subtenant, the Multitenant User Role permissions in that Tenant will automatically be reduced to match the Tenant Role permissions.

**Create a Single Tenant User Role**

1. In the Master Account, navigate to Administration > Roles
2. Select + CREATE ROLE
3. Enter a name for the Role and optional Description
4. For TYPE, select “User Role”
5. Leave the “Multi-tenant Role” checkbox blank.
6. Optionally select an existing Role to copy in the COPY FROM ROLE dropdown. * This will configure the new Role with the same configuration as the selected role to copy. A new role that is not copied from another role will be generated with all permissions set to NONE.
7. Select SAVE CHANGES

After saving the Role will be created, and you will be redirected to the Roles Permissions settings.
Create a MultiTenant User Role

A Multitenant User Role is automatically copied into all existing subtenants as well as placed into a subtenant when created. Useful for providing a set of predefined roles a Customer can use. The Multitenant Locked option prevent subtenant from modifying FEATURE ACCESS settings in the Role. Note Group, Instance Type and Blueprint Access settings will still be editable as Groups are unique per Tenant, and Instance and Blueprints can be a mix of unique and shared items.

1. In the Master Account, navigate to Administration > Roles
2. Select + CREATE ROLE
3. Enter a name for the Role and optional Description
4. For TYPE, select “User Role”
5. Optionally select an existing Role to copy in the COPY FROM ROLE dropdown. * This will configure the new Role with the same configuration as the selected role to copy. A new role that is not copied from another role will be generated with all permissions set to NONE.
6. Select the MULTITENANT ROLE checkbox
7. Optionally select the MULTITENANT LOCKED checkbox * When enabled, the FEATURE ACCESS settings in the Role will not be editable by subtenants. Group, Instance Type and Blueprint Access settings will still be editable as Groups are unique per Tenant, and Instance and Blueprints can be a mix of unique and shared items.
8. Select SAVE CHANGES

After saving the Role will be created, and you will be redirected to the Roles Permissions settings.

Important: Multitenant Roles still need to be configured/managed be each subtenant, as Groups are unique per Tenant, and Instance and Blueprints can be a mix of unique and shared items.

Note: User Roles cannot exceed Tenant Role permissions. If a Multitenant User Role has higher permissions than the Tenant Role assigned to a subtenant, the Multitenant User Role permissions in that Tenant will automatically be reduced to match the Tenant Role permissions.

Tenant Roles

A Tenant Role sets the highest possible permissions for a Tenant. User Roles within that Tenant cannot exceed those of the Tenants assigned Tenant Role. Tenant Roles can be assigned to single or multiple Tenants, and do not apply to the Master Account.

To create a Tenant Role:

1. In the Master Account, navigate to Administration > Roles
2. Select + CREATE ROLE
3. Enter a name for the Role and optional Description
4. For TYPE, select “Tenant Role”
5. Optionally select an existing Role to copy in the COPY FROM ROLE dropdown. * This will configure the new Role with the same configuration as the selected role to copy. A new role that is not copied from another role will be generated with all permissions set to NONE.

6. Select SAVE CHANGES

After saving, the Role will be created and you will be redirected to the Roles Permissions settings.

9.5 Users & User Groups

9.5.1 Users

Overview

The Users page displays a list of all Users. The following fields are surfaced for each User:

- Tenant
- Display Name
- Username
- Email
- Role

Users which are grayed out in the list are currently inactive and cannot log in. From the Actions menu in each User row, the option is given to Impersonate the User, Edit, or Remove the User.

In Morpheus 4.2.1 and higher, click on the hyperlinked Display Name of the User to see a page detailing their effective Role permissions. This is especially useful for Users in multiple Roles where it might otherwise be difficult to determine their exact rights. This page looks identical to a User Role create/edit page except none of the fields are editable. Edit the User Role permissions for the User if changes need to be made.

Note: Some User data created through an Identity Source integration (such as Active Directory) is not editable in Morpheus, as it is synced from the Identity Source.

Create User

Users can be created from Administration > Users or Administration > Tenants > (selected Tenant) > Users tab.

Note: Authorized Identity Source Users will be automatically created upon first sign in.

To create a User:

1. Navigate to either Administration > Users or Administration > Tenants > Select a Tenant.
2. Select + CREATE USER.
3. From the New User Wizard input:
   - **Username & Email**
     - First Name
     - Last Name
• Username
• Email address

Receive Notifications Enable to receive Provisioning and Policy email notifications.

Roles Role(s) to be inherited by the user. If multiple roles are selected, the higher permission levels of one role will override the other role(s).

Password Password must contain at least one uppercase letter, one lowercase letter, a number, and a symbol.

Enabled If unchecked, the user will no longer be able to sign into Morpheus, but their user data will remain.

Password Expired If enabled, the User will be forced to create a new password upon next login. The expired password cannot be used again.

Linux Settings Creates a User with the supplied Username, Password and/or Key-pair on Linux Instances when “Create my User” is selected during provisioning, or a User Group is added to an Instance of which this Morpheus user is a member of.

Windows Settings Creates a User with the supplied Username, Password and/or Key-pair on Windows Instances when “Create my User” is selected during provisioning, or a User Group is added to an Instance of which this Morpheus user is a member of.

Important: Please ensure password entered is allowable by Windows.

Note: Instance Resource Limits for a user are now configured through Policies

1. Select SAVE CHANGES.

Edit User

User settings can be edited from Administration > Users, Administration > Tenants > Select a Tenant > Users tab’, or from User Settings.

Note: Some User data from Users created via an Identity Source Integration such as Active Directory is not editable in Morpheus, as it is synced with the Identity Source.

To edit a User from the Administration > Users Section:

1. Select the Administration link in the navigation bar.
2. Select the Users link in the sub navigation bar.
3. Click ACTIONS on the row of the user to edit.
4. Select EDIT in the ACTIONS dropdown.
5. Make changes.
6. Select SAVE CHANGES.

To edit a User from the Administration > Tenants > Select a Tenant > Users tab’:

1. Select the Administration link in the navigation bar.
2. Select the Tenants link in the sub navigation bar.
3. Select a Tenant
4. Click **ACTIONS** on the row of the user to edit.
5. Select **EDIT** in the ACTIONS dropdown.
6. Make changes.
7. Select **SAVE CHANGES**.

**User Settings**

Additional settings for a User can be found in the User Settings section, including:

- User Photo
- Default Group
- Default Cloud
- API Access

To access User Settings:

1. Select your name in the header
2. Select **User Settings**

To edit the User you are currently logged in as from **User Settings**:

1. Select your name in the header
2. Select **User Settings**
3. Make changes.
4. Select **SAVE**.

**API Access**

API and CLI Access Tokens can be regenerated from the **User Settings** section.

To regenerate a CLI or API Access Token:

1. Select your name in the header
2. Select **User Settings**.
3. Select **API ACCESS** under the **Windows Settings** section.
4. Select **ACTIONS** for the Client ID the token will be generated for.
5. Select **Regenerate**.
6. Copy the Generated Access Token.

**Important**: The Access Token will be masked after User Setting are saved.

7. Select **SAVE**.
Delete User

To delete a User from the Administration > Users Section:

1. Select the Administration link in the navigation bar.
2. Select the Users link in the sub navigation bar.
3. Select **ACTIONS** on the row of the user to delete.
4. Select **REMOVE** in the ACTIONS dropdown.
5. Confirm

To delete a User from the Administration > Tenants > Select a Tenant > Users tab:

1. Select the Administration link in the navigation bar.
2. Select the Tenants link in the sub navigation bar.
3. Select a Tenant
4. Click ACTIONS on the row of the user to delete.
5. Select REMOVE in the ACTIONS dropdown.
6. Confirm

9.5.2 User Groups

Overview

User Groups can be selected during provisioning to add each group members credentials to the Instance. User Groups can be configured for sudo access and in Linux will assign Group members to a groupId in linux.

Creating User Groups

1. Navigate to Administration > Users
2. Select the USER GROUPS tab.
3. Select + CREATE USER GROUP.
4. Enter the following:
   - **NAME**  Name of the User Group
   - **DESCRIPTION**  Optional User Group Description
   - **SERVER GROUP**  Name of the groupId to assign Group members to in linux.
   - **SUDO ACCESS**  Enable to give Group members sudo access
   - **USERS**  Search for and select existing Users to add to the User Group.
5. Select SAVE CHANGES.
Editing User Groups

1. Navigate to Administration > Users
2. Select the USER GROUPS tab.
3. Select the ACTIONS dropdown next to the target User Group.
4. Select EDIT
5. Make changes, add or remove users from the group.
6. Select SAVE CHANGES.

Adding a User Group when Provisioning

1. When provisioning, in the CONFIG section expand the USER section.
2. Select an existing Group from the USER GROUP dropdown.
3. Users will be created for members in the selected User Group on the provisioned Instance(s).

9.6 Integrations

9.6.1 Integrations

To add an integration select + ADD and choose your integration. Many Morpheus-supported integrations can be configured in this section, though not all. Some integrations, such as networking integrations, must be configured within their own areas of the application. The following integrations can be configured in this section:

- Chef
- Puppet
- Ansible
- Salt Masters
- Ansible Tower
- vRealize Orchestrator
- Microsoft DNS
- PowerDNS
- Route 53
- Bind DNS
- Git
- Github
- Docker Repositories
- Jenkins
- ServiceNow
- Cherwell
- Remedy
• Venafi

Please see the *Guides* for each specific integration type for more detailed information on setup steps and features supported by the integration.

### 9.6.2 Packages

#### Overview

The `/administration/packages` is where Morpheus packages (.mpg) can be uploaded to appliances. Morpheus packages contain Library objects, such as Instance Types, Layouts, Node Types, Spec Temples and Cluster Layouts. Morpheus packages consist of library objects as code compiled into a simple `.mpg` file, allowing for agile distribution, updated and sharing of Library configurations.

The addition of `/administration/packages` in v5.3.4 is targeted for uploading future Morpheus provided MPGs, however users will be able to create, distribute and/or import custom Morpheus packages.

#### Role Permissions

Access and capabilities for the Packages section is determined by the following role permissions:

**Role: Feature Access:** Admin: Plugins

- None: Cannot access Admin: Plugins section
- Full: Access to Admin: Plugins and ability to upload Morpheus packages (.mpg)

#### Uploading Packages

`/administration/packages` is targeted for uploading future Morpheus provided mpg’s, however users will be able to create, distribute and/or import custom Morpheus packages. Additional information on creating custom packages will be provided.

### 9.6.3 Plugins

#### Overview

Morpheus is extendable with custom plugins for Task types, UI tabs, approvals, cypher, and more. Plugins are added from the Plugins tab of the Integration page under Administration (Administration > Integrations > Plugins). Simply browse for a local plugin file (.jar) to add it to the UI. Custom plugins can also be deleted by clicking on the trash can icon in the corresponding row.

Please visit the [Morpheus Developer Portal](#) for Plugin Architecture SDK documentation and help getting started with custom Plugin development.
9.6.4 Distributed Workers

Overview

The Morpheus distributed worker is installed using the same package as the VDI Gateway worker. Organizations which have already deployed VDI Gateway(s) can use the same worker for both purposes if desired, you’d simply need to update configuration in `/etc/morpheus/morpheus-worker.rb` and run a reconfigure. When creating a distributed worker or VDI Gateway object in Morpheus UI, an API key is generated. Adding one or both types of API keys to the worker configuration file determines if the worker is running in VDI gateway and/or distributed worker mode.

Installation

A distributed worker VM is installed and configured similarly to a Morpheus appliance via `rpm` or `deb` package.

Note: Package URLs for the distributed worker are available at [https://morpheushub.com](https://morpheushub.com) in the downloads section.

Requirements

<table>
<thead>
<tr>
<th>Table 4: Supported Operating Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS</td>
</tr>
<tr>
<td>----------</td>
</tr>
<tr>
<td>Amazon Linux</td>
</tr>
<tr>
<td>CentOS</td>
</tr>
<tr>
<td>Debian</td>
</tr>
<tr>
<td>RHEL</td>
</tr>
<tr>
<td>SUSE SLES</td>
</tr>
<tr>
<td>Ubuntu</td>
</tr>
</tbody>
</table>

- **Memory**: 4 GB RAM minimum recommended
- **Storage**: 10 GB storage minimum recommended. Storage is required for installation packages and log files
- **CPU**: 4-core minimum recommended
- **Network connectivity to** the Morpheus appliance over TCP 443 (HTTPS)
- **Superuser privileges** via the `sudo` command for the user installing the Morpheus worker package
• Access to base `yum` or `apt` repos. Access to Optional RPM repos may be required for RPM distros

Download the appropriate package from Morpheus Hub based on your target Linux distribution and version for installation in a directory of your choosing. The package can be removed after successful installation.

```
wget https://downloads.morpheusdata.com/path/to/morpheus-worker-$version.$distro
```

Validate the package checksum as compared with the values indicated on Hub. For example:

```
sha256sum morpheus-worker-$version.$distro
```

Next, install the package using your selected distribution’s package installation command and your preferred options. Example, for RPM:

```
rpm:
  sudo rpm -ihv morpheus-worker-$version.$distro
```

```
Preparing... #...[100%]
Updating / installing...
  1:morpheus-worker-x.x.x-1.$distro #...[100%]
Thank you for installing Morpheus Worker!
Configure and start the Worker by running the following command:
  sudo morpheus-worker-ctl reconfigure
```

### Configuration

With the package installed, we need to add a new distributed worker in Morpheus UI. Distributed workers are added in Administration > Integrations > Distributed Workers. To create one, populate the following fields:

- **NAME**: A name for the distributed worker in Morpheus
- **DESCRIPTION**: An optional description for the distributed worker
- **PROXY HOSTS**: A comma-delimited list of global proxy hosts, any endpoint listed here will be proxied through the Morpheus worker. For VMware, you must list the host addresses for any vCenter you wish to proxy through the worker. Xen hosts must be listed here as well. Other Cloud types which are supported by the Morpheus worker need only have the worker configured on the Edit Cloud modal (Infrastructure > Clouds > Selected Cloud > Edit button)
- **ENABLED**: When marked, the selected worker is available for use

After clicking **SAVE CHANGES**, an API key is generated and displayed. Make note of this as it will be needed in a later configuration step.
With the worker configured in Morpheus, the next step is to update any Cloud integrations which should be proxied through the worker. Select the desired Cloud from the Clouds List Page (Infrastructure > Clouds) and click **EDIT** from the chosen Cloud’s Detail Page. Within the Advanced Options section, choose a configured worker from the DISTRIBUTED WORKER dropdown menu. Click **SAVE CHANGES**.

With the API key in hand and configuration complete in Morpheus UI, head back to the worker box. Configure the gateway by editing `/etc/morpheus/morpheus-worker.rb` and updating the following:

```ruby
worker_url 'https://gateway_worker_url' # This is the worker URL the appliance can resolve and reach on 443
worker['appliance_url'] = 'https://morpheus_appliance_url' # The resolvable URL or IP address of appliance which the worker can reach on port 443
worker['apikey'] = 'API KEY FOR THIS GATEWAY' # VDI Gateway API Key generated from appliance VDI Pools > VDI Gateways configuration. For worker only mode, a value is still required but can be any value, including the 'API KEY FOR THIS GATEWAY' default template value
worker['worker_key'] = 'DISTRIBUTED WORKER KEY' # Distributed Worker API Key from AdmIntDis configuration
```

(continues on next page)
Note: By default the worker_url uses the machine’s hostname, ie https://your_machine_name. The default worker_url value can be changed by editing /etc/morpheus/morpheus-worker.rb and changing the value of worker_url. Additional appliance configuration options are available below.

After all configuration options have been set, run sudo morpheus-worker-ctl reconfigure to install and configure the worker, nginx and guacd services:

```
sudo morpheus-worker-ctl reconfigure
```

The worker reconfigure process will install and configure the worker, nginx and guacd services and dependencies.

Tip: If the reconfigure process fails due to a missing dependency, add the repo that the missing dependency can be found in and run

```
Note: Configuration options can be updated after the initial reconfigure by editing /etc/morpheus/morpheus-worker.rb and running sudo morpheus-worker-ctl reconfigure again.
```

Once the installation is complete the morpheus worker service will automatically start and open a web socket with the specified Morpheus appliance. To monitor the startup process, run morpheus-worker-ctl tail to tail the logs of the worker, nginx and guacd services. Individual services can be tailed by specifying the service, for example morpheus-worker-ctl tail worker

### 9.7 Policies

#### 9.7.1 Overview

Policies add governance, ease of use, cost-savings, and auditing features to Morpheus. Morpheus enables end users to create Policies scoped to Users, Roles, Groups, Clouds, Tenants and Global scoping to give Admins full control and governance over their environments! Policy generation is a role permission.

#### 9.7.2 Policy Types

- **Approve Delete** Sets an approval requirement for deleting Instances or Apps within the Policy scope. When setting the Policy, users have the option of using Morpheus Approvals or an Approval Integration such a ServiceNow.

- **Approve Provision** Sets an approval requirement for provisioning Instances or Apps within the Policy scope. When setting the Policy, users have the option of using Morpheus Approvals or an Approval Integration such a ServiceNow.

- **Approve Reconfigure** Sets an approval requirement for reconfiguring Instances and servers within the Policy scope. When setting the Policy, users have the option of using Morpheus Approvals or an Approval Integration such a ServiceNow.

- **Backup Creation** Disable or enable the ability to create a backup when provisioning an instance.

- **Backup Targets** A master account can determine storage provider options for backups with Backup Targets policies.
**Budget**  Sets a maximum total combined price for all instances in the Group, Cloud, Tenant or owned by the User this policy is applied to.

**Cluster Resource Name**  The name of Cluster hosts (master and workers) when creating Kubernetes, Docker and KVM Clusters. Pre-populates a fixed or editable Resource Name value for the cluster using \${variable} naming patterns and/or text, including \${sequence} numbering. Toggle whether sequence numbers are reusable (after the resource using them is destroyed) by enabling **Reuse Naming Sequence Numbers** in Administration > Settings.

**Delayed Delete**  Delayed Delete Policies allow for soft deletion of Instances and Apps. Instead of deleting immediately, Instances and Apps with a Delayed Removal policy applied will be shutdown upon deletion request and hidden by default from the UI. The Instance/App will then be in **Pending Removal** status.

**Expiration**  Sets an expiration timeframe in days after which the Instance will be deleted. Extensions can be auto-approved or require approval immediately or after x amount of auto-extensions using Morpheus Approvals or an Approval Integration.

**File Share Storage Quota**  Sets a Storage Quota for File Share usage (in GB) to scoped User, Role, Tenant or Global.

**Hostname**  The hostname or computer name which is set in the OS and DNS. On some platforms, hostnames are restricted by length, spaces, and/or special characters. Pre-populates a fixed or editable name for hostnames/machine names using \${variable} naming patterns and/or text, including \${sequence} numbering. Toggle whether sequence numbers are reusable (after the resource using them is destroyed) by enabling **Reuse Naming Sequence Numbers** in Administration > Settings.

**Instance Name**  Pre-populates a fixed or editable name for Instance Names using \${variable} naming patterns and/or text, including \${sequence} numbering. Toggle whether sequence numbers are reusable (after the resource using them is destroyed) by enabling **Reuse Naming Sequence Numbers** in Administration > Settings.

**Max Containers**  Sets the max number of Containers for the Group or Cloud the Policy is added to.

**Max Cores**  Sets the max number of total of Cores combined for Instances in the Group or Cloud the Policy is added to.

**Max Hosts**  Sets the max number of total Hosts in the Group or Cloud the Policy is added to.

**Max Memory**  Sets the max number of total of RAM combined for Instances in the Group or Cloud the Policy is added to.

**Max Storage**  Sets the max number of total of Storage combined for Instances in the Group or Cloud the Policy is added to.

**Max VMs**  Sets the max number of Virtual Machines for the Group or Cloud the Policy is added to.


---

**Note:**  Requires role permission: Admin: **Message Of the Day** set to “Full” to create and manage MOTD Policies.

---

**Network Quota**  Limits the number of networks that can be created within the policy’s scope.

**Object Storage Quota**  Sets a Storage Quota for Object Storage usage (in GB) to scoped User, Role, Tenant or Global.

**Power Scheduling**  Adds a Power Schedule for the Instances in a Group or Cloud. Power Schedules can be created in Library > Automation > Power Scheduling.

**Router Quota**  Limits the number of routers that can be created within the policy’s scope.
**Shutdown**  Sets a shutdown timeframe in days upon provision after which the Instance will be stopped. Extensions can be auto-approved or require approval immediately or after x amount of auto-extensions using Morpheus Approvals or an Approval Integration.

**Storage Server Storage Quota**  Sets a Storage Quota for selected Storage Server (in GB), applied Globally or per specified Tenants.

**Tags**  Requires the user to add compliant Tags at provision time, this can be enforced on a strict or passive basis

---

**Note:**  Tag scanning and enforcement is currently only available for Azure, Amazon, Google, and VMware clouds. For a more comprehensive guide on implementing Tag Policies, see the associated article in our KnowledgeBase.

---

**User Creation**  Controls the “CREATE YOUR USER” flag in the User Config options during provisioning do be always disabled, always enabled, enabled by default, or disabled by default.

**User Group Creation**  Forces User Creation of members in the selected User Group during Provisioning.

**Workflow**  Forces execution of selected Workflow for Instance Provisioning.

---

### 9.7.3 Creating Policies

Policies can be created in three different locations.

- Administration > Policies
- Infrastructure > Groups > Group > Policies
- Infrastructure > Clouds > Cloud > Policies

Policies can be disabled and re-enabled at anytime.

---

**Important:**  Precedence is applied to matching or conflicting Policies in the following order: Cloud > Group > Role > User > Global.

---

**To create a Global Policy:**

1. Navigate to Administration > Policies
2. Select *ADD Policy* and choose from the available policy types.
3. Refer to Policy Type sections below for Configuration options.
4. Under Filter next to scope select *Global*
5. Select *SAVE CHANGES*
To create a Policy for a User:

1. Navigate to Administration > Policies
2. Select + ADD Policy and choose from the available policy types.
3. Refer to Policy Type sections below for Configuration options.
4. Under filter next to scope select User a drop down menu will appear below allowing you to select a user
5. Select SAVE CHANGES

To create a Policy for a Role:

1. Navigate to Administration > Policies
2. Select + ADD Policy and choose from the available policy types.
3. Refer to Policy Type sections below for Configuration options.
4. Under filter next to scope select Role a drop down menu will appear below allowing you to select a Role
5. For APPLY INDIVIDUALLY TO EACH USER IN ROLE
   • Select for Max Resource/Quota Policies to be calculated per user
   • Leave unselected to calculate by total usage of all users within that Role.
6. Select SAVE CHANGES

To create a Policy for a Cloud:

Note: Resource Limitation Policies apply to all Instances in the Cloud the Policy is added to. Approval, Naming, Power, Shutdown and Expiration Policies apply to Instances created or moved into the Group after the Policy is enabled.

1. Navigate to Infrastructure > Clouds
2. Select a Cloud by clicking on the name of the Cloud to go to the Cloud Detail page.
3. Select the POLICIES tab in the Cloud Detail page.
4. Select + ADD and choose from the available policy types.
5. Refer to Policy Type sections below for Configuration options.
6. Select SAVE CHANGES

To create a Policy for a Group:

Note: Resource Limitation Policies apply to all Instances in the Group the Policy is added to. Approval, Naming, Power, Shutdown and Expiration Policies apply to Instances created after the Policy is enabled.

1. Navigate to Infrastructure > Groups
2. Select a Group by clicking on the name of the Group to go to the Group Detail page.
3. Select the POLICIES tab in the Group Detail page.
4. Select + ADD and choose from the available policy types.
5. Refer to Policy Types sections below for Configuration options.
6. Select SAVE CHANGES

9.7.4 Policy Types

Expiration Policies

Expiration policies set an expiration timeframe for any instance provisioned into the cloud, role, group or by the user the policy is added to. When an instance expires, it is terminated and deleted.

Configuration options for expiration policies:

Expiration Type
- User Configurable- expiration timeframe is editable during provisioning
- Fixed Expiration- user cannot change expiration timeframe

Expiration Days  Configures the number of days the instance is allowed to exist before being removed.

Renewal Days  If the instance is renewed, this is the number of days by which the expiration date is increased.

Notification Days  This allows an email notice to be sent out X days before the instance is set to expire.

Notification Message  Customizable message for notification emails. The default message is Instance
  ${instance?.name} is set to expire on ${instance?.expireDate}

Auto Approve Extensions  Enable this to auto-approve extension requests, bypassing approval workflows.

Instances with expirations show the time until expiration in the instance detail pane. Instances with active expiration policies can be extended by selecting the EXTEND NOW button in the instance detail pane. The extension length is set in the policy by the RENEWAL DAYS field.

Expirations can also be added to any instance during provisioning by entering the number of days in the EXPIRATION DAYS field in the Lifecycle section of the automation section of the provisioning wizard. Expiration can be added to any instance even if no policies have been created.

Note: Expiration and Shutdown Policies will be enforced on Instances created when converting a discovered host to managed.

Instance and Host Names

Naming Policies will populate a fixed or editable name for instances, hosts and hostnames. The Name Pattern field uses ${variable} string interpolation.

NAMING TYPE
- User Configurable  Naming pattern will pre-populate during provisioning but can be edited by the user.
- Fixed Name  Naming pattern will pre-populate during provisioning and cannot be changed.

NAME PATTERN  The Name Pattern field uses Static text and/or ${variable} string interpolation, such as morpheus${cloudCode}${type}${sequence+3000}

An example Instance Name Policy using a naming pattern with User Initials, Cloud Code, Instance Type, and a sequential number starting at 3000 is
\$\{userInitials\}-\$\{cloudCode\}-\$\{type\}-\$\{sequence+3000\}, resulting in an Instance Name of \texttt{md-vmwd3-centos-3001} for the first instance, followed by \texttt{md-vmwd3-centos-3002} and so on.

Commonly used variables for naming patterns include:

\begin{verbatim}
\$\{groupName\} \\
\$\{groupCode\} \\
\$\{cloudName\} \\
\$\{cloudCode\} \\
\$\{type\} \\
\$\{accountId\} \\
\$\{account\} \\
\$\{accountType\} \\
\$\{platform\} \\
\$\{platform == 'windows' ? 'w':'l'} # results in `w` for Windows platforms and `l` for Linux Platforms \\
\$\{userId\} \\
\$\{username\} \\
\$\{userInitials\} \\
\$\{provisionType\} \\
\$\{instance.instanceContext\} # Environment Code \\
\$\{sequence\} # results in 1 \\
\$\{sequence+100\} # results in 101 \\
\$\{sequence.toString().padLeft(5,'0')} #results in 00001
\end{verbatim}

Cloud codes and Group codes are fields found in their respective configuration panes.

**AUTO RESOLVE CONFLICTS** Morpheus will automatically resolve naming conflicts by appending a sequential number to the name when enabled.

**Shutdown Policies**

Shutdown policies dictate the number of days an instance is allowed to run before it is shut down. Shutdown is consistent across cloud types i.e.: in VMware, a VM is powered off. In AWS, an instance is stopped. Etc.

Configuration options for shutdown policies:

**Shutdown Type**

\begin{itemize}
\item \textbf{User Configurable} Shutdown timeframe is editable during provisioning.
\item \textbf{Fixed Expiration} User cannot change shutdown timeframe during provisioning.
\end{itemize}

**Expiration Days** Configures the number of days the instance is allowed to exist before being shut down.

**Renewal Days** If the instance is renewed, this is the number of days by which the shutdown date is increased.

**Notification Days** This allows an email notice to be sent out X days before the instance is set to shut down.

**Notification Message** Customizable message for notification email.

**Auto Approve Extensions** Enable this to auto-approve extension requests, bypassing approval workflows.

\begin{itemize}
\item \textbf{Note:} Expiration and Shutdown Policies will be enforced on Instances created when converting a discovered host to managed.
\end{itemize}
Provision Approval

Morpheus Provision Approvals enable an approval workflow via internal Morpheus approval or via ServiceNow workflow. If a ServiceNow integration is present, the ServiceNow option is enabled. The Approval workflow to be selected is dynamically created by querying the ServiceNow Workflow table in the integrated ServiceNow instance.

This ServiceNow approval integration enables users to use the Morpheus Self-Service provisioning portal to provision new instances and still respect the required ServiceNow business approval workflow.

Power Schedules

Power Schedules set daily times to shutdown and startup instances. Power schedule can be created and managed in Library > Automation > Power Scheduling

**Note:** Power Schedule Policies will apply to Instances created in a Group or Cloud after the Policy is enabled, and will not apply to pre-existing Instances.

Configuration options for Power Schedule Policies:

**DESCRIPTION** Add details about your Policy for reference in the Policies tab.

**Enabled** Policies can be edited and disabled or enabled at any time. Disabling a Power Schedule Policy will prevent the Power Schedule from running on the Groups Instances until re-enabled.

**ENFORCEMENT TYPE**

- User Configurable: Power Schedule choice is editable by User during provisioning.
- Fixed Schedule: User cannot change Power Schedule setting during provisioning.

**POWER SCHEDULE** Select Power Schedule to use in the Policy. Power schedule can be added in Library > Automation > Power Scheduling

**TENANTS** Leave blank for the Policy to apply to all Tenants, or search for and select Tenants to enforce the Policy on specific Tenants.

Max Resources

Max Resource policies allow setting quotas for Clouds, Groups, Roles or Users for maximum amount of Memory, Storage, Cores, Hosts, VM’s, or Containers that can be created in the Cloud, Group, Role or by the User the Policy is assigned to.

Configuration options for Max Resources Policies:

**Max Containers** Sets the maximum combined total of Containers in Instances per Policy Scope.

**Max Cores** Sets the maximum combined total of Cores in Instances per Policy Scope.

**Max Hosts** Sets the maximum total of Hosts per Policy Scope.

**Max Memory** Sets the maximum combined total of RAM (capacity) for Instances per Policy Scope.

**Max Storage** Sets the maximum combined total of Storage (capacity) for Instances per Policy Scope.

**Max VMs** Sets the maximum total of managed Virtual Machines per Policy Scope.

**TENANTS** Leave blank for the Policy to apply to all Tenants, or search for and select Tenants to enforce the Policy on specific Tenants.
User Creation

The User Creation policy controls the “CREATE YOUR USER” flag in the User Config options during provisioning to be always disabled, always enabled, enabled by default, or disabled by default.

Configuration options for User Creation Policies:

**TYPE**  User Creation

**DESCRIPTION**  Description to identify the policy config

**Enabled**  Policies enforcement can be disabled or enabled at any time.

**ENFORCEMENT TYPE**

- User Configurable: User Creation choice is editable by User during provisioning.
- Fixed: User cannot change User Creation setting during provisioning.

**CREATE USER**  Check to allow or force user creation. Uncheck to disable by default or force no user creation.

**TENANTS**  Leave blank for the Policy to apply to all Tenants, or search for and select Tenants to enforce the Policy on specific Tenants.
The Morpheus Health section provides an overview of the health of your Morpheus appliance. It includes data on the following:

- Health Levels
- CPU
- Memory
- Database
- Elastic
- Queues
Note: An Elasticsearch warning status is typical for single node Appliances due to a single elasticsearch node and default replica count exceeding available nodes.

HEALTH LEVELS include
- Morpheus CPU
- System CPU
- Morpheus Memory
- System Memory
- Used Swap

CPU include
- Processor Count
- Process Time
- Morpheus CPU
- System CPU
- System Load

MEMORY includes
- Morpheus Memory
- Morpheus Used Memory
- Morpheus Free Memory
- Morpheus Memory Usage
- System Memory
- System Used Memory
- System Free Memory
- System Memory Usage
- System Swap
- Free Swap

DATABASE includes
- Lifetime Connections
- Aborted Connections
- Max Used Connections
- Max Connections
- Threads Running
- Threads Connected
- Slow Queries
- Temp Tables
- Key Reads
• Handler Reads
• Buffer Pool Free
• Open Tables
• Table Scans
• Full Joins
• Key Read Requests
• Key Reads
• Engine Waits
• Lock Waits
• Handler Reads
• Engine IO Writes
• Engine IO Reads
• Engine IO Double Writes
• Engine Log Writes
• Engine Memory
• Dictionary Memory
• Buffer Pool Size
• Free Buffers
• Database Pages
• Old Pages
• Dirty Page Percent
• Max Dirty Pages
• Pending Reads
• Insert Rate
• Update Rate
• Delete Rate
• Read Rate
• Buffer Hit Rate
• Read Write Ratio
• Uptime

ELASTIC includes
• Status
• Cluster
• Node Count
• Data Nodes
• Shards
• Primary Shards
• Relocating Shards
• Initializing
• Unassigned
• Pending Tasks
• Active Shards

Note: Warning status is typical for Elasticsearch

Elastic Nodes include
• Node
• Master
• Location
• Heap Usage
• Memory Usage
• CPU Usage
• 1M Load
• 5M Load
• 15M Load

Elastic Indices include
• Health
• Index
• Status
• Primary
• Replicas
• Doc
• Count
• Primary
• Size
• Total Size

QUEUES INCLUDE
• Queue Count
• Busy Queues
• Error Queues
9.9 Settings

The `AdmSet` section sets global configuration parameters for the Morpheus appliance, whitelabeling, provisioning, monitoring, backups, logs, software licenses, and the license for Morpheus itself.

9.9.1 Appliance

Appliance Settings

**Appliance URL**  The default URL used for Agent install and Agent functionality. All Instances and Hosts must be able to resolve and reach this URL over 443 for successful agent install and communication.

**Note:** Alternate Appliance URLs can be configured per Cloud in the *Edit Cloud > Advanced Options* section.

**Internal Appliance URL (PXE)**  For PXE-Boot your appliance needs to be routable directly with minimal NAT masquerading. This allows one to override the default appliance url endpoint for use by the PXE Server. If this is unset, the default appliance url will be used instead.

**API Allowed Origins**  Specifies which origins are allowed to access the Morpheus API.

**Cloud Sync Interval**  Data is refreshed through cloud integrations at the interval specified here in seconds, the default value is 300 seconds (five minutes). Appliances managing a very large number of clouds may be adversely affected by setting this value too low.

**Denied Hosts**  A comma-delimited list of IP addresses and/or hostnames which should not be allowed sources for HTTP Tasks or REST-populated Option Lists.

**Approved Hosts**  A comma-delimited list of IP addresses and/or hostnames which are the only approved sources for HTTP Tasks or REST-populated Option Lists. By entering any values here, all others are automatically denied.

**Enable SSL Verification of Agent (Communications)**  Enabling SSL Verification of Agent Communications requires a valid Certificate be installed on the Appliance.

**Disable SSH Password Authentication**  Only allow ssh login using SSH keys. When true, SSH Password Authentication will not be enabled for VM’s and Hosts provisioned after the setting is enabled.

**Default Appliance Locale**  Sets the default language and region for all users on the Morpheus appliance. Users with individual language preferences may also override this selection on their User Settings page.

Tenant Management Settings

**Registration Enabled**  If enabled, the appliance login screen will have a “NEED AN ACCOUNT? SIGN UP HERE” link added, enabling new Tenant registration.

**Default Tenant Role**  Sets the default Tenant Role applied to Tenants created from Tenant Registration.

**Default User Role**  Sets the default User Role applied to the User created from a Tenant Registration.
User Management Settings

Min Password Length User passwords must at least be as many characters in length as the entered value

Min Password Uppercase User passwords must include at least as many uppercase characters as the entered value

Min Password Numbers User passwords must include at least as many numerals as the entered value

Min Password Symbols User passwords must include at least as many special characters as the entered value

Session Expires (Minutes) A user session is forcibly logged out after the entered number of minutes of inactivity

Session Warning (Minutes) A pop-up warning is shown to the user when they have been inactive for the number of minutes entered. Example: If sessions are set to expire after 90 minutes, warn the user after 60 minutes if you intend to provide 30 minutes advance warning

Expire Password After (Days) User account passwords will expire after the entered number of days. Enter 0 or leave the field empty to opt out of this feature.

Disable User After Attempts (Number of Attempts) Disable a User account after a specified number of failed login attempts. Enter 0 or leave the field empty to opt out of this feature.

Disable User If Inactive For (Days) Disable a User account if inactive for the entered number of days. The User will not be able to log into the appliance again until another User with sufficient rights enables the account. Enter 0 or leave the field empty to opt out of this feature.

Send warning email before deactivating (Days) Enter the number of days prior to account deactivation that a warning email should be sent. For example, enter “5” to warn the User when they are five days short of the deactivation time entered in the prior field. Enter 0 or leave the field empty to opt out of this feature.

Email Settings

In this section, you can configure an SMTP server for email notification delivery. You will need to provide Morpheus the following information, your mail server systems administrator can assist you in filling these fields and with the preferred encryption method.

- From Address
- SMTP Server
- SMTP Port
- SSL Enabled
- TLS Encryption
- SMTP User
- SMTP Password

We recommend that you add the Morpheus server to your SMTP whitelist as well as using user authentication as an additional security measure.

Once you have added your SMTP server information into Morpheus, scroll down to the bottom of the page and press the blue SAVE button which can be found under the Enabled Clouds section.

When you have saved your SMTP server settings in the Morpheus appliance you will then need to restart the UI. To restart the morpheus-ui, connect to your Morpheus server via SSH and run the below command:

```bash
sudo morpheus-ctl restart morpheus-ui
```
**Important:** If you do not restart morpheus-ui, the notifications will not be sent. Please note it can take up to three minutes for the UI to become reachable again.

---

**Twilio SMS Settings**

Configure SMS text message delivery for Morpheus alerts. Previously, customers could use Morpheus’ own account for delivery, but for security reasons clients must now supply their own. Complete the fields indicated below and then restart all Morpheus nodes to apply the changes.

- **Account SID:** Twilio Account SID
- **SMS From #:** The “From” number to receive the text message from
- **Auth Token:** The Twilio API authentication token for your account

---

**Proxy Settings**

The Morpheus Appliance can be configured to communicate through a Proxy server for Cloud API’s and Agent communication back to the Appliance.

**Note:** Additional Proxy configuration is available in the *Infrastructure > Network > Proxies* section. Added Proxies can be scoped to Clouds in the *Edit Cloud > Advanced Options* section of the Cloud.

Add a Global Proxy server by entering the following:

- Proxy Host
- Proxy Port
- Proxy User
- Proxy Password
- Proxy Domain
- Proxy Workstation

---

**Currency Settings**

In Morpheus, Tenants are separate environments which can be defined as using currencies that are unique from one Tenant to the next. In addition, these currencies may be different from the currency in which Price Sets have been defined. In order to present pricing to Subtenant users in their designated currency, Morpheus allows for integration with currency conversion services “open exchange rates” and “fixer.io”. This article goes through the process of setting up the integration and how it works to determine pricing conversions.
Integrating With a Currency Exchange Provider

1. Navigate to Administration > Settings > Appliance
2. Under the Currency Settings heading, make a “Currency Provider” selection
3. Enter your “Provider API Key”

The service is now integrated and can be used as described in the next section.

Consuming Currency Exchange in Morpheus

Currency exchange data is synced from the integrated provider once every 12 hours. When needed, Morpheus will use this cached data to present currency conversions rather than hitting the API directly each time. This limits the total number of API hits and reduces costs.

Exchanged currency values will be shown under conditions similar to the following scenario:

A user is working in a Subtenant configured for Currency B. The user is attempting to provision an instance with pricing sets that have only been defined in Currency A. Morpheus will convert the pricing data from currency A to Currency B for this user (and all users in this Subtenant) since price conversion has been enabled.

Enabled Clouds (Types)

Controls which types of Cloud can be created.

- When a Cloud type is disabled, it will be removed from the available options when adding new Clouds in Infrastructure > Clouds. Existing Clouds are not affected by changes to this setting.

9.9.2 Whitelabel

Whitelabel Settings

Overview

Morpheus Tenants can be WhiteLabeled with custom Logos, Colors, Copy, and custom CSS. Sub-Tenants can be individually white-labeled, or the Master Tenant Whitelabel can apply to all Sub-Tenants.

Enable Whitelabel  Turns on the configured Whitelabel settings. Disabling will return the Appliance to the default colors and logos, but the configured options will remain saved and will apply if Whitelabel is re-enabled.

Appliance Name  Replaces Morpheus in page titles.

Header Logo  Top left header logo. Uploaded image is resized to 38 pixels high with a proportional width at that height.

Disable Support Menu  Enable this flag to hide the support dropdown menu in the header.

Support Menu Links  Customize support links. Label Code can be used for translations and is optional. Be sure to specify fully qualified url if linking to external sites.

Security Banner

The Security Banner section in /admin/settings#!whitelabel displays content on the login screen for Security and Consent messaging and warnings.

- Applicable at Global and Tenant levels
- Security Banner input field accepts plain text and markdown
• Content is displayed below login section in scoped /login/auth pages.

**Footer Logo** Footer Logo in bottom left. Uploaded image is resized to 27 pixels high with a proportional width at that height.

**Login Logo** Logo shown on Login screen. Uploaded image is resized to 192 pixels wide with an unbound height proportional to that locked width.

**Favicon** Must be a .ico file type.

**Reset** When selected and Whitelabel settings are saved, associated logo is returned to blank default value.

**Colors**

Update Colors by entering HEX value or selecting the Color Selector pop-up next to each filed and selecting a color.

• Header Background
• Header Foreground
• Nav Background
• Nav Foreground
• Nav Hover
• Primary Button Bg
• Primary Button Fg
• Primary Button Hover Bg
• Primary Button Hover Fg
• Footer Background
• Footer Foreground
• Login Background

**Override CSS**

Override CSS settings by entering CSS in *Override CSS* field.

Example: (this will add one continues background image to the Header)

```css
textarea .CodeMirror-code 
header #topHeader {
    background-image: url(http://image_url.png);
}
header {
    background-image: url(http://image_url.png);
}
```
Copy

Add custom Copyright String, Terms of Use, Privacy Policy contained in the Footer text and links in the App and on the login page and emails.

Available Copy fields

- Copyright String
- Terms and Privacy String
- Terms of Use
- Privacy Policy

Note: Terms of Use and Privacy Policy Footer links will load internal pages at https://appliance_url/privacy-policy and https://appliance_url/terms-of-use displaying the entered info as plain text. The Terms and Privacy String will update the legal text displayed on the Morpheus login page. This field takes any custom HTML markup allowing you to link to the internal legal pages or to your own outside legal pages if you prefer.

UI Loading Page

When the Morpheus UI is restarted or loading, a default “Morpheus is Loading” page is displayed. This page can be changed by adding the following to /etc/morpheus/morpheus.rb and adjusting the values.

Note: morpheus-ctl reconfigure must be ran for any changes to /etc/morpheus/morpheus.rb to take effect.

```ruby
nginx['web_root_internal'] = "/opt/morpheus/embedded/nginx/html"
nginx['loading_pages']['max_loops'] = 6 * 10 # 10 secs per loop x 6 times to get 60
  # seconds x 10 to get to 10 minutes
nginx['loading_pages']['timeout_page'] = '/timeout.html'
nginx['loading_pages']['iteration_time'] = 10_000
nginx['loading_pages']['loading_page_title'] = 'Morpheus Loading'
nginx['loading_pages']['loading_page_h1'] = 'Morpheus is Loading...'
nginx['loading_pages']['loading_page_h2'] = 'please wait'
nginx['loading_pages']['timeout_page_title'] = 'Morpheus timeout, please try again...'
nginx['loading_pages']['timeout_page_h1'] = 'Timeout waiting for Morpheus to load, click below to try again.'
nginx['loading_pages']['failure_page_title'] = 'Morpheus Server Error'
nginx['loading_pages']['failure_page_h1'] = 'Morpheus Server Error'
nginx['loading_pages']['failure_page_h2'] = 'Please contact your system administrator for assistance.'
```
9.9.3 Provisioning

Provisioning Settings

**Allow Cloud Selection**  Displays or hides Cloud Selection dropdown in Provisioning wizard.

**Allow Host Selection**  Displays or hides Host Selection dropdown in Provisioning wizard.

**Require Environment Selection**  Forces users to select and Environment during provisioning.

**Show Pricing**  Displays or hides Pricing in Provisioning wizard and Instance and Host detail pages.

**Hide Datastore Stats On Selection**  Hides Datastore utilization and size stats in provisioning and app wizards.

**Cross-Tenant Naming Policies**  Enable for the sequence value in naming policies to apply across tenants.

**Reuse Naming Sequence Numbers**  When selected, sequence numbers can be reused when Instances are removed. Deselect this option and Morpheus will track issued sequence numbers and use the next available number each time.

**Deployment Archive Store**  Default Storage Provider for storing Deployment Archives.

---

**Note:**  Storage Providers can be configured and managed in the Infrastructure > Storage section.

Cloud-Init Settings

Morpheus can add global users for Linux and Windows at provision time. Cloud-init/Cloudbase-Init or VMware Tools installed on the provisioned virtual images is required.

**Linux**

- **Username:** Enter User to be added to Linux Instances during provisioning.
- **Password:** Enter password to be set for the above Linux user.
- **KeyPair:** Select KeyPair to be added for the above Linux user.

**Note:**  Either a password, keypair, or both can be populated for the Linux user. Keypairs can be added in the Infrastructure > Keys & Certs section.

Windows Settings

- **Administrator Password:** Enter password to be set for the Windows Administrator User during provisioning.

PXE Boot Settings

**Default Root Password**  Enter the default password to be set for Root during PXE Boots.
Overview

The Environments section is where you create and manage your environment labels, which are available in the Environment dropdown during Instance or App provisioning. An Instance’s environment label can be changed by editing the Instance.

Creating Environments

1. Select + Create Environment
2. Populate the following for the New Environment:
   - **Name**  The friendly name for the environment in Morpheus
   - **Code**  Shortcode used for API and CLI
   - **Description**  Environment description displayed on the Environments list page
   - **Display Order**  The order in which environments are presented when provisioning, a value of “0” will position the environment at the top of the list
   - **Visibility**
     - *Private:* Available only in the Tenant the environment is created in
     - *Public:* Available for all Tenants. Public is only applicable for environments created in the the Master Tenant.

**Note:** User-created environments can be edited, hidden, or removed from the Actions menu on the environments list page. Morpheus-default environments can only be hidden from users during provisioning.

Overview

The License section is for automating the application of Licenses to Instances while provisioning. Licenses can be added to Morpheus and then attached to images. Morpheus will then apply the license to Instances provisioned using the images with license attached. Licenses can be configured for single or multiple Tenants.

Creating Licenses

1. Select + Create License
2. In the New License modal, enter the following:
   - **License Type**  Windows
   - **Name**  Name of the License in Morpheus
   - **License Key**  Enter the License Key
   - **Org Name**  The Organization Name (if applicable) related to the license key
   - **Full Name**  The Full Name (if applicable) related to the license key
   - **Version**  The License Version
   - **Copies**  The Number of copies available on the License
• **Description** License description displayed in the Licenses list in Morpheus, helpful for identifying the License after creation

• **Virtual Images**

  Search for existing Virtual Images by name and select to attach the image to the license.

  Note: Virtual Images are synced from Clouds or added in the Library > Virtual Images section.

• **Tenant Permissions** Search for and select the Tenant(s) the License will be available for. Multiple Tenants can be added.

  3. Save Changes

**Provisioning with Licenses**

When a Virtual Image is added to a license, Morpheus will automatically apply the License to Instances configured with the Virtual Image during provisioning, including Instance Types with a Node Type that is configured with the Virtual Image, or if the image is selected when using generic Cloud Instances types (VMware, AWS, Nutanix, Openstack etc). Virtual Images can be removed from a License by editing the License.

**Managing Licenses**

Created Licenses details are displayed in the License page, including the number of copies applied per License, the Tenants added to the License, and the Virtual Images attached to the License.

The Name, Version, Copies, Description, Virtual Images and Tenant Permissions are editable but selecting the **Actions** dropdown on a License.

Note: License Types, Keys, Org Names and Full Names are not editable after a license has been created.

License can also be removed using the **Actions** dropdown on a License.

**App Blueprint Settings**

Determines the Default Blueprint Type selected in new App Wizard

- Morpheus
- ARM Template
- CloudFormation
- Terraform
- Kubernetes Spec
- Helm Chart
**Terraform Settings**

- **Terraform Runtime**: Select “auto” or “manual”. When selecting “auto”, Morpheus will automatically download and use the Terraform version indicated in the VERSION field on the Spec Templates that make up a Terraform Instance type or Blueprint. When selecting “manual”, Morpheus will use the version of Terraform installed on your appliance.

**9.9.4 Monitoring**

**Morpheus Monitoring Settings**

- **Auto Create Checks**: When enabled a Monitoring Check will automatically be create for Instances and Apps.

- **Availability Time Frame**: The number of days availability should be calculated for. Changes will not take effect until your checks have passed their check interval.

- **Availability Precision**: The number of decimal places availability should be displayed in. Can be anywhere between 0 and 5.

- **Default Check Interval**: The default interval to use when creating new checks.

*Note*: Monitoring Checks can be manually configured if Auto Create Checks is disabled.

**AppDynamics**

AppDynamics Monitoring Integration Settings

- **Enabled**: Enables the AppDynamics Integration

- **Controller Host**: This is the host name or the IP address of the AppDynamics Controller. This is the same host that you use to access the AppDynamics browser-based user interface.

- **Controller Port**: This is the HTTP(S) port of the AppDynamics Controller. This is the same port that you use to access the AppDynamics browser-based user interface. If the Controller SSL Enabled property is set to true, specify the HTTPS port of the Controller; otherwise specify the HTTP port.

- **Controller SSL Enabled**: This property specifies whether the agent should use SSL (HTTPS) to connect to the Controller. If SSL Enabled is true, set the Controller Port property to the HTTPS port of the Controller.

- **Tenant Name**: This is the account name used to authenticate with the Controller.

- **Access Key**: This is the account access key used to authenticate with the Controller.

- **Controller Version**: This is the controller version and can be obtained at the bottom of the controller login page.

- **Application Name**: This is the name of the logical business application. Note that this is not the deployment name(ear/war/jar) on the application server. (Maximum of 30 numbers or letters)

- **Tier Name**: This is the name of the logical tier. (Maximum of 30 numbers or letters)

- **Controller User**: A user that can login to the Controller ui and upload a dashboard.

- **Controller Password**: Password for the Controller User.
Service Now

ServiceNow Monitoring Integration Settings

Note: A ServiceNow Integration must be already configured in Administration > Integrations to enable the ServiceNow Monitoring Integration.

Enabled Enables the ServiceNow Monitoring Integration
Integration Select from a ServiceNow Integration added in Administration > Integrations
New Incident Action The Service Now action to take when a Morpheus incident is created.
Close Incident Action The Service Now action to take when a Morpheus incident is closed.

Incident Severity Mapping

<table>
<thead>
<tr>
<th>Morpheus Severity</th>
<th>ServiceNow Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Info</td>
<td>Low/Medium/High</td>
</tr>
<tr>
<td>Warning</td>
<td>Low/Medium/High</td>
</tr>
<tr>
<td>Critical</td>
<td>Low/Medium/High</td>
</tr>
</tbody>
</table>

New Relic

New Relic Integration Settings

Enabled Enables the New Relic Monitoring Integration
License Key License Key to be used when installing the New Relic agent in order for the agent to report data to your New Relic account

Note: The License Key is the 40-character hexadecimal string that New Relic provides when you sign up for your account.

9.9.5 Backups

Backup Settings

The Backup settings page allows you to enable or disable scheduled backups, select a default backup bucket, and administer global settings related to backups. Changes to global settings only affect new backups going forward and do not affect existing backups.
Morpheus Backup Settings

Scheduled Backups  Enable automatic scheduled backups for provisioned instances

Create Backups  When enabled, Morpheus will automatically configure instances for manual or scheduled backups

Backup Appliance  When enabled, a backup will be created for the Morpheus appliance database. Select the Backup text link to view or edit settings related to the appliance backup

Default Backup Bucket  Select an existing bucket as the default for future backup runs. Click the Infrastructure Storage text link to add a new storage bucket to Morpheus if needed

Default Backup Schedule  Choose a default schedule interval for automated backups. The available selections in this dropdown menu are Execution Schedules defined in Library > Automation > Execute Scheduling

Default Backup Retention  Choose the default number of backups to be retained for automated Instance and appliance backup jobs

9.9.6 Logs

Logging Settings

Overview

Morpheus contains a built-in logging solution that aggregates logs from hosts and services. Logs are displayed, searchable, and filterable in the Instance, App, Host and overall Logs sections. Logs can also be forwarded using Syslog Forward rules to any external solution that supports syslogs.

The logs displayed in the Instance, App, Host and overall Logs sections are only from Managed VMs and Hosts that have the Morpheus agent installed. Instances can be configured to show additional logs by configuring the LOG FOLDER in the Library NODE TYPE. Logs from any .log file in the specified folder will be forwarded by the Morpheus agent to the Morpheus appliance or forwarded with Syslog Forward rules.

Note:  The Logs section does not contain Morpheus appliance logs, which can be found in /var/log/morpheus/ and in Administration - Health.

Logs are stored in ElasticSearch and retention can be set by adjusting the Availability Time Frame in the Administration > Settings > Logs section.

Logging Settings for the built-in logging and syslog forwards are also configurable in the Administration > Settings > Logs section.
Morpheus guidance is an important tool that makes recommendations for resource and cost optimization. It analyzes CPU, memory, and storage activities over time to make intelligent recommendations on sizing and power state. These recommendations can free up resources and save organizations significant amounts of money over time. Out of the box, Morpheus is configured for sensible thresholds used in making these recommendations but they can be edited here if needed.

### Power Settings

Morpheus will recommend shutting down a resource if *all* three of the baselines in this section are exceeded:

- **Average CPU (%):** Shutdown will be recommended if the average CPU usage is below this value. Values over 100% are possible as this value factors the number of CPU cores. Default value: 75

- **Maximum CPU (%):** Shutdown will be recommended if the CPU usage never exceeds this value. Values over 100% are possible as this value factors the number of CPU cores. Default value: 500

- **Network Threshold (bytes):** Shutdown will be recommended if the average network bandwidth is below this value. Default value: 2000 bytes/second

### 9.9.7 Guidance

**Overview**

Morpheus guidance is an important tool that makes recommendations for resource and cost optimization. It analyzes CPU, memory, and storage activities over time to make intelligent recommendations on sizing and power state. These recommendations can free up resources and save organizations significant amounts of money over time. Out of the box, Morpheus is configured for sensible thresholds used in making these recommendations but they can be edited here if needed.
CPU Up-size Settings

CPU up-size will be recommended when both of the following baselines are exceeded for a resource:

- **Average CPU (%)**: CPU up-size is recommended if the average CPU percentage exceeds this value (and other criteria are also met). Default value: 50
- **Maximum CPU (%)**: CPU up-size is recommended if the maximum CPU percentage exceeds this value. Default value: 99

Memory Up-size Settings

Memory up-size will be recommended when both of the following thresholds are met for a resource:

- **Minimum Free Memory (%)**: Memory up-size will be recommended if free memory dips below this value. Default value: 10

Memory Down-size Settings

Memory down-size will be recommended when both of the following thresholds are met for a resource:

- **Average Free Memory (%)**: Memory down-size is recommended if the average free memory is above this value. Default value: 60
- **Maximum Free Memory (%)**: Memory down-size is recommended if free memory has never dipped below this value. Default value: 30

9.9.8 Environments

Overview

The Environments section is where you create and manage your environment labels, which are available in the Environment dropdown during Instance or App provisioning. An Instance’s environment label can be changed by editing the Instance.

Creating Environments

1. Select + Create Environment
2. Populate the following for the New Environment:
   - **Name**: The friendly name for the environment in Morpheus
   - **Code**: Shortcode used for API and CLI
   - **Description**: Environment description displayed on the Environments list page
   - **Display Order**: The order in which environments are presented when provisioning, a value of “0” will position the environment at the top of the list
   - **Visibility**
     - **Private**: Available only in the Tenant the environment is created in
     - **Public**: Available for all Tenants. Public is only applicable for environments created in the the Master Tenant.
Note: User-created environments can be edited, hidden, or removed from the Actions menu on the environments list page. Morpheus-default environments can only be hidden from users during provisioning.

9.9.9 Software Licenses

Overview

The License section is for automating the application of Licenses to Instances while provisioning. Licenses can be added to Morpheus and then attached to images. Morpheus will then apply the license to Instances provisioned using the images with license attached. Licenses can be configured for single or multiple Tenants.

Creating Licenses

1. Select + Create License
2. In the New License modal, enter the following:
   - **License Type** Windows
   - **Name** Name of the License in Morpheus
   - **License Key** Enter the License Key
   - **Org Name** The Organization Name (if applicable) related to the license key
   - **Full Name** The Full Name (if applicable) related to the license key
   - **Version** The License Version
   - **Copies** The Number of copies available on the License
   - **Description** License description displayed in the Licenses list in Morpheus, helpful for identifying the License after creation
   - **Virtual Images**
     
     Search for existing Virtual Images by name and select to attach the image to the license.

     Note: Virtual Images are synced from Clouds or added in the Library > Virtual Images section.

   - **Tenant Permissions** Search for and select the Tenant(s) the License will be available for. Multiple Tenants can be added.
3. Save Changes
Provisioning with Licenses

When a Virtual Image is added to a license, Morpheus will automatically apply the License to Instances configured with the Virtual Image during provisioning, including Instance Types with a Node Type that is configured with the Virtual Image, or if the image is selected when using generic Cloud Instances types (VMware, AWS, Nutanix, Openstack etc). Virtual Images can be removed from a License by editing the License.

Managing Licenses

Created Licenses details are displayed in the License page, including the number of copies applied per License, the Tenants added to the License, and the Virtual Images attached to the License.

The Name, Version, Copies, Description, Virtual Images and Tenant Permissions are editable but selecting the Actions dropdown on a License.

Note: License Types, Keys, Org Names and Full Names are not editable after a license has been created.

License can also be removed using the Actions dropdown on a License.

9.9.10 License

Overview

Morpheus requires a valid license for provisioning new Instances, Apps and Hosts, and converting existing Instances and Hosts to managed. Licenses can be applied and updated in this section, and the current license status can be checked.

Note: Morpheus is licensed for a certain number of concurrent workload elements (WLEs) that may be managed or inventoried at any one time. See our Knowledge Base for specific information on the types of WLEs that count against Morpheus licensing.

Current License

If a License Key has already been applied, the License status is shown in the Current License section:

Tenant Name  Company name the License was generated for.
Start Date  Date and time the current License started.
End Date  Date and time the current License expires.
Space  Amount of used and unused Managed RAM under the current License.

EXAMPLE: On a 1 TB License with 182 GB of RAM under management, the Space section will show Used Space 182.9GB Unused Space 841.0GB

Note: Once a current License expires or has reached its Space limit, users will no longer be able to provision new Instances, Apps, Hosts, or Bare Metal, or convert existing Hosts, Virtual Machines, or Bare Metal to managed. Morpheus will otherwise continue to function.
Upgrade License Key

To add a new or update an existing License:

1. Copy the License Key into the License Key field
2. Click UPDATE

If valid, the new License will be applied.

Request new License

Licenses can be requested at https://morpheushub.com, or by contacting support@ or sales@ morpheusdata.com.

9.9.11 Utilities

System administrators have access to a utilities panel with the following options:

- Reindex all searchable data: Execute
- Toggle Maintenance Mode: Enable

Note: Maintenance mode cleanly places Morpheus into a state where maintenance can be performed on the appliance. This drains any active sessions and queues so an auto-scaling group can scale down. It also drains active sessions across services. Restarting Morpheus UI disables maintenance mode.

9.10 User Settings

User settings are accessed by clicking on your display name in the far upper-right corner of the application window. In this dropdown menu, click on the “USER SETTINGS” link.

9.10.1 User Photo

Upload a custom image for your user avatar that is displayed in the top header and user administration sections. Suggested Photo Dimensions: 128 x 128

9.10.2 User Settings

The fields included in this section are described below. By entering any new values in these fields and clicking SAVE, the existing value will be overwritten.

- Username: Your Morpheus username
- First Name: Your first name (together with Last Name makes up your display name)
- Last Name: Your last name (together with First Name makes up your display name)
- Email: Your email address
- Password: Enter a value and save changes to update your password. The value in the Confirm field below must match
- Confirm: Confirm the new password you’ve entered
• **RECEIVE NOTIFICATIONS** Determines if Provisioning notifications are emailed to this User.

User Photo

![User Photo](image)

**Suggested Photo Dimensions:**
128 x 128

[UPLOAD PHOTO]

User Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>morphUser</td>
</tr>
<tr>
<td>First Name</td>
<td>morpheus</td>
</tr>
<tr>
<td>Last Name</td>
<td>user</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:morpheus@morpheus.cloud">morpheus@morpheus.cloud</a></td>
</tr>
<tr>
<td>Password</td>
<td>***************************</td>
</tr>
<tr>
<td>Confirm</td>
<td>***************************</td>
</tr>
</tbody>
</table>

[RECEIVE NOTIFICATIONS]

[API ACCESS]
9.10.3 2 Factor Authentication

Morpheus supports two-factor authentication (2FA) for local user accounts as well as those authenticating through Active Directory and LDAP identity sources. Authentication is handled through a 2FA app such as Authy or Google Authenticator. Other common methods for handling 2FA, such as through email or SMS text message are not currently supported. Two-factor authentication is handled on a per-user basis through the User Settings section. There is not currently a way for an administrator to enforce the use of two-factor authentication appliance-wide.

Setting Up Two-Factor Authentication

When two-factor authentication isn’t yet set up, this section contains a single button: ENABLE 2FA. To get started, click this button and Morpheus will prompt for your password. After entering the password, you’ll be shown a QR code which can be scanned into your authenticator application of choice. Once the QR code is shown, 2FA is active and the supplemental code will need to be entered each time the user logs in.

On subsequent login attempts, the user will be prompted to enter a 2FA code after successful entry of the username and password. Retrieve this code from the 2FA app you set up in the prior section and enter it to complete the login process.
Disabling Two-Factor Authentication

When two-factor authentication is set up, this section contains two buttons: DISABLE 2FA and GET 2FA CODE. To generate a new QR code and configure an authenticator app, click GET 2FA CODE. Once you generate a new QR code, the old one is no longer valid. At that point you must reconfigure your authenticator app or you will not be able to access your account on the next login attempt. Generating a new QR code requires your password.

To disable 2FA, click DISABLE 2FA. This action does not require a password.

Handling User Lock-Out

If a user loses the device they’ve configured for authentication or if they cannot proceed through 2FA login for any other reason, an administrator should impersonate the user’s account, reset their password, disable 2FA, then share the new temporary password with the user. At that point, the user can login, reset their password to something more secure, and re-enable 2FA (if desired).

9.10.4 Preferences

- **Default Group**: Sets the default Group selection when provisioning
- **Default Cloud**: Sets the default Cloud selection when provisioning
- **Default Persona**: Sets the default Persona used when logging in
- **Default Locale**: Sets the user’s preferred language and region, this setting will override the global locale for the individual user

### Preferences

<table>
<thead>
<tr>
<th>Preferences</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Group</td>
<td>Labs</td>
</tr>
<tr>
<td>Default Cloud</td>
<td>Azure Labs</td>
</tr>
<tr>
<td>Default Persona</td>
<td>Standard</td>
</tr>
</tbody>
</table>

9.10.5 Linux Settings

When provisioning a Linux-based resource and opting to have your user created during the provisioning process, the credentials entered in this section will be used to seed that user into the provisioned resource.

- **Username**: The username that will be used with your Linux user
- **Password**: The password that will be used with your Linux user (optional if specifying key)
- **Confirm**: Confirm your entered password. These must match in order for the new password value to be saved
• **SSH Key**: Select a pre-existing SSH key pair object in Morpheus. Required if not specifying password and creating your user during provisioning, or required if ssh password authentication has been disabled.

**Warning**: If your users Linux Settings password and/or key are not defined, and ‘Create User” is enabled during provisioning (default), a random password will be generated but not exposed and you will not be able to login with your user.

### Linux Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>morphUser</td>
</tr>
<tr>
<td>Password</td>
<td>✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧�</td>
</tr>
<tr>
<td>Confirm</td>
<td>✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧✧�</td>
</tr>
<tr>
<td>SSH Key</td>
<td>morpheus-3-D4XB8L</td>
</tr>
</tbody>
</table>

### 9.10.6 Windows Settings

When provisioning a Windows-based resource and opting to have your user created during the provisioning process, the credentials entered in this section will be used to seed that user into the provisioned resource.

- **Username**: The username that will be used with your Windows accounts
- **Password**: The password that will be used with your Windows accounts
- **Confirm**: Confirm your entered password. These must match in order for the new password value to be saved.

**Warning**: If your users Windows Settings password is not defined, and ‘Create User” is enabled during provisioning (default), a random password will be generated but not exposed and you will not be able to login with your user.
9.10.7 API Access

Click the *API Access* button to expand the “API ACCESS” modal. In this modal you can generate or refresh access tokens that can be used with Morpheus API and Morpheus CLI.

If no token yet exists for a particular “CLIENT ID”, click *ACTIONS* and then Generate. If a token has expired, we can also regenerate that token by clicking *ACTIONS* and then Regenerate. After regenerating a particular token, you would need to ensure any scripts using those tokens are updated.

- **morph-api**: Used for Morpheus API access and should be the default token-type used
- **morph-cli**: Used for Morpheus CLI access
- **morph-automation**: Used by the internal Task engine and by jRuby-type Tasks to make API calls. It shouldn’t be used externally for other types of access or in external automation. It is surfaced in the UI so users can see if a token exists and can clear it when necessary
- **morph-customer**: This token is available for legacy implementations and was previously recommended for custom API access (similar to the morph-api token). It’s not recommended for use but is still available to maintain support for legacy custom automation which may still be in use on customer sites

After navigating away from the User Settings page, the complete access and refresh tokens will be masked from view. If these are lost or compromised, you can eliminate a token completely by clicking *ACTIONS* and then Clear. If you need to generate a new token for the same Client ID, click *ACTIONS* and then Regenerate.
**Note:** Access Tokens are only displayed/available after generation. Copy new Tokens and store appropriately before navigating from `/user-settings`, they will not be displayed again.
Personas are alternate views in Morpheus UI. A user’s access to the various Personas is controlled by Role permissions. At present, there are three Persona types: Standard, Service Catalog, and Virtual Desktop. The Standard Persona is the typical default view. The Service Catalog Persona is a simplified view where users are presented with pre-configured Instance types, Blueprints, and Workflows to choose from based on their Role. The Virtual Desktop Persona allows administrators to grant user access to remote workstations and applications.

The rest of this section goes through the use of the Service Catalog Persona and Virtual Desktop Persona in greater detail, including how administrators can curate catalog item and virtual desktop selections for their users.

### 10.1 Service Catalog Persona

The Service Catalog Persona presents a simplified catalog where users can select and deploy Instances or Blueprints with pre-defined configuration with just a few clicks and without presenting an overwhelming list of options.

#### 10.1.1 Configuring Catalog Item Access

Within the Service Catalog Persona, users are presented with Catalog Items based on their User Role. Additionally, Catalog Item access can be set on the Tenant Role to restrict certain items from all users in the Tenant. By default, User Roles have no access to any catalog items (and no access to the Service Catalog Persona). When enabling Service Catalog Persona access for User Roles, you will also need to give access to some or all Catalog Items.

Configuring Global Access:

- **Full**: Gives access to all Catalog Items
- **Custom**: Gives access to individually-selected items from the list below
- **None**: No access is given to any Catalog Items

**Tip:** When giving Custom access, be sure to set access on some of the individual catalog items to Full in order to reveal those items to the Role group.
10.1.2 Dashboard

The default page for the Service Catalog Persona is the Dashboard. The Dashboard shows a selection of featured catalog items, a listing of the last few items the user has ordered, and a selection from the user’s inventory.

10.1.3 Catalog

The catalog shows the complete list of pre-defined catalog items available to the user for provisioning. Catalog items are not created in the Service Catalog Persona. For more on creating catalog items, see the Self Service section (Tools > Self Service) of Morpheus docs.
10.1.4 Inventory

The Inventory Page reveals the complete list of items which have been ordered by the user and provisioned. Users will only see their own items in this section.
10.1.5 Inventory Detail

Access the detail page for an item in your inventory by clicking the View Details link. The page displayed will look very similar to an Instance or App detail page in the Standard Persona. Highly detailed information on the health of the Instance or App are shown here. We can also take actions against Instances such as running Tasks or Workflows, reconfiguring the Instance, controlling the power state, and more.

10.1.6 Placing Orders

From the Catalog page, select the tile for your chosen item to see any custom options that may need to be set prior to provisioning.
Once the item is in the cart, make any additional selections to complete the order. Once finished, proceed to the cart by clicking on the cart icon at the top of the application window. Click “Review Order”. When reviewing your order, each selected item is listed along with its estimated cost. The total estimated cost for the entire order is also computed.

Once PLACE ORDER is clicked, the provisioning process will begin and the user is redirected back to the catalog page. Any new orders can be viewed in Inventory and additional details can be accessed through the Inventory item detail page.
10.2 Virtual Desktop Persona

The Morpheus VDI Persona provides a virtual desktop environment to grant users access to workstations and applications in a secure manner. Deploy pools of virtual machines on any supported Morpheus Cloud for users to reserve and use! Morpheus leverages open source client technologies, such as Apache Guacamole, to provide a performant and secure virtual desktop client for the end user while wrapping its frontend in a completely new framework. For information on configuring VDI pools for consumption in the Virtual Desktop Persona, see the Tools section of Morpheus docs.

Note: This is not an integration with existing VDI Pool Managers such as VMWare Horizon, Citrix VDI, or Nutanix XiFrame. It is a standalone Morpheus feature.
10.2.1 Key Features

- VDI Pool Management
- Virtual Desktop Persona
- RDP/SSH/VNC Console Support
- RDP Remote App Support
- Clipboard Copy/Paste
- HiDPI Support
- Auto Compression Scanning based on User Bandwidth
- Audio Playback (RDP)
- Local Printer (RDP)
- Auto-Resize
- Auto-Login based on Morpheus User Settings
- Customizable User Background

10.2.2 Configuring Access to the Virtual Desktop Persona

Access to the Virtual Desktop Persona and individual VDI pools is handled through the user Role and, where applicable, Tenant Role. When creating a new Role, access is restricted to the Virtual Desktop Persona and all VDI pools by default. To grant access:

1. Navigate to the Role (Administration > Roles > Selected Role)
2. Access the Personas tab
3. Toggle the Virtual Desktop permission to “Full” or “None”
4. Access the VDI Pool Access tab
5. Toggle access to selected VDI pools to “Full” or “None”, you can also toggle permission on all pools to “Full” or “None” with the Global Access selection
6. Role changes are saved automatically, there is no need to manually save

10.2.3 Launching a VDI Instance

VDI Instances are launched from the Virtual Desktops Persona. Depending on Role permissions, your account may default to this view or may even restrict you solely to this view. To access the Virtual Desktops Persona from the standard view or from another Persona, click on the user’s name in the upper-right corner of the application window. When available, this dropdown menu will list the standard Morpheus Persona view as well as any other Personas the user has permission to access. Click on Virtual Desktop to access the Virtual Desktop Persona.

The Virtual Desktop Persona view lists out each of the virtual desktop types they can access. Click on the desired virtual desktop type to launch it. If there are virtual apps available for any listed desktop types, they are presented in a flyout menu alongside a “desktop” option to access the base OS over an individual app. Items categorized as “Desktops” are VDI pools configured in the Tools menu of the Standard Persona. Items categorized as “Instances” are Instances favored by the current user in the Standard Persona (if they have access and they have favorited any Instances). Clicking on an Instance tile offers quick access to the Instance console.
**Important:** Virtual Desktops are launched in a pop-up window. Be sure your web browser is not blocking pop-ups or create an appropriate exception for Morpheus virtual desktop pop-ups.

### 10.2.4 Changing the Virtual Desktop Persona Background

The Morpheus Virtual Desktop Persona includes default backgrounds for an elegant look out of the box. If desired, users may change this background to suit personal taste or organizational branding. This change is unique to each individual account. At this time, there is no option for appliance-wide whitelabeling for Virtual Desktop Persona backgrounds.

1. Click on the user’s name in the far upper-right corner of the application window
2. Click USER SETTINGS
3. The section for “VDI Settings” is in the lower-right corner of the page
4. Mark the RESET box and click SAVE to reset the Virtual Desktop Persona to the default background
5. Click “Browse” and upload a local image to add a custom background
6. Click SAVE

### 10.3 Configuring Persona Access

Access to Personas is controlled by a user’s Role. Additionally, Persona access can be configured on the Tenant Role to set maximum Persona access for any user in the Tenant. By default, new Roles and Roles that existed prior to the creation of Personas will only have access to the Standard Persona. If desired, new Roles can be configured to have access to one or both Personas and existing Roles can be edited in the same way.

**Tip:** It’s recommended to set access to all Personas to “None” if you intend not to use Personas at all. Under this configuration, Morpheus gives access only to the Standard Persona and hides the Persona selection menu from the user. New Roles and Roles that existed prior to creation of the Personas feature are pre-configured in this way.

Edit Persona access on a Role with the following steps:

1. Navigate to Administration > Roles
2. Select the desired Role to edit
3. Go to the Personas tab
4. Allow access to one or both Personas as needed, changes are saved automatically
Switch Personas by clicking on your name in the upper-right corner of the application window. If your Role gives you access to any additional Personas, they will be listed here.
11.1 Ansible Troubleshooting

When a workflow is executed manually, the Ansible run output is available in the Instance History tab. Select the i bubble next to the Ansible task to see the output. You can also see the run output in UI logs at `/var/log/morpheus/morpheus-ui/current`. These can be tailed by running `morpheus-ctl tail morpheus-ui`.

11.1.1 Verify Ansible is installed on the Morpheus Appliance

Ansible should be automatically installed but certain OS or network conditions can prevent the automated install. You can confirm installation by running `ansible --version` in the Morpheus appliance, or by viewing the Ansible integration details page (Administration > Integrations > Select Ansible Integration). We also see it in the Ansible tab of a Group or Cloud scoped to Ansible, just run `--version` as ansible is already included in the command.

If Ansible is not installed

Follow these instructions to install, or use your preferred installation method

Ubuntu:

```
sudo apt-get install software-properties-common
dsud apt-add-repository ppa:ansible/ansible
sudo apt-get update
sudo apt-get install ansible python-requests
```

CentOS:

```
sudo yum install epel-release
sudo yum install ansible python-requests
```

Then create the working Ansible directory for Morpheus:

```
sudo mkdir /opt/morpheus/.ansible
sudo chown morpheus-app.morpheus-app /opt/morpheus/.ansible
```
11.1.2 Validate Git repo authorization and the configured paths

The public and private SSH keys need to be added to the Morpheus appliance via Infrastructure > Keys & Certs and the public key needs to be added to the Git repo via user settings. If both are set up correctly, you will see the playbooks and roles populate in the Ansible Integration details page.

The Git Ref field on playbook tasks is to specify a different git branch than default. It can be left to use the default branch. If your playbooks are in a different branch you can add the branch name in the Git Ref field.

When running a playbook that is in a workflow, the additional playbooks fields do not need to be populated, they are for running a different playbook than the one set in the Ansible task in the Workflow, or using a different Git Ref.

**Note:** If you are manually running Workflows with Ansible tasks on existing Instances through Actions > Run Workflow and not seeing results, set the Provision Phase on the Ansible task to Provision as there may be issues with executing tasks on other phases when executing manually.

11.2 Attaching Logs to Case

When submitting a case it is critical to attach the relevant logs. The logs can be found at /var/log/morpheus/morpheus-ui/current. Logs can be attached to the case at anytime.

When submitting logs please reproduce the error right before capturing and sending the log file. This will ensure the activity that took place and resulted in an error is contained in the logs.

Log rotation takes the current file each night or after it’s a certain size and compresses them. The *.*.s files in the current directory are rotated and zipped logs that can be sent as is.

The logs can also be captured from the Morpheus UI. Under Administration > Health > Morpheus Logs. Please copy relevant logs and add to case as an attachment.
11.3 Blank Dashboard

Problem: A blank dashboard or 500 error after installing morpheus

Note: A blank or 500 error on just the dashboard is different than the entire morpheus-ui not loading. Please see UI note loading article for troubleshooting the ui not loading after an upgrade.

Cause: Elasticsearch restarting prior to being fully bootstrapped during the initial install.

Solution: To fix, purge elasticsearch by running the following on the Morpheus Appliance:

```bash
curl -XDELETE http://localhost:9200/*
morpheus-ctl restart elasticsearch
morpheus-ctl restart morpheus-ui
```

Another option is:

```bash
sudo rm -rf /var/opt/morpheus/elasticsearch/data/morpheus
morpheus-ctl restart elasticsearch
morpheus-ctl restart morpheus-ui
```

If you get a term/timeout on ui restart, run

```bash
morpheus-ctl kill morpheus-ui
morpheus-ctl start morpheus-ui
```

Note: The morpheus-ui may take a few minutes to load and be available after being restarted

11.4 CLI Troubleshooting

If you have installed the Morpheus CLI successfully and get a successful login but see this error Error Communicating with the Appliance. SSL_connect returned=1 errno=0 state=error: certificate verify failed

run the command

```bash
morpheus remote update {appliancename} --insecure
```

11.5 Cannot Login

11.5.1 Forgot password

If a user forgets their password, they can use the FORGOT PASSWORD? link on the login page. They can then enter their username or email address to send a reset password email to the email address defined on the user.

If the default or user added SMTP server is not functioning or blocked, a System Admin user can impersonate that user and update their password.

If the System Admin user password needs to be reset and the default or user added SMTP server is not functioning or blocked, please contact Morpheus support for assistance.
11.5.2 Sub-Tenant user cannot login after 3.4.0 upgrade

Morpheus v3.4.0 added support for all subtenant users to login via the main tenant url using subtenant id or subdomain prefix, ie `tenantId\username` or `subdomain\username`.

**Note:** Tenant subdomains can be defined by editing Tenant settings and updating the *SUBDOMAIN* field.

**Important:** Subtenant local users will no longer be able to login from main login url without using their subtenant id or subdomain prefix.

The login requirements were added in v3.4.0 to allow subtenant users with identity source integration generated user accounts to be able to login to the master tenant, gain API and CLI access, and remove the requirement for usernames to be unique across all tenants.

Previously subtenant users that had local/morpheus generated user accounts could login to their tenant via the master tenant url, while subtenant users that had identity source integration generated user accounts had to use the subtenant specific login url.

In v3.4.0+ all subtenant users can login via the master tenant url by specifying their tenant id or subdomain prefix, \, then username. Subtenants can still use the tenant specific login url as well.

**Example:** I have a username `subuser` that belongs to a tenant with the subdomain `acme` and tenant id `58`. When logging in from the main login url, I now need to enter in: `acme\subuser` and the password. Alternatively the tenant ID can be used, ie `58\subuser`

11.5.3 Active Directory user suddenly cannot Login

In Morpheus v3.4.0 and prior, OU changes in Active Directory can disable logins for AD users who had previously authenticated/have existing user accounts in Morpheus. If an Active Directory user cannot login to Morpheus after their OU was changed in AD, please contact Morpheus support for a resolution. The OU association for the user(s) can also be manually updated in the database. This issue is resolved in Morpheus versions 3.4.1 and higher.
11.6 Common Ports & Requirements

The following chart is useful for troubleshooting Agent install, Static IP assignment, Remote Console connectivity, and Image transfers.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Method</th>
<th>OS</th>
<th>Source</th>
<th>Destination</th>
<th>Port</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Communication</td>
<td>All</td>
<td>All</td>
<td>Node</td>
<td>Appliance</td>
<td>443</td>
<td>DNS Resolution from node to appliance url</td>
</tr>
<tr>
<td>Agent Install</td>
<td>All</td>
<td>Linux</td>
<td>Node</td>
<td>Appliance</td>
<td>80</td>
<td>Used for appliance yum and apt repos</td>
</tr>
<tr>
<td>SSH</td>
<td>Linux</td>
<td>Node</td>
<td>Appliance</td>
<td>Node</td>
<td>22</td>
<td>DNS Resolution from node to appliance url</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Virtual Images configured</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SSH Enabled on Virtual Image</td>
</tr>
<tr>
<td>WinRM</td>
<td>Windows</td>
<td>Windows</td>
<td>Appliance</td>
<td>Node</td>
<td>5985</td>
<td>DNS Resolution from node to appliance url</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Virtual Images configured</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>WinRM Enabled on Virtual Image(\texttt{winrm quickconfig})</td>
</tr>
<tr>
<td>Cloud-init</td>
<td>Linux</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Cloud-init installed on template/image</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Cloud-init settings populated in User Settings or in \texttt{Admin \rightarrow Provisioning}</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Agent install mode set to Cloud-Init in Cloud Settings</td>
</tr>
<tr>
<td>Cloudbase-init</td>
<td>Windows</td>
<td>Windows</td>
<td>Appliance</td>
<td></td>
<td></td>
<td>Cloudbase-init installed on template/image</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Cloud-init settings populated in User Settings or in \texttt{Admin \rightarrow Provisioning}</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Agent install mode set to Cloud-Init in Cloud Settings</td>
</tr>
<tr>
<td>VMtools</td>
<td>All</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>VMtools installed on template</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Cloud-init settings populated in Morpheus user settings or in \texttt{Administration \rightarrow Provisioning} when using Static IP’s</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Existing User credentials entered on Virtual Image</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>when using DHCP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RPC mode set to VMtools in VMware cloud settings.</td>
</tr>
<tr>
<td>Static IP Assignment &amp; IP Pools</td>
<td>Cloud-Init</td>
<td>All</td>
<td></td>
<td></td>
<td></td>
<td>Network configured in Morpheus (Gateway, Primary and Secondary DNS, CIDR populated, DHCP disabled)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Cloud-init/Cloudbase-init installed on template/image</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Cloud-init settings populated in Morpheus user settings or in \texttt{Administration \rightarrow Provisioning}</td>
</tr>
</tbody>
</table>
11.7 Deleting Instances

It is important to know the difference between deleting an Instance from the Provisioning section, and deleting a VM from the Infrastructure section.

**Important:** Deleting an Instance a with Virtual Machines in it will always try to delete the actual Virtual Machines.

Instances are managed resources that may have one or multiple Virtual Machines associated. Since the VMs in the Instance are managed by Morpheus, deleting an Instance with a Virtual Machines in it will always try to delete the actual Virtual Machines.

There are scenarios where deleting, or attempting to delete the associated Virtual Machines is not desired:

- The Instance needs to be deleted, but the actual Virtual Machines need to remain.
- The actual Virtual Machines have already been deleted outside of Morpheus, so only the orphaned records in Morpheus need to be removed.

### 11.7.1 Deleting an Instance without deleting Infrastructure

It is not possible to delete an Instance from the Provisioning section without removing the associated Infrastructure/VMs. However, this can be accomplished from the Infrastructure section by deselecting “Remove Infrastructure” when deleting the VM:

1. Navigate to the Virtual Machine record by clicking on the VM name in the Virtual Machines section of the Instance detail page or by navigating to Infrastructure > Compute > Virtual Machines and selecting the VM.
2. Click “DELETE”
3. In the delete confirmation modal:
   - Uncheck “Remove Infrastructure”
   - Check “Remove Associated Instances”
Important: Ensure “Remove Infrastructure” is NOT checked if you do not want to delete the actual Virtual Machine.

4. Select DELETE

This will delete the Virtual Machine record as well as the Instance record but leave the Infrastructure/VM in place. If the VM is in a Cloud that is being inventoried, it will sync back into Morpheus after the next Cloud refresh. You can disable automatic Cloud inventory by editing the Cloud (Infrastructure > Clouds > selected Cloud > EDIT button) and turning off this feature.

11.7.2 Deleting an Instance/VM that does not exist anymore

Deleting a managed resource outside of Morpheus is not recommended as it will leave stranded record in Morpheus and cause deleting the records in Morpheus to get stuck on delete when Morpheus tries to remove infrastructure that is no longer there.

To select an Instance and/or VM record in Morpheus for a Virtual Machine that no longer exists:

1. Navigate to the Virtual Machine record by clicking on the VM’s name in the Virtual Machines section in the Instances details section, or by navigating to Infrastructure > Compute - Virtual Machines and selecting the VM.
2. Click “DELETE”
3. In the delete confirmation modal:
   • Uncheck “Remove Infrastructure”
   • Check “Remove Associated Instances”
**Important:** Ensure “Remove Infrastructure” is NOT checked. If it is checked, Morpheus will try to delete the actual VM, and since it is not there anymore, the delete will not complete successfully since Morpheus will not be able to verify successful deletion of the Infrastructure.

4. Select DELETE

The key point is when deleting an Instance, or when selecting “Remove Infrastructure” when deleting a VM record, Morpheus will always try to remove the Infrastructure. If the Infrastructure/VM no longer exists, or you do not want to remove it, simply delete from the Infrastructure section and uncheck “Remove Infrastructure”.

**Note:** When deleting a managed VM, if that VM is the only VM inside the associated Instance, the Associated Instance must also be removed. Additionally, when removing Instances, even if the infrastructure is not removed, some related teardown tasks are still performed. These can include removing IP addresses or IPAM integration entries, deletion of Active Directory objects, and any Teardown-phase Workflow Tasks. This is done to prevent orphaned records in the Morpheus database and any associated integrations. Please consider how these processes could affect your infrastructure and take any needed actions to prevent issues.

### 11.8 How to un-manage an Instance/VM/Host

#### 11.8.1 Description

A managed VM (and associated Instance) needs to be unmanaged and returned to Discovered type.
11.8.2 Solution

Delete the record from the Infrastructure > Compute (! not from Provisioning - Instances) selection with the following configuration in the Delete modal:

- Remove Infrastructure UNCHECKED
- Remove Associated Instances Must be checked if the server has an associated Instance, as deleting the VM but not the Instance would result in an abandoned Instance thus not allowed.
- Force Delete UNCHECKED

The most important items to be aware of when “un-managing” an Instance/VM/Host are:

1. The “Remove from Infrastructure” flag when deleting a VM or Host in Morpheus determines if the actual VM is deleted from the target Infrastructure.
   - Checking “Remove Infrastructure” means you WANT TO DELETE THE ACTUAL VM. Typing “DELETE” in the confirmation field is required when “Remove From Infrastructure” is enabled.
   - Unchecking “Remove Infrastructure” means you only want to delete the record in Morpheus but leave the actual VM untouched.

2. Deleting an Instance will always remove Infrastructure.

   **Important:** REPEAT: Deleting an Instance from the Provisioning section will always remove the VM aka Infrastructure.

3. After removing the record from Morpheus, the VM must be in a Cloud with Inventory enabled to automatically be re-discovered.

11.8.3 Process

Steps to delete a managed VM from Morpheus and, when necessary, remove the associated Instance:

1. Navigate to the VM (not Instance) detail page at Infrastructure > Compute - VMs

   **Note:** VM’s inside an Instance can be navigated to inside the Instance Details page by selecting the VM in the VM’s section on the Instance Details page.

2. Select DELETE

3. Configure the DELETE HOST modal with the following settings:
4. Select DELETE
5. The VM and associated Instance will be removed from Morpheus but the actual VM will remain.
6. Wait up to 5 min or click REFRESH on the associated Clouds details page to force a cloud sync.

Note: Inventory must be enabled on the associated cloud for the VM to automatically be re-discovered by Morpheus.

7. The VM is now back in Morpheus as discovered/unmanaged. To managed and create a new Instance from the VM, select ACTIONS: Convert To Managed.
11.9 MySQL Too many connections error

If you see the following error in the Morpheus UI logs:

```
SqlExceptionHelper - Data source rejected establishment of connection, message from_server: "Too many connections"
```

it means the number connections between Morpheus application and mysql have reached the `max_connections` limit set in mysql (default is 151), or the `max_active` setting, which limits the number of connections on the Morpheus end (default is 100), and the limit needs to be raised, either in Morpheus or mysql, or both depending on the number of connections and configuration.

**Note:** The `max_connections` setting in mysql and the maximum used connections between an app node and mysql can be viewed in the Morpheus ui in the Administration - Health section under Database.

**Important:** In Single Morpheus app node configurations, the `max_active` setting on the app node must be less than the `max_connections` setting in mysql.

**Important:** In HA configurations, the `max_active` setting is per app node, and the `max_connections` setting in mysql must be greater than all app nodes `max_active` values combined, ie `(max_active * $number_of_app_nodes) <= max_connections`.

### 11.9.1 Morpheus `max_active` setting

Edit `/etc/morpheus/morpheus.rb` and add `mysql['max_active'] = $value` replacing `$value` with desired desired number of maximum connections allowed by Morpheus to mysql. For example, to set `max_active` at 150:

```
mysql['max_active'] = 150
```

Replacing 100 with the desired number of maximum connections allowed by Morpheus to mysql.

Run `morpheus-ctl reconfigure` for the setting to be applied. Reconfigure will not restart the ui unless additional ram has been added to the appliance host since the previous reconfigure. To edit the `max_active` without a reconfigure, update the `max_active` setting in `/opt/morpheus/conf/application.yml`. Please note the default setting of 100 will be applied upon the next reconfigure unless `max_active` is defined as instructed above in the `morpheus.rb` file.

### 11.9.2 mysql `max_connections` setting

**Important:** Customers are responsible for configuring and maintaining external databases used by Morpheus. This explains how to set the `max_connections` setting, but the value for the setting needs to be established by a customers qualified db admin.

In mysql prompt,

```
rq mysql> SET GLOBAL max_connections = $value;
```
This will immediately write the variable, however it is only a temporary setting that will be overwritten upon restart of the mysql service.

To persist the max_connections setting, edit my.cnf, and add max_connections = $value replacing $value with desired value, ie to set max_connections at 300 in my.cnf, add:

| max_connections = 300 |

### 11.10 Morpheus Agent Install Troubleshooting

When provisioning an Instance, there are network and configuration requirements to consider in order to successfully install the Morpheus Agent. Typically, when a VM Instance is still in the provisioning phase long after the VM is up, the Instance is unable to reach Morpheus. Depending on the Agent install mode, it could also mean Morpheus is unable to reach the Instance.

The most common reason an Agent install fails is the provisioned Instance cannot reach the Morpheus Appliance via the Appliance URL set in Administration > Settings over port 443. When an Instance is provisioned from Morpheus, it must be able to reach the Morpheus appliance via the Appliance URL or the Agent will not be installed.

In addition to the main Appliance URL in Administration > Settings, additional Appliance URLs can be set per Cloud in the Advanced Options section of the Cloud configuration modal when creating or editing a Cloud. When this field is populated, it will override the main Appliance URL for anything provisioned into that Cloud.

**Tip:** The Morpheus UI current log, located at /var/log/morpheus/morpheus-ui/current, is very helpful when troubleshooting Agent installations.
11.10.1 Agent Install Methods

Morpheus Agent installation supports multiple install methods.

- SSH/WinRM
- VM Tools
- Cloud-Init & Cloudbase-Init
- Windows Unattended
- Manual

For All Agent Install Methods

When an Instance is provisioned and the Agent does not install, verify the following for any Agent install mode:

- The Morpheus Appliance URL (Administration > Settings) is both reachable and resolvable from the provisioned node
- The Appliance URL begins with https://, not http://

**Note:** Be sure to use https:// even when using an IP address for the appliance.

- Inbound connectivity access to the Morpheus appliance from provisioned VMs and container hosts on port 443 (needed for Agent communication)
- Private (non-Morpheus provided) VM images and templates must have their credentials stored. These can be entered or edited in the Library > Virtual Images section by clicking the Actions dropdown on an image detail page and selecting Edit.

**Note:** Administrator user is required for Windows Agent install.

- The Instance does not have an IP address assigned. For scenarios without a DHCP server, static IP information must be entered by selecting the Network Type: Static in the Advanced Options section during provisioning. IP Pools can also be created in the Infrastructure > Networks > IP Pools section and added to Cloud network sections for IPAM
- DNS is not configured and the node cannot resolve the appliance. If DNS cannot be configured, the IP address of the Morpheus appliance can be used as the main or Cloud appliance

**SSH**

- Port 22 is open for Linux images, and SSH is enabled
- Credentials set on the image if using a custom or synced image. Credentials can be entered on images in the Library > Virtual Images section
WinRM

- Port 5985 must be open and WinRM enabled for Windows images
- Credentials have been entered on the image if using a custom or synced image. Credentials can be entered on images in the Library > Virtual Images section

**Note:** Administrator user is required for Windows Agent install.

VMware Tools (vmtools)

- VMware Tools is installed on the template(s)
- Credentials have been entered on the image if using custom or synced image. Credentials can be entered on images in the Library > Virtual Images section
- Sudo privileges required for Linux
- Administrator User required for Windows (SID 500)

Cloud-Init

- Cloud-Init settings configured in Administration > Settings > Provisioning section
- Cloud-Init installed on Virtual Image
- Cloud-Init enabled on Virtual Image config

Cloudbase-Init

- Windows Administrator Password defined in Administration > Settings > Provisioning section
- Cloudbase-Init installed on Virtual Image
- Cloud-Init enabled on Virtual Image config
- Cloudbase-Init is only required for OpenStack Cloud types

**Note:** Unattend Agent Installation and customizations are recommended over Cloudbase-Init

Windows Unattended

- Windows Administrator Password defined in Administration > Settings > Provisioning section
- VMware: Force Guest Customizations set to forced on Virtual Image config when using DHCP (Static Assignment will already force Guest Customizations)
- Nutanix & SCVMM: Virtual Image is sysprepped and shutdown, Sysprep Enabled flagged on Virtual Image config

11.10. Morpheus Agent Install Troubleshooting
Manual

Agent Install scripts can be downloaded from Morpheus by selecting Actions > Download Agent Script from an Instance detail page, then run manually on the target host when required for a given managed resource. Please note the script will be unique per managed resource and should not be saved to run as needed on any arbitrary resources in the future.

When installing on Windows, continue with the steps below to complete manual installation:

- Open powershell as an administrator
- Run the `unblock-file` cmdlet against the download agent installation script:
  
  ```powershell
  Unblock-File -Path C:\Users\User01\Documents\Downloads\agentInstall.ps1
  Get-ExecutionPolicy
  Set-ExecutionPolicy -ExecutionPolicy Unrestricted -Scope CurrentUser
  ```

- After running the powershell script, ensure the script downloaded the msi and the Agent service started correctly:
  
  ```powershell
  Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope CurrentUser
  ```

Following setup, verify that the Agent is reporting back to the Morpheus appliance.

11.10.2 Restarting the Morpheus Agent

In some situations, it may necessary to restart the Morpheus Agent on the host to re-sync communication from the Agent to the Morpheus appliance.

**Linux**

On the target host, run `sudo morpheus-node-ctl restart morphd` and the Morpheus agent will restart. `morpheus-node-ctl status` will also show the agent status.

**Windows**

The Morpheus Windows Agent service can be restarted in Administrative Tools > Services.

**Tip:** The Morpheus Remote Console is not dependent on Agent communication and can be used to install or restart the Morpheus agent on an Instance.

11.10.3 Uninstall Morpheus Agent

**Linux Agents**

You can use the following to uninstall the linux agent (contains commands for both rpm and deb agents)
sudo rm /etc/apt/sources.list.d/morpheus.list \
sudo morpheus-node-ctl kill \
sudo apt-get -y purge morpheus-node \
sudo apt-get -y purge morpheus-vm-node \
sudo yum -y remove morpheus-node \
sudo yum -y remove morpheus-vm-node \
sudo yum clean all \
sudo systemctl stop morpheus-node-runsvdir \
sudo rm -f /etc/systemd/system/morpheus-node-runsvdir.service \
sudo systemctl daemon-reload \
sudo rm -rf /var/run/morpheus-node \
sudo rm -rf /opt/morpheus-node \
sudo rm -rf /var/log/morpheus-node \
sudo kill runsv \
sudo kill runsvdir \
sudo kill morphd \
sudo usermod -l morpheus-old morpheus-node \

Windows Agents

```powershell
$app = Get-WmiObject -Class Win32_Product
-Filter "Name = 'Morpheus Windows Agent'"
$app.Uninstall()
```

11.10.4 CentOS/RHEL 7 Images

For custom CentOS 7 images we highly recommend setting up Cloud-Init and fixing the network device names. More information for custom CentOS images can be found in the CentOS 7 image guide.

11.11 Morpheus UI not loading after upgrade or reconfigure

**Problem:** The Morpheus ui does not load after performing an upgrade.

**Common Causes:**

1. The morpheus-ui has not finished loading
2. The morpheus-ui was not fully stopped before reconfigure, or not started after reconfigure
3. Morpheus was forced to restart or shut down while the database schema was being migrated during an upgrade

**Solutions:**

1. The morpheus-ui has not finished loading.
   
   An easy way to see when the ui is finished loading and running is to tail the ui current file and look for the morpheus logo with version and start time
   
   ```bash
   morpheus-ctl tail morpheus-ui
   ```

11.11. Morpheus UI not loading after upgrade or reconfigure
Note: After running `morpheus-ctl start morpheus-ui`, the Morpheus ui takes around 3 minutes to run depending on hardware.

1. The morpheus-ui was not fully stopped before reconfigure, or not started after reconfigure

   The morpheus ui must be stopped prior to running morpheus-ctl reconfigure when upgrading. Sometimes running morpheus-ctl stop morpheus-ui will timeout and the ui is not actually stopped. If stopping the ui does timeout, run morpheus-ctl kill morpheus-ui prior to reconfigure, and be sure to run morpheus-ctl start morpheus-ui after reconfigure is completed.

   If you ran a reconfigure before stopping the ui, run:

   ```
   sudo morpheus-ctl kill morpheus-ui
   sudo morpheus-ctl reconfigure
   sudo morpheus-ctl start morpheus-ui
   ```

   Wait for the ui to come up.

2. Morpheus was forced to restart or shut down while the database schema was being migrated during an upgrade

   If the ui fails to start and you see the error `Invocation of init method failed; nested exception is liquibase.exception.LockException: Could not acquire change log lock. Currently locked by morpheus` it likely means morpheus was forced to restart or shut down while the database schema was being migrated during an upgrade, and the lock was not released.

   To release the lock, you will need to run a mysql query. You will need to install mysql-client on the morpheus appliance, and grab the password for morpheus mysql. The username and db name are both morpheus. The password to login to mysql can be found in the application.yml file located at `/opt/morpheus/conf/application.yml`

   Then run the following:

   ```
   mysql -u morpheus -p -h 127.0.0.1 morpheus
   ```

   At the prompt, enter the mysql password from the application.yml

   Then run:

   ```
   DELETE FROM DATABASECHANGELOGLOCK;
   ```

   Then restart morpheus-ui:

   ```
   sudo morpheus-ctl restart morpheus-ui
   ```

   If the restart timesout, run:

   ```
   sudo morpheus-ctl kill morpheus-ui
   sudo morpheus-ctl start morpheus-ui
   ```
11.12 Remote Console

Morpheus has a built in Remote Console for Instances, Hosts, Virtual Machines and Bare Metal. The following information reviews the Roles Settings, Protocols, and Requirements necessary to configure and troubleshoot Remote Console access.

11.12.1 Role Settings

User Role settings determine if the Console tab or Open Console Action appear for a user, and if a login prompt is presented or the user is automatically logged in when using the Console.

• Remote Console (None, Provisioned, Full)
  - None The user will not have access to remote console.
  - Provisioned The user will only have remote console access for Instances they provisioned.
  - Full The user will have remote console access for all instances they have access to.

• Remote Console: Auto Login (No, Yes)
  - No A login prompt will be present in the console for Linux platforms, and the main login screen will present for Windows platforms.
  - Yes Morpheus will automatically login to the remote console using the credentials defined on the VM or Host. For provisioned Instances, the credentials are defined either from the credentials defined on the Virtual Image used, added via cloud-init or VMware Tools using the global cloud-init settings (Administration - Provisioning) or the Linux or Windows settings defined in User Settings. For Instances created when converting a VM or Host to managed, the credentials are entered when converting to managed. These credentials can be changed by editing the underlying VM or Host of the Instance.

Note: If the credentials defined on the VM or Host are not valid, and the Remote Console: Auto Login Role setting is set to Yes, the console will not be able to connect and no console window or login prompt will be presented. The credentials on the underlying VM or Host must be edited or Remote Console: Auto Login Role setting can be set to No for a login prompt to present in the console. Credentials cannot be changed from an Instance view, only in the Infrastructure VM or Host view.

11.12.2 Protocols

Platform Type and Cloud Settings determines the protocol and port used for Remote Console connections.

• SSH The SSH protocol will be used for Linux and OSX platform types, and 22 is the default port used.
• RDP The RDP (Remote Desktop) protocol will be used for Windows platform types over port 3389 by default.
• VNC The VNC protocol will be used for all platform types in Clouds with the Hypervisor Console option enabled in cloud settings. VNC connection are made directly to the Hypervisor Host over port 443.

Note: Alternative ports can be configured per VM or Host by editing the VM or Host and editing the Port field in the RPC host section.
**SSH**

For all Linux and OSX platform types, Morpheus will use the SSH protocol via port 22 by default for Remote Console connections, unless the *Hypervisor Console* option is enabled for VMware type clouds.

Morpheus will SSH using the username, password, RPC Host IP address and Port defined in the VM or Host record.

Default Requirements for SSH Connectivity

- SSH Enabled on the target VM or Host
- Port 22 incoming open on the target VM or Host firewalls and security groups from the Morpheus Appliance (not from the users IP address)
- An IP address defined on the VM or Host record that is routable from the Morpheus Appliance.
- Valid credentials defined on the VM or Host record in the RPC host field.
- *Remote Console* Role Permissions set to *Provisioned* or *Full* if the User provisioned the instance, or *Full* if the user did not provision the instance.

**RDP**

For all Windows platform types, Morpheus will use the RDP protocol via port 3389 by default for Remote Console connections, unless the *Hypervisor Console* option is enabled for VMware type clouds.

Morpheus will RDP using the username, password, RPC Host IP address and Port defined in the VM or Host record.

Default Requirements for RDP Connectivity

- Remote Access enabled on the target VM or Host and Remote Desktop enabled in the Windows Firewall settings. If the VM or Host is on a different network than the Morpheus appliance, public access for Remote Desktop must be enabled in the Firewall settings.
- Port 3389 incoming open on the target VM or Host firewalls and security groups from the Morpheus Appliance (not from the users IP address)
- An IP address defined on the VM or Host record that is routable from the Morpheus Appliance.
- Valid credentials defined on the VM or Host record in the RPC host field.
- *Remote Console* Role Permissions set to *Provisioned* or *Full* if the User provisioned the instance, or *Full* if the user did not provision the instance.

**Note:** If *Remote Console: Auto Login* is set to *No* in a users Role permissions, *Allow connections only from computers running Remote Desktop with Network Level Authentication* in the *Windows System Properties > Remote* settings must be DISABLED for Remote Console to connect.

**VNC (VMware Hypervisor Console)**

When the *Hypervisor Console* option is enabled in cloud settings, the VNC protocol will be used for all platform types that Cloud.

When using VNC Hypervisor Console, the Morpheus Appliance connects directly to the host the VM is on, not directly to the VM.

Morpheus features Remote Console support directly to hypervisors. To enable this feature a few prerequisites must be met:
• The Morpheus Appliance must have network access to the host the VM is on over 443.
• The Morpheus Appliance must be able to resolve the hypervisor hostnames.

**Note:** VNC connections for VMs and Hosts in VMware type clouds are made directly to the ESXi hosts, not vCenter.

Unlike SSH and RDP, valid credentials do not need to be set on the VM or Host records in Morpheus for VNC hypervisor console connections. An IP address is also not required on the VM or Host for VNC hypervisor console connections. Morpheus will be able to connect to the VM or Host as soon as the Host (Hypervisor) record is set, which can be viewed in the Info section on the VM or Host detail page.

**Note:**

• Auto-login is not supported for Hypervisor Console. Auto-login role settings do not apply to console connecting when using Hypervisor Console. Please note Hypervisor Console sessions persist on the ESXi host and once a user manually logs in to the VM they will continue to be logged in, even if the console tab/window in Morpheus is closed, until they manually log out.

• Copy and Paste and Text selection in Linux terminals is not supported when using VNC (VMware Hypervisor Console).

• In Morpheus versions 3.2.0 and higher, a newer Guacamole version is installed that is not compatible with MacOS Platform Types over VNC.

### 11.12.3 Copy and Paste

**Note:** Copy and Paste for Text is supported for SSH and RDP protocols only.

To Copy text from the console:

1. Select text in the Console window.
2. Click the COPY button at the top of the Console window.
3. The selected text is copied to the users clipboard.

To Paste text into console:

1. Copy text on the local computer to you clipboard
2. Right click into the “Paste Text Here” field at the top of the Console window. The field will the display “Text Copied, Use Console to Paste.”
3. Right click into the console window.
4. The text is pasted into the VM.
11.12.4 Guacamole

Overview

Morpheus uses Apache Guacamole, a clientless remote console. Guacamole is installed on the Morpheus Appliance during the initial reconfigure. In Morpheus versions 3.2.0 and higher, Guacamole 0.9.14 is automatically installed. On Morpheus versions older than 3.2.0, 0.9.9 is installed. The 0.9.14 version is required for VNC Hypervisor Console functionality on ESXi v6.5 and later.

The Guacamole proxy daemon, guacd, is used for all Remote Console connections and must be running for Remote Console functionality.

Troubleshooting guacd

If all console connections are not functioning, the Guacamole proxy daemon (guacd) process may not be running or have a stuck process preventing console connections. This is evident when only the header appears in the console tab/window, and no console window appears below the header and no connection status is show in the console header. The following commands can be used on the Morpheus Appliance to restore console functionality.

**morpheus-ctl status** Lists all local Morpheus services including guacd and their states. If guacd is stopped, it will need to be started again for Remote Console to function.

**morpheus-ctl start guacd** Starts the guacd process

**morpheus-ctl stop guacd** Stops the guacd process

**morpheus-ctl kill guacd** Forcefully kills the guacd process

**morpheus-ctl restarts guacd** Restarts the guacd process

**morpheus-ctl tail guacd** Tails the guacd current and state logs, located by default at /var/log/morpheus/guacd/. This log is useful when troubleshooting console connections, guacamole service status, and to determine the protocol being used for the Remote Console connection.

If guacd continues to stop even after being started, or if guacd is running and no properly configured console connections are functioning, there may be a stuck guacd or multiple guacd processes running, which will need to killed and guacd started again.

To kill all guacd processes on the Morpheus Appliance and start guacd again:

1. Kill the morpheus gaucd process: **morpheus-ctl kill guacd**
2. Grep for all running guacd processes: sudo ps -aux | grep guacd and note the guacd pid(s) (minus the process from the grep)
3. Kill all running guacd processes: kill -9 pid replacing *pid* with the pid(s) of the target processes
4. Start guacd again: **morpheus-ctl start guacd**
5. Tail the guacd logs to verify guacd is started and listening: **morpheus-ctl tail guacd** The log output will resemble below when guacd is properly running:

```
guacd[16899]: INFO: Guacamole proxy daemon (guacd) version 0.9.14 started
guacd[16899]: INFO: Listening on host 127.0.0.1, port 4822
```

6. Additional information in the guacd logs appears when Morpheus is making a console connection. A successful connecton will resemble:

---

Chapter 11. Troubleshooting
Guacamole Version

In Morpheus versions 3.2.0 and higher, Guacamole version 0.9.14 is automatically installed. On Morpheus versions older than 3.2.0, 0.9.9 is installed. The 0.9.14 version is required for VNC Hypervisor Console functionality on ESXi v6.5 and later.

Note Guacamole version 0.9.14 is not compatible with MacOS Platform Types over VNC on ESXi v6.0 or prior (6.5 is supported). If necessary, the guacamole version can be reverted to 0.9.9.

To revert the guacamole version from 0.9.14 to 0.9.9.

1. Kill guacd: `morpheus-ctl kill guacd`

2. Check if any guacd processes are still running: `ps -aux | grep guac`

3. If so, kill the processes: `kill -9 pid` with id being the actual process id, like 16101.

4. Go to the guac 0.9.9 directory: `cd /var/opt/morpheus/guacamole-server-0.9.9`

5. Run: `make install`

6. Start guacd: `morpheus-ctl start guacd`

11.13 SSL Self-signed Certificate Regeneration

When Morpheus is deployed it generates a 10 year self-signed non-trusted SSL certificate. Below details the process to regenerate this certificate and key.

11.13.1 Replacing both the certificate and private key

1. Delete the certificate and key files in `/etc/morpheus/ssl/` that end in `.crt` and `.key`

2. Run Reconfigure: `morpheus-ctl reconfigure`

3. Restart NGINX: `morpheus-ctl restart nginx`
11.13.2 Replacing only the certificate

1. Delete the certificate file in /etc/morpheus/ssl/ it ends in .crt
2. Run Reconfigure morpheus-ctl reconfigure
3. Restart NGINX morpheus-ctl restart nginx

11.14 Unable to Delete Tenant

Problem When trying to delete a tenant, a message stating manage resources must be removed or other error occurs and the tenant is not deleted. The tenant may be stuck in a deleting status or return to OK status after delete attempt.

Cause All managed resources must be removed from a tenant in order for that tenant to be deleted. This includes instances and their underlying managed vm’s

Solution

1. Login or impersonate that an Admin user inside the tenant
2. Navigate to Infrastructure > Hosts
3. Under Hosts and VM’s, delete any managed resources
   • Uncheck remove infrastructure when deleting a VM to only remove it from Morpheus but not from the underlying hypervisor/cloud
   • You must check remove associated instances if the VM has an associated instance
   • If the VM no longer exists but there is still a record in Morpheus, uncheck remove infrastructure and check force delete
4. Once all managed resources are removed from the tenant, the tenant can then be deleted
5. In certain situations other components may prevent a tenant from being deleted. If you have removed all managed resources from a tenant and the tenant still cannot be deleted, please contact Morpheus support

Warning: Managed resources can also be removed by deleting instances, but be aware this will delete VM’s associated with the instance from the underlying hypervisor/cloud

11.15 Unable to Provision a Custom Image

Prior to provisioning an custom image, the image must be configured in the Library > Virtual Images section by selecting Edit on the Actions dropdown of the Virtual Image.

In the Edit Virtual Image pane:

1. Select “Cloud Init Enabled?” only if the Virtual Image is a linux image with cloud init installed.
2. Enter the username and password that are set on the Virtual Image.

Note: When using Static IP’s or IP Pools in VMware, VMware tools must also be installed on the template in order for Morpheus to set the static IP address when provisioning.
Note: Morpheus agents only support 64-bit vm’s prior to versions 2.12.3 and 3.0.2
12.1 Getting started with Morpheus and AWS

12.1.1 Introduction

This guide is designed to help you get started and quickly get the most out of Morpheus with AWS. By the end, you will integrate your first cloud, configure networking, prepare and consume images, provision instances, and get started with automation. We will briefly discuss installation and account setup but will provide links to additional resources for those very first steps. For the most part, this guide assumes you are able to get Morpheus installed and are ready to move forward from that point. There is a lot more to see and do in Morpheus that is beyond the scope of this guide. For more, consult the complete Morpheus documentation or take part in our user community forum.

12.1.2 Installation & Setup

In the simplest configuration, Morpheus needs one appliance server which will contain all the components necessary to orchestrate virtual machines and containers. Full requirements, including storage and networking considerations, can be found in requirements. In order to provision any new instances, hosts, or applications, (or convert any discovered resources to managed resources) you will need a valid license. If you don’t have one, Morpheus will automatically set up a lab license on installation. A lab license is a time-unlimited license for Morpheus that limits you to 25 managed and discovered workloads. If you have a timed trial or a paid license, the license can be applied in Administration > Settings > License.

12.1.3 Groups

Groups in Morpheus define which resources a user has access to. Clouds are added to groups and a user can only access clouds that are in the groups to which their roles give them access. More information on Morpheus groups is available in the Groups section. A deep dive into groups goes beyond the scope of this guide but it’s often useful to create a group that contains all clouds for testing purposes. We will create that group now so that we can add our first cloud into this group in the next section.

Navigate to Infrastructure > Groups. Here we will see a list of all configured groups but, of course, this will be empty immediately after installation. Click “+CREATE”. Give your group a name, such as “All Clouds”. The “CODE” field is used when calling Morpheus through Morpheus API or Morpheus CLI. It’s useful in most cases to have an “All Clouds” group for testing purposes so this will likely help you down the road.
12.1.4 Integrating Your First Cloud

Clouds in Morpheus consist of any consumable endpoint whether that be On-Prem, Public clouds, or even bare metal. In this guide, we will focus on integrating and working with AWS.

To get started, we will navigate to Infrastructure > Clouds. This is the cloud detail page which lists all configured clouds. It will be empty if you’ve just completed installation and setup of Morpheus but soon we will see our integrated AWS cloud here.

Click the “+ADD” button to pop the “CREATE CLOUD” wizard. Select “AMAZON” and click the “NEXT” button.

On the “CONFIGURE” tab, give your cloud a “NAME”. Select your Amazon region and enter your credentials in the “ACCESS KEY” and “SECRET KEY” fields. We can also set a number of advanced options here that may be relevant to your AWS use case.

Once you’re satisfied with your selections, click “NEXT”.

We have now arrived at the “GROUP” tab. In this case, we will mark the radio button to “USE EXISTING” groups if you wish to use the group we configured earlier.

Once you’ve selected the group, click “NEXT”.

On the final tab of the “CREATE CLOUD” wizard, you’ll confirm your selections and click “COMPLETE”. The new cloud is now listed on the cloud detail page. After a short time, Morpheus will provide summary information and statistics on existing virtual machines, networks, and other resources available in the cloud.

Click “SAVE CHANGES”. Your group is now ready to accept clouds.
12.1.5 Viewing Cloud Inventory

Now that we’ve integrated our first AWS cloud, we can stop for a moment to review what Morpheus gives us from the cloud detail page. We can see that Morpheus gives us estimated costs and cost histories, metrics on used resources, and also lists out resource counts in various categories including container hosts, hypervisors, and virtual machines. We can drill into these categories to see lists of resources in the various categories individual resources within them by clicking on the category tabs. We can link to the detail page for any specific resource by clicking on it from its resource category list.

12.1.6 Configuring Resource Pools

With our AWS cloud configured, Morpheus will automatically sync in available resource pools and data stores. Resource pools, once Morpheus has had time to ingest them, will be visible from the cloud detail page. Navigate to Infrastructure > Clouds > (your AWS cloud) > RESOURCES tab. In here, we are able to see and control access to the various resource pools that have been configured in Amazon. For example, we can restrict access to a specific resource pool within Morpheus completely by clicking on the “ACTIONS” button, then clicking “Edit”. If we unmark the “ACTIVE” button and then click “SAVE CHANGES” we will see that the resource pool is now grayed out in the list. The resources contained in that pool will not be accessible for provisioning within Morpheus.

Often our clients will want to make specific blocks of resources available to certain groups. This can be easily and conveniently controlled through the same “EDIT RESOURCE POOL” dialog box we were just working in. If we expand the “Group Access” drawer, we are able to give or remove access to each pool to any group we’d like. We can also choose to make some or all of our resource pools available to every group. Specific resource pools can also be defined as the default for each group if needed.
Additionally, we may choose to allow only certain service plans to be provisioned into a specific pool of resources. For example, perhaps a specific cluster is my SQL cluster and only specific services plans should be consumable within it. We can control that through this same dialog box.

### 12.1.7 Configuring Network for Provisioning

When configuring networking, we can set global defaults by going to **Infrastructure > Network > NETWORKS tab**. Here we can add or configure networks from all clouds integrated into Morpheus. Depending on the number of clouds Morpheus has ingested, this list may be quite large and may also be paginated across a large number of pages. In such a case, it may be easier to view or configure networks from the specific cloud detail page so that networks from other clouds are not shown.

Still in **Infrastructure > Network**, make note of the “INTEGRATIONS” tab. It’s here that we can set up any integrations...
that may be relevant, such as IPAM integrations. Generally speaking, when adding IPAM integrations, we simply need to name our new integration, give the API URL, and provide credentials. There’s more information in the *Networking Integrations* section of Morpheus Docs.

In *Infrastructure > Networking* we can also set up IP address pools from the IP Pools tab. These pools can be manually defined, known as a Morpheus-type IP pool, or they can come from any IPAM integrations you’ve configured. As instances are provisioned, Morpheus will assign IP addresses from the pool chosen during provisioning. When the instance is later dissolved, Morpheus will automatically release the IP address to be used by another instance when needed. When adding or editing a network, we can opt to scope the network to one of these configured IP address pools. Edit an existing network by clicking the pencil icon on the Networks List Page (*Infrastructure > Networks > Networks Tab*) and fill in the “Network Pool” field to associate the IP Pool with the network.
Since this guide is focused on working within the AWS cloud that we integrated at the start, we will take a look at our network configurations on the cloud detail page as well. Navigate to Infrastructure > Clouds > (your AWS cloud) > NETWORKS tab. Just as with resource pools, we have the ability to make certain networks inactive in Morpheus, or scope them to be usable only for certain groups or tenants.

12.1.8 Prepping an Image

As we’ll discuss and try out in the next section, Morpheus comes out of the box with a default set of blueprints that are relevant to many modern deployment scenarios. For the most part, these are base operating system images with a few additional adjustments. However, in many on-premise deployments, there are often custom image and networking requirements. We will work with the images included in Morpheus by default but have guides in Morpheus Docs for vmware-templates which are consumable in Morpheus.
12.1.9 Provisioning Your First Instance

At this point, we are ready to provision our first image. As a first instance, we’ll provision an Apache web server to our AWS cloud.

Navigate to \ProIns\ If any instances are currently provisioned, we will see them listed here. To start a new instance we click the “+ADD” button to pop the “CREATE INSTANCE” wizard. We’ll scroll down to and select the Apache instance type and click “NEXT”.

First, we’ll specify the group to provision into which determines the clouds available. If you’ve followed this guide to this point, you should at least have a group that houses all of your clouds which you can select here. This will allow us to select the AWS cloud from the “CLOUD” dropdown menu. Provide a unique name to this instance and then click “NEXT”.

From the “CONFIGURE” tab, we’re presented with a number of options. The options are cloud and layout-specific, more generalized information on creating instances and available options is Morpheus Agent. For our purposes, we’ll select the following options:

- **LAYOUT**: Includes options such as the base OS, custom layouts will also be here when available
- **PLAN**: Select the resource plan for your instance. Some plans have minimum resource limits, Morpheus will only show plans at or above these limits. User-defined plans can also be created in \AdmPla\.
- **VOLUMES**: The minimum disk space is set by the plan, this value may be locked if you’ve selected a custom plan that defines the volume size
- **NETWORKS**: Select a network, note that IP pools must be linked with the networks defined in VMware in order to assign static IP addresses
- **SECURITY GROUPS**
Under the “User Config” drawer, mark the box to “CREATE YOUR USER”. Click NEXT.

**Note:** “CREATE YOUR USER” will seed a user account into the VM with credentials set in your Morpheus user account settings. If you’ve not yet defined these credentials, you can do so by clicking on your username in the upper-right corner of the application window and selecting “USER SETTINGS”.

For now, we’ll simply click “NEXT” to move through the “AUTOMATION” tab but feel free to stop and take a look at the available selections here. There is more information later in this guide on automation and even more beyond that in the rest of Morpheus docs.

Review the settings for your first instance and click COMPLETE.

We are now dropped back onto the instances list page. We can see a new entry in the list at this point with a status indicator that the new machine is being launched (rocket icon in the status field). We can double click on the instance in the list to move to the instance detail page. For now we will see a progress bar indicating that the instance is being created and is starting up. The exact amount of time this process will take depends selections made when provisioning the instance. For more detailed information on the status of various provisioning processes, we can scroll down and select the “HISTORY” tab. The “STATUS” icon will change from the blue rocket to a green play button when the instance is fully ready. Furthermore, we can click on the hyperlinked IP address in the “VMS” section of this page to view a default page in a web browser to confirm success.

**12.1.10 Creating Your First Library Item**

In the prior section, we manually provisioned our first instance. However, Morpheus allows you to build a catalog of custom provisionable items to simplify and speed provisioning in the future. In this section, we’ll build a catalog item and show how that can translate into quick instance provisioning after configuration.

**Note:** Before starting this process, it’s important to decide which virtual image you plan to use. If you’re not using a Morpheus-provided image, you’ll want to ensure it’s uploaded. You will not be able to complete this section without selecting an available image. In this example we will use Morpheus Redis 3.0 on Ubuntu 14.04.3 v2.

Navigate to Library > Blueprints > Node Types and click +ADD.

In this example, I am going to set the following options in the “NEW NODE TYPE” wizard:

- **NAME**
- **SHORT NAME**
- **VERSION:** 1 (In this particular case, the version is not important)
- **TECHNOLOGY:** Amazon
With the new node created, we’ll now add a new instance type which will be accessible from the provisioning wizard once created. Move from the “NODE TYPES” tab to the “INSTANCE TYPES” tab and click “+ADD”.

In the “NEW INSTANCE TYPE” wizard, I’ll simply enter a NAME and CODE value. Click “SAVE CHANGES”.

- **AMI IMAGE**: Morpheus Redis 3.0 on Ubuntu 14.04.3 v2
Now that we’ve created a new instance type, access it by clicking on the name in the list of custom instances you’ve created. In my case, I’ve given the name “NewInstanceType”.

Once we’ve opened the new instance type, by default, we should be on the “LAYOUTS” tab. Click “+ADD LAYOUT”. I’ve set the following fields on my example layout:

- **NAME**
- **VERSION**: This is the version number of the layout itself, which is labeled 1.0 in the example
- **TECHNOLOGY**: Amazon
• **Nodes**: Select the node we created earlier, if desired you can specify multiple nodes.

Click “SAVE CHANGES”.

At this point we’ve completed the setup work and can now provision the instance we’ve created to our specifications. Navigate to [ProIns] and click “+ADD”. From the search bar we can search for the new instance type we’ve created. In the example case, we called it “newinstancetype”. Click “NEXT”.

As before, we can select a group and cloud to provision this new instance. Click “NEXT”. On the “CONFIGURE” tab, make note that the layout and plan are already selected because they were configured as part of creating the new instance type. Select a network and click “NEXT”. Once again we will also click “NEXT” through the “AUTOMATION” tab. Finally, click “COMPLETE”.

As before when we manually provisioned an instance, Morpheus will now begin to spin up the new VM. Once the provisioning process has completed, open the instance detail page in Morpheus and click on the “CONSOLE” tab. You’ll be logged in with your user account and are then able to confirm the machine is ready and available.

### 12.1.11 Automation and Configuration Management

Morpheus automation is composed of Tasks and Workflows. A task could be a script added directly, scripts or blueprints pulled from the Morpheus Library, playbooks, recipes, or a number of other things. The complete list of task types can be found in *Automation*. Tasks can be executed individually but they are often combined into workflows. We can opt to run a workflow at provision time or they can be executed on existing instances through the Actions menu.

In this guide we will set up an Ansible integration, create a task, add the task to a workflow, and run the workflow against a new and existing instance. If you’ve worked through this guide to this point, you should already have an Apache instance running. If you don’t yet have that, provision one before continuing with this guide and ensure it’s reachable on port 80.

We’ll first set up the Ansible integration, you can integrate with the sample repository referenced here or integrate with your own. Go to ‘Administration > Integrations’. Click “+ NEW INTEGRATION” and select Ansible from the dropdown menu. Fill in the following details:

- **NAME**
- **ANSIBLE GIT URL**: https://github.com/ncelebic/morpheus-ansible-example, or enter the URL for your own Ansible git repository
• **PLAYBOOKS PATH**
• **ROLES PATH**
  - Mark the box to “USE MORPHEUS AGENT COMMAND BUS”

**Note:** If your git repository requires authentication, you should create a keypair and use the following URL format: git@github.com:ncelebic/morpheus-ansible-example.git.
Click “SAVE CHANGES”. You’ll now see our new Ansible integration listed among any other configured integrations. If we click on this new integration to view detail, a green checkmark icon indicates the git repository has been fully synced.

With the Ansible integration set up, we can now create a task that includes our playbook. Go to |LibAut|, click “+ADD”. We’ll first set our “TYPE” value to Ansible Playbook so that the correct set of fields appear in the “NEW TASK” wizard. Set the following options:

- **NAME**
- **ANSIBLE REPO**: Here we will choose the Ansible integration that we just created
- **PLAYBOOK**: In our example case, enter ‘playbook.yml’

Click “SAVE CHANGES” to save our new task. We can test the new task on our Apache VM now by going to |ProIns| and clicking into our VM. From the “ACTIONS” menu select “Run Task”. From the “TASK” dropdown menu, select the task we just added and click “EXECUTE”.

To see the progress of the task, click on the “HISTORY” tab and click on the (i) button to the right of each entry in the list. In this case, we can also see the results of the task by clicking on the link in the “LOCATION” column of the “VMS” section.

Now that our task is created, we can put it into a workflow. Back in |LibAut| we will click on the “WORKFLOWS”
tab. Click “+ADD” and select Provisioning Workflow. We’ll give the new workflow a name and expand the Post Provision section. As we begin to type in the name of the task we’ve created, it should appear as a selection. Click “SAVE CHANGES”.
Now that we have a workflow, return to |ProIns| and begin to provision another Apache instance. More detailed
instructions on provisioning a new Apache instance are included earlier in this guide if needed. Now, when you reach the “AUTOMATION” section of the “CREATE INSTANCE” wizard, we have a workflow to select. From the “WORKFLOW” dropdown menu, select the workflow we just created and complete provisioning of the new instance.

As the instance is provisioning, we can go to the “HISTORY” tab and see Morpheus executing the tasks that were contained in our workflow.

This is just one example of using Morpheus to automate the process of configuring and instance to your needs. There are a number of other automation types that can be built into your workflows as well. For further information, take a look at the Automation Integrations guide in Morpheus docs.

12.1.12 Conclusion

At this point you should be up and running in Morpheus, ready to consume AWS. This guide only scratches the surface, there is a lot more to see and do in Morpheus. Take a look at the rest of Morpheus Docs for more information on supported integrations and other things possible.

12.2 Getting started with Morpheus and VMware

12.2.1 Introduction

This guide is designed to help you get started and quickly get the most out of Morpheus with VMWare. By the end, you will integrate your first cloud, configure networking, prepare and consume images, provision instances, and get started with automation. We will briefly discuss installation and account setup but will provide links to additional resources for those very first steps. For the most part, this guide assumes you are able to get Morpheus installed and
are ready to move forward from that point. There is a lot more to see and do in Morpheus that is beyond the scope of this guide. For more, consult the complete Morpheus documentation or take part in our user community forum.

12.2.2 Installation & Setup

In the simplest configuration, Morpheus needs one appliance server which will contain all the components necessary to orchestrate virtual machines and containers. Full requirements, including storage and networking considerations, can be found in Morpheus documentation here. In order to provision any new instances, hosts, or applications, (or convert any discovered resources to managed resources) you will need a valid license. If you don’t have one, you can request a lab license for free at Morpheus Hub. Once obtained, the license can be applied in Administration > Settings > License.

12.2.3 Groups

Groups in Morpheus define which resources a user has access to. Clouds are added to groups and a user can only access clouds that are in the groups to which their roles give them access. More information on Morpheus groups is here. A deep dive into groups goes beyond the scope of this guide but it’s often useful to create a group that contains all clouds for testing purposes. We will create that group now so that we can add our first cloud into this group in the next section.

Navigate to Infrastructure > Groups. Here we will see a list of all configured groups but, of course, this will be empty immediately after installation. Click “+CREATE”. Give your group a name, such as “All Clouds”. The “CODE” field is used when calling Morpheus through Morpheus API or Morpheus CLI. It’s useful in most cases to have an “All Clouds” group for testing purposes so this will likely help you down the road.

Click “SAVE CHANGES”. Your group is now ready to accept clouds.
12.2.4 Integrating Your First Cloud

Clouds in Morpheus consist of any consumable endpoint whether that be On-Prem, Public clouds, or even bare metal. In this guide, we will focus on integrating and working with VMWare vCenter.

To get started, we will navigate to Infrastructure > Clouds. This is the cloud detail page which lists all configured clouds. It will be empty if you’ve just completed installation and setup of Morpheus but soon we will see our integrated vCenter cloud here.

Click the “+ADD” button to pop the “CREATE CLOUD” wizard. Select “VMWARE VCENTER” and click the “NEXT” button.

On the “CONFIGURE” tab, we’re asked to set the initial connection strings into vSphere. The API URL should be in the following format: https://<URL>/sdk. The USERNAME should be in user@domain format.
Morpheus allows vCenter clouds to be scoped to the VDC and CLUSTER or even the specific RESOURCE POOL if you choose. Once you’ve entered your URL and credentials, these dropdown menus will become populated.

The RPC MODE setting determines how Morpheus will connect to VMs and make configuration and scripting calls if Morpheus Agent is not installed. In a VMware environment we have the additional option to select VMware Tools if WinRM/SSH are not available.

Additionally, we can opt to INVENTORY EXISTING INSTANCES to begin polling VMs for statistics and rightsizing recommendations as well as ENABLE HYPERVISOR CONSOLE to use native vSphere console with port 443 connectivity between Morpheus and ESXi hosts.

To move on, expand the “Advanced Options” section.

Within the “Advanced Options” drawer are additional configurations to consider for your first cloud. Some of these won’t usable until they reference additional configured integrations. Common settings to consider are DOMAIN, STORAGE TYPE, APPLIANCE URL (overrides the Morpheus URL for external systems), GUIDANCE (setting “Manual” will make recommendations for rightsizing), and AGENT INSTALL MODE.
Once you’re satisfied with your selections, click “NEXT”

We have now arrived at the “GROUP” tab. In this case, we will mark the radio button to “USE EXISTING” groups if you wish to use the group we configured earlier.

Once you’ve selected the group, click “NEXT”

On the final tab of the “CREATE CLOUD” wizard, you’ll confirm your selections and click “COMPLETE”. The new cloud is now listed on the cloud detail page. After a short time, Morpheus will provide summary information and statistics on existing virtual machines, networks, and other resources available in the cloud.
### 12.2.5 Viewing Cloud Inventory

Now that we’ve integrated our first VMware cloud, we can stop for a moment to review what Morpheus gives us from the cloud detail page. We can see that Morpheus gives us estimated costs and cost histories, metrics on used resources, and also lists out resource counts in various categories including container hosts, hypervisors, and virtual machines. We can drill into these categories to see lists of resources in the various categories individual resources within them by clicking on the category tabs. We can link to the detail page for any specific resource by clicking on it from its resource category list.

### 12.2.6 Configuring Resource Pools

With our VMware cloud configured, Morpheus will automatically sync in available resource pools and data stores. For resource pools, once Morpheus has had time to ingest them, then will be visible from the cloud detail page. Navigate to **Infrastructure > Clouds > (your VMware cloud) > RESOURCES tab**. In here, we are able to see and control access to the various resource pools that have been configured in vCenter. For example, we can restrict access to a specific resource pool within Morpheus completely by clicking on the “ACTIONS” button, then clicking “Edit”. If we unmark the “ACTIVE” button and then click “SAVE CHANGES” we will see that the resource pool is now grayed out in the list. The resources contained in that pool will not be accessible for provisioning within Morpheus.

Often our clients will want to make specific blocks of resources available to their own customers. This can be easily and conveniently controlled through the same “EDIT RESOURCE POOL” dialog box we were just working in. If we expand the “Group Access” drawer, we are able to give or remove access to each pool to any group we’d like. We can also choose to make some or all of our resource pools available to every group. Specific resource pools can also be defined as the default for each group if needed.
Additionally, we may choose to allow only certain service plans to be provisioned into a specific pool of resources. For example, perhaps a specific cluster is my SQL cluster and only specific services plans should be consumable within it. We can control that through this same dialog box.

12.2.7 Configuring Data Stores

To take a look at data stores, we’ll move from the “RESOURCES” tab to the “DATA STORES” tab on our cloud detail page.

Morpheus gives the user similar control with data stores to what we saw with our resources pools earlier. Just like with resource pools, we can disable access within Morpheus completely by clicking on “ACTIONS” and then “Edit”. If we unmark the “ACTIVE” checkbox and click “SAVE CHANGES”, you will see that specific data store has been grayed out.

Just like with resource pools, we are also able to scope data stores to specific groups. This ensures that the members of each group are only able to consume the data stores they should have access to.
12.2.8 Configuring Folders

Still within the “RESOURCES” tab, within the “FOLDERS” subtab we see the folders discovered from the vCenter Cloud. Edit folder configurations by selecting “ACTIONS” from the end of the row, then clicking “Edit”. Consider the following configurations for specific folders:

- **DEFAULT:** If selected, this folder will be pre-selected when provisioning new Instances to this Cloud (See the Folder option on the CONFIGURE tab of the Instance provisioning wizard)

- **IMAGE TARGET:** Morpheus will look in the image target folder(s) to onboard VMware images

After saving the changes, you’ll see any folders set as default or image target indicated in the folders list.

12.2.9 Configuring Network for Provisioning

When configuring networking, we can set global defaults by going to *Infrastructure > Network > NETWORKS tab.* Here we can add or configure networks from all clouds integrated into Morpheus. Depending on the number of clouds Morpheus has ingested, this list may be quite large and may also be paginated across a large number of pages. In such a case, it may be easier to view or configure networks from the specific cloud detail page so that networks from other clouds are not shown.

Still in *Infrastructure > Network*, make note of the “INTEGRATIONS” tab. It’s here that we can set up any integrations that may be relevant, such as IPAM integrations. Generally speaking, when adding IPAM integrations, we simply need to name our new integration, give the API URL, and provide credentials. There’s more information in the IPAM integration section of Morpheus Docs.
In **Infrastructure > Networking** we can also set up IP address pools from the IP Pools tab. These pools can be manually defined, known as a Morpheus-type IP pool, or they can come from any IPAM integrations you’ve configured. As instances are provisioned, Morpheus will assign IP addresses from the pool chosen during provisioning. When the instance is later dissolved, Morpheus will automatically release the IP address to be used by another instance when needed. When adding or editing a network, we can opt to scope the network to one of these configured IP address pools. Edit an existing network by clicking the pencil icon on the Networks List Page (Infrastructure > Networks > Networks Tab) and fill in the “Network Pool” field to associate the IP Pool with the network.

Since this guide is focused on working within a VMware cloud that we integrated at the start, we will take a look at our network configurations on the cloud detail page as well. Navigate to **Infrastructure > Clouds > (your VMware cloud) > NETWORKS tab**. Just as with resource pools and data stores, we have the ability to make certain networks inactive in Morpheus, or scope them to be usable only for certain groups or tenants.
Prepping an Image

As we’ll discuss and try out in the next section, Morpheus comes out of the box with a default set of blueprints that are relevant to many modern deployment scenarios. For the most part, these are base operating system images with a few additional adjustments. However, in many on-premise deployments, there are often custom image and networking requirements. We will work with images included in Morpheus by default in this guide but it’s important to discuss how to prep custom images as well.

Creating a Windows Image

The following versions of Windows Server are supported:

- 2008 R2
- 2012
- 2012 R2
- 2016
- 2019

To start, create a new Windows machine in vCenter using a base version of your selected Windows build.

**Note:** It’s recommended to make the VMDK drive as small as possible for your purposes as this generally speeds cloning and deploy times. Morpheus provisioning and post-deploy scripts allow to to expand the drive to any size that you need.

Once the machine is created, ensure VMtools is installed on the operating system. Then, apply all updates and service packs. Next, configure WinRM and open the firewall:

```bash
winrm quickconfig
```

**Note:** WinRM configuration is optional if using VMtools RPC mode for agent install and Morpheus Agent for guest exec.

Next, we’ll install .NET 4.5 or higher. Ensure Windows Firewall will allow WinRM connections and shut down the virtual instance. Finally, convert it to a template.

**Note:** Morpheus will Sysprep images based on the “Force Guest Customizations” flag under VM settings when using DHCP. If this flag is enabled or if using static IP addresses or IP pools when provisioning, ensure a Sysprep has not been performed. In such cases, guest customization will always be performed and a Sysprep will be triggered.
Creating a CentOS/RHEL Image

Create a new machine in vCenter and install a base version of your preferred Linux distro.

**Note:** If you are using cloud-init as part of your image, you will need to ensure your virtual machine has a cdrom.

Before installing the operating system, set up a single ext or xfs partition without a swap disk. Next, install the distro applying any updates to the operating system or security updates. Once the operating system is running and updated, install the following:

```bash
yum install cloud-init
yum install cloud-utils-growpart
yum install open-vm-tools
yum install git
yum install epel-release
```

Set selinux to permissive as the enforced setting can cause problems with cloud-init:

```bash
sudo vi /etc/selinux/config
```

Cloud-Init

We’ll get started by installing cloud-init using the following command:

```bash
yum -y install epel-release
yum -y install git wget ntp curl cloud-init dracut-modules-growroot
rpm -qa kernel | sed 's/^kernel-//' | xargs -I {} dracut -f /boot/initramfs-{}.img {}
```

**Note:** The above command will install some core dependencies for cloud-init and automation later as you work with your provisioned instances. For example, we install Git here as it is used for Ansible automation. If you had no plans to use Ansible, this installation could be skipped. The dracut-modules-growroot is responsible for resizing the root partition upon initial boot which was potentially adjusted during provisioning.

One key benefit of using cloud-init is that we don’t have to lock credentials into the blueprint. We recommend configuring a default cloud-init user that will get created automatically when the VM is booted by cloud-init. We can define that default user in `|AdmSetPro| > Cloud-Init`.

Network Interfaces

As of CentOS 7, network interface naming conventions have changed. You can check this by running `ifconfig` and noting that the primary network interface has some value similar to "ens2344". The naming is dynamic and typically set based on hardware ID. We don’t want this to fluctuate when provisioning this blueprint in our VMware environments. To accomplish this end, we will rename the interface back to "eth0" using the steps below.

First, adjust the bootloader to disable interface naming:

```bash
sed -i -e 's/quiet/quiet net.ifnames=0 biosdevname=0/" /etc/default/grub
grub2-mkconfig -o /boot/grub2/grub.cfg
```

The next step is to adjust network scripts in CentOS. Start by confirming the presence of a file called `/etc/sysconfig/network-scripts/ifcfg-eth0`. Once confirmed, run the following script:

```bash
export iface_file=${(basename "$(find /etc/sysconfig/network-scripts/ -name 'ifcfg*' - ˓→not -name 'ifcfg-lo' | head -n 1")")
export iface_name=${iface_file:6}
```

(continues on next page)
echo $iface_file
echo $iface_name
sudo mv /etc/sysconfig/network-scripts/$iface_file /etc/sysconfig/network-scripts/
˓→ifcfg-eth0
sudo sed -i -e "s/$iface_name/eth0/" /etc/sysconfig/network-scripts/ifcfg-eth0
sudo bash -c 'echo NM_CONTROLLED="no" >> /etc/sysconfig/network-scripts/ifcfg-eth0'

This script tries to confirm there is a new ifcfg-eth0 config created to replace the old config file. Confirm this config exists after running and if not you will have to build your own:

```
TYPE=Ethernet
DEVICE=eth0
NAME=eth0
ONBOOT=yes
NM_CONTROLLED="no"
BOOTPROTO="dhcp"
DEFROUTE=yes
```

For more on CentOS/RHEL image prep, including additional configurations for specific scenarios, take a look at the VMware image prep page in Morpheus Docs.

**Creating an Ubuntu 20.04 Image**

Download the Ubuntu 20.04 ISO from Canonical, and upload the base image to vCenter. Then, create a new virtual machine in vCenter.

**Note:** Since we’ll include cloud-init with our image, we will need to ensure the virtual machine has a cdrom. Select the Ubuntu 20.04 ISO we just downloaded from the CD/DVD drive dropdown menu when creating the new virtual machine.

Before installing the operating system, set up a single ext partition without a swap disk. Then, continue on installing Ubuntu making the following selections during the setup process:

- Update to the latest installer if a later version is available
- Use the entire disk and deselect the option to set up the disk as an LVM group
- Configure an account and set a password
- Opt to install OpenSSH Server
- Other optional packages aren’t needed for this basic Ubuntu image

Complete the installation process and reboot the machine. Update the package list and apply any upgrades:

```
apt-get update
apt-get upgrade
```

Disable assignment of new styled names for network interfaces (instead of ens### they will be eth#):

```
sudo sed -i -e 's/GRUB_CMDLINE_LINUX=""/GRUB_CMDLINE_LINUX="net.ifnames=0
˓→biosdevname=0"
"/ /etc/default/grub
```

Update GRUB:

```
update-grub
```

Update the 70-persistent-net.rules file:
Remove `subiquity-disable-cloudinit-networking.cfg` as `cloud-init` will skip network configuration if it's present:

```bash
rm -f /etc/cloud/cloud.cfg.d/subiquity-disable-cloudinit-networking.cfg
```

Update `99-pve.cfg`:

```bash
cat << EOF > /etc/cloud/cloud.cfg.d/99-pve.cfg
datasource_list: [ConfigDrive, NoCloud]
EOF
```

Remove Netplan files, they will not be regenerated if they exist:

```bash
rm -f /etc/netplan/00-installer-config.yaml
rm -f /etc/netplan/50-cloud-init.yaml
```

Run `cloud-init` clean:

```bash
cloud-init clean
```

Next, reboot the system and confirm the network interface is labeled `eth0` once the machine comes back up. Then, clear BASH history for root. The history entry has a copy in the memory and it will flush back to the file when you log out. You can avoid this with the following command:

```bash
cat /dev/null > ~/.bash_history && history -c && exit
```

Shutdown the system:

```bash
shutdown -h now
```

Convert the VM to a template in vCenter before moving back to Morpheus to onboard the image and use it to begin building your provisioning library.

### 12.2.11 Provisioning Your First Instance

At this point, we are ready to provision our first image. As a first instance, we’ll provision an Apache web server to our vCenter cloud.

Navigate to |ProIns|. If any instances are currently provisioned, we will see them listed here. To start a new instance we click the “+ADD” button to pop the “CREATE INSTANCE” wizard. We’ll scroll down to and select the Apache instance type and click “NEXT”.

---

```bash
substitution
```
First, we’ll specify the group to provision into which determines the clouds available. If you’ve followed this guide to this point, you should at least have a group that houses all of your clouds which you can select here. This will allow us to select the vCenter cloud from the “CLOUD” dropdown menu. Provide a unique name to this instance and then click “NEXT”.

From the “CONFIGURE” tab, we’re presented with a number of options. The options are cloud and layout-specific, more generalized information on creating instances and available options is here. For our purposes, we’ll select the following options:

- **LAYOUT**: Includes options such as the base OS, custom layouts will also be here when available
- **PLAN**: Select the resource plan for your instance. Some plans have minimum resource limits, Morpheus will only show plans at or above these limits. User-defined plans can also be created in |AdmPla|.
- **VOLUMES and DATASTORES**: The minimum disk space is set by the plan, this value may be locked if you’ve selected a custom plan that defines the volume size
- **NETWORKS**: Select a network, note that IP pools must be linked with the networks defined in VMware in order to assign static IP addresses

Under the “User Config” drawer, mark the box to “CREATE YOUR USER”. Click “NEXT”.

---

12.2. Getting started with Morpheus and VMware
Note: "CREATE YOUR USER" will seed a user account into the VM with credentials set in your Morpheus user account settings. If you’ve not yet defined these credentials, you can do so by clicking on your username in the upper-right corner of the application window and selecting “USER SETTINGS”.

For now, we’ll simply click “NEXT” to move through the “AUTOMATION” tab but feel free to stop and take a look at the available selections here. There is more information later in this guide on automation and even more beyond that in the rest of Morpheus docs.

Review the settings for your first instance and click “COMPLETE”.

---

Chapter 12. Guides
We are now dropped back onto the instances list page. We can see a new entry in the list at this point with a status indicator that the new machine is being launched (rocket icon in the status field). We can double click on the instance in the list to move to the instance detail page. For now we will see a progress bar indicating that the instance is being created and is starting up. The exact amount of time this process will take depends on your environment and selections made when provisioning the instance. Initially, Morpheus will guess as to how long this will take and the progress bar may not be accurate. Over time, Morpheus will learn how long these processes take and progress bar accuracy will improve. For more detailed information on the status of various provisioning processes, we can scroll down and select the “HISTORY” tab. The “STATUS” icon will change from the blue rocket to a green play button when the instance is fully ready. Furthermore, we can click on the hyperlinked IP address in the “VMS” section of this page to view a default page in a web browser to confirm success.
12.2.12 Creating Your First Library Item

In the prior section, we manually provisioned our first instance. However, Morpheus allows you to build a catalog of custom provisionable items to simplify and speed provisioning in the future. In this section, we’ll build a catalog item and show how that can translate into quick instance provisioning after configuration.

Note: Before starting this process, it’s important to decide which virtual image you plan to use. If you’re not using a Morpheus-provided image, you’ll want to ensure it’s uploaded. You will not be able to complete this section without selecting an available image. In this example we will use Morpheus Redis 3.0 on Ubuntu 14.04.3 v2.

Navigate to Library > Blueprints > Node Types and click “+ADD”.

In this example, I am going to set the following options in the “NEW NODE TYPE” wizard:

• NAME

• SHORT NAME

• VERSION: 1 (In this particular case, the version is not important)

• TECHNOLOGY: VMware

• VM IMAGE: Morpheus Redis 3.0 on Ubuntu 14.04.3 v2

Note: Within the “VMware VM Options” section you should add anything that will always be used for this node, regardless of the specific deployment details. This can include LDAP Authentication, bash scripts that should run on installation, among other things.
With the new node created, we’ll now add a new instance type which will be accessible from the provisioning wizard once created. Move from the “NODE TYPES” tab to the “INSTANCE TYPES” tab and click “+ADD”.

<table>
<thead>
<tr>
<th>NAME</th>
<th>customnodetype</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHORT NAME</td>
<td>customnodetype</td>
</tr>
<tr>
<td>VERSION</td>
<td>1</td>
</tr>
<tr>
<td>TECHNOLOGY</td>
<td>VMware</td>
</tr>
</tbody>
</table>

### VMware VM Options

- **VM IMAGE**: Morpheus Redis 3.0 on Ubuntu 14.04.3 v2

- **LOG FOLDER**

- **CONFIG FOLDER**

- **DEPLOY FOLDER**
  
  (Optional) If using deployment services, this mount point will be replaced with the contents of said deployments.

- **EXTRA OPTIONS**

- **SERVICE PORTS**
  
  `port`  
  `name`  
  `No LB`  

- **SCRIPTS**

- **FILE TEMPLATES**

  ```
  Advanced Options
  ```

  **SAVE CHANGES**
In the “NEW INSTANCE TYPE” wizard, I’ll simply enter a **NAME** and **CODE** value. Click “SAVE CHANGES”.

Now that we’ve created a new instance type, access it by clicking on the name in the list of custom instances you’ve created. In my case, I’ve given the name “NewInstanceType”.

Once we’ve opened the new instance type, by default, we should be on the “LAYOUTS” tab. Click “+ADD LAYOUT”.

I’ve set the following fields on my example layout:

- **NAME**
- **VERSION**: This is the version number of the layout itself, which is labeled 1.0 in the example
- **TECHNOLOGY**: VMware
• **Nodes**: Select the node we created earlier, if desired you can specify multiple nodes

Click “SAVE CHANGES”.

At this point we’ve completed the setup work and can now provision the instance we’ve created to our specifications. Navigate to [ProIns] and click “+ADD”. From the search bar we can search for the new instance type we’ve created. In the example case, we called it “newinstancetype”. Click “NEXT”.

12.2. Getting started with Morpheus and VMware
As before, we can select a group and cloud to provision this new instance. Click “NEXT”. On the “CONFIGURE” tab, make note that the layout and plan are already selected because they were configured as part of creating the new instance type. Select a network and click “NEXT”. Once again we will also click “NEXT” through the “AUTOMATION” tab. Finally, click “COMPLETE”.

As before when we manually provisioned an instance, Morpheus will now begin to spin up the new VM. How long this will take depends on your environment but Morpheus will predict how long this process will take and represent that on a progress bar. Over time, Morpheus begins to learn how long these processes take and becomes more accurate
in predicting spin-up time.

Once the provisioning process has completed, open the instance detail page in Morpheus and click on the “CONSOLE” tab. You’ll be logged in with your user account and are then able to confirm the machine is ready and available.

12.2.13 Automation and Configuration Management

Morpheus automation is composed of Tasks and Workflows. A task could be a script added directly, scripts or blueprints pulled from the Morpheus Library, playbooks, recipes, or a number of other things. The complete list of task types can be found in the Automation section of Morpheus docs. Tasks can be executed individually but they are often combined into workflows. We can opt to run a workflow at provision time or they can be executed on existing instances through the Actions menu.

In this guide we will set up an Ansible integration, create a task, add the task to a workflow, and run the workflow against a new and existing instance. If you’ve worked through this guide to this point, you should already have an Apache instance running. If you don’t yet have that, provision one before continuing with this guide and ensure it’s reachable on port 80.
We’ll first set up the Ansible integration, you can integrate with the sample repository referenced here or integrate with your own. Go to ‘Administration > Integrations’. Click “+NEW INTEGRATION” and select Ansible from the dropdown menu. Fill in the following details:

- **NAME**
- **ANSIBLE GIT URL**: https://github.com/ncelebic/morpheus-ansible-example, or enter the URL for your own Ansible git repository
- **PLAYBOOKS PATH**
- **ROLES PATH**
  - Mark the box to “USE MORPHEUS AGENT COMMAND BUS”

**Note:** If your git repository requires authentication, you should create a keypair and use the following URL format: `git@github.com:ncelebic/morpheus-ansible-example.git`.

Click “SAVE CHANGES”. You’ll now see our new Ansible integration listed among any other configured integrations.
tions. If we click on this new integration to view detail, a green checkmark icon indicates the git repository has been fully synced.

With the Ansible integration set up, we can now create a task that includes our playbook. Go to |LibAut|, click “+ADD”. We’ll first set our “TYPE” value to Ansible Playbook so that the correct set of fields appear in the “NEW TASK” wizard. Set the following options:

- **NAME**
- **ANSIBLE REPO**: Here we will choose the Ansible integration that we just created
- **PLAYBOOK**: In our example case, enter ‘playbook.yml’

Click “SAVE CHANGES” to save our new task. We can test the new task on our Apache VM now by going to |ProIns| and clicking into our VM. From the “ACTIONS” menu select “Run Task”. From the “TASK” dropdown menu, select the task we just added and click “EXECUTE”.

To see the progress of the task, click on the “HISTORY” tab and click on the (i) button to the right of each entry in the list. In this case, we can also see the results of the task by clicking on the link in the “LOCATION” column of the “VMS” section.

Now that our task is created, we can put it into a workflow. Back in |LibAut| we will click on the “WORKFLOWS” tab. Click “+ADD” and select Provisioning Workflow. We’ll give the new workflow a name and expand the Post Provision section. As we begin to type in the name of the task we’ve created, it should appear as a selection. Click “SAVE CHANGES”.

12.2. Getting started with Morpheus and VMware 627
Now that we have a workflow, return to |ProIns| and begin to provision another Apache instance. More detailed instructions on provisioning a new Apache instance are included earlier in this guide if needed. Now, when you reach the “AUTOMATION” section of the “CREATE INSTANCE” wizard, we have a workflow to select. From the “WORKFLOW” dropdown menu, select the workflow we just created and complete provisioning of the new instance.
As the instance is provisioning, we can go to the “HISTORY” tab and see Morpheus executing the tasks that were contained in our workflow.

This is just one example of using Morpheus to automate the process of configuring and instance to your needs. There are a number of other automation types that can be built into your workflows as well. For further information, take a look at the automation integrations guide in Morpheus docs.

12.2.14 Conclusion

At this point you should be up and running in Morpheus, ready to consume VMware. This guide only scratches the surface, there is a lot more to see and do in Morpheus. Take a look at the rest of Morpheus Docs for more information on supported integrations and other things possible.

12.3 Getting started with Morpheus and Azure

12.3.1 Introduction

This guide is designed to help you get started and quickly get the most out of Morpheus with Microsoft Azure public cloud. By the end, you will integrate your first cloud with Morpheus, configure networking, prepare and consume images, provision instances, and get started with automation. We will briefly discuss installation and account setup but will provide links to additional resources for those very first steps. For the most part, this guide assumes you are able to get Morpheus installed and are ready to move forward from that point. There is a lot more to see and do in Morpheus that is beyond the scope of this guide. For more, consult the complete Morpheus documentation or take part in our Reddit user community forum.
12.3.2 Installation & Setup

In the simplest configuration, Morpheus needs one appliance server which will contain all the components necessary to orchestrate virtual machines and containers. Full requirements, including storage and networking considerations, can be found in Morpheus documentation here. In order to provision any new Instances, hosts, or applications (or convert any discovered resources to managed resources) you will need a valid license. If you don’t have one, you can request a community edition license for free at Morpheus Hub. Once obtained, the license can be applied in Administration > Settings > License. For more, take a look at our community edition welcome package.

12.3.3 Groups

Groups in Morpheus define which resources a user has access to. Clouds are added to Groups and a user can only access Clouds that are in the Groups to which their roles give them access. More information on Morpheus Groups is here. A deep dive into Groups goes beyond the scope of this guide but it’s often useful to create a Group that contains all Clouds for testing purposes. We will create that group now so that we can add our first Cloud into this Group in the next section.

Navigate to Infrastructure > Groups. Here we will see a list of all configured groups but, of course, this will be empty immediately after installation. Click “+CREATE”. Give your group a name, such as “All Clouds”. The “CODE” field is used when calling Morpheus through Morpheus API or Morpheus CLI. It’s useful in most cases to have an “All Clouds” group for testing purposes so this will likely help you down the road.

Click SAVE CHANGES. Your Group is now ready to accept Clouds.
12.3.4 Integrating Your First Cloud

Clouds in Morpheus consist of any consumable endpoint whether that be on-prem, public clouds, or even bare metal. In this guide, we will focus on integrating and working with Microsoft Azure public cloud.

To get started, we will navigate to *Infrastructure > Clouds*. This is the Cloud list page which lists all configured Clouds. It will be empty if you’ve just completed installation and setup of Morpheus but soon we will see our integrated Azure cloud here.

Click the “+ADD” button to pop the “CREATE CLOUD” wizard. Select “AZURE (PUBLIC)” and click the “NEXT” button.

On the “CONFIGURE” tab, we’re asked to provide Azure-specific details to connect to the cloud. Morpheus Azure integration requires Owner or Contributor access to subscription via App Registration. Adding an Azure Cloud or Clouds to Morpheus will require the following:

- Azure Subscription ID
- Directory (tenant) ID
- Application (client) ID
- Application (client) Secret
- Application (client) must be Owner or Contributor of Subscription

CSP Accounts require the additional following input:

- CSP Directory (tenant) ID
- CSP Application (client) ID
- CSP Application (client) SECRET
CREATE CLOUD

CLOUD  CONFIGURE  GROUP  REVIEW

NAME

CODE

LOCATION

VISIBILITY: Private

TENANT: morpheus

ENABLED

AUTOMATICALLY POWER ON VMS

Details

CLOUD TYPE: Global

SUBSCRIPTION ID

TENANT ID

CLIENT ID

CLIENT SECRET

LOCATION

RESOURCE GROUP: No Locations found: verify credentials above.

INVENTORY EXISTING INSTANCES

INVENTORY LEVEL: Basic

ACCOUNT TYPE: Standard
Create App Registration

Morpheus authenticates with Azure via an App Registration with an Owner or Contributor Role on a Subscription. Use the steps below to create and collect the required credentials and assign the required permissions to integrate Azure with Morpheus.

**Warning:** Using an App Registration (service principal) that has selective resource permissions and is not an Owner or Contributor of the Subscription is not supported and will cause failures/issues. Please confirm the App Registration you use to integrate Azure with Morpheus has Owner or Contributor permissions on the specified Subscription.

If you do not have an existing Azure Active Directory App Registration, or you wish to use an new one for Morpheus, you will need to create one using the steps below. If you already have one you wish to use, continue to the next section.

1. Log into the Azure portal
2. Select “Azure Active Directory”
3. Select “App Registrations”
4. Select “New Registration”

5. Next, give the app a name, specify Web app / API for the type (default) and enter any URL for the Sign-on URL:
6. Click Create and your new App Registration will be created.
Now that we have our App Registration, we will gather the credentials required for the Morpheus Azure integration in the next section.

Copy Directory (tenant) and Application (client) IDs

The App Registration Directory (tenant) and Application (client) ID are required for the Morpheus Azure integration. Both can be found in the overview section of the App Registration.

1. Go to the Overview section of your App Registration
2. Copy the Directory (tenant) ID
3. Store/Paste for use as the Tenant ID when adding your Azure cloud in Morpheus
4. Copy the Application (client) ID
5. Store/Paste for use as the Client ID when adding your Azure cloud in Morpheus
Generate a Client Secret

While still in your App Registration:

1. Select “Certificates & secrets” in the Manage section
2. Select + New client secret
3. The “Add a client secret” modal will come up
4. Add a description to help identify the secret in the future
5. Select an expiration duration
6. Click Add

7. Copy the newly-generated client secret value.

**Important:** Copy the client secret value before continuing as it will not be viewable again later.

8. Store/Paste client secret for use later when adding your Azure cloud in Morpheus

You now have three of the four credentials required for Morpheus Azure cloud integration. The last credential required is the Azure Subscription ID which we will gather in the next section.
Subscription ID

To get the Azure Subscription ID:

1. Navigate to the Subscriptions section. The search function can help to locate these sections if they aren’t immediately apparent in the UI menu.

2. In the Subscriptions section, copy the Subscription ID.

3. Store/Paste for use as the Subscription ID when adding your Azure cloud in Morpheus.
Make App Registration owner or contributor of Subscription

The App Registration used needs to be an owner of the Azure Subscription used for the Morpheus cloud integration. If lesser permissions are given or permissions are assigned at individual resource levels, Morpheus will not be able to properly inventory existing cloud resources, create resources or remove them.

1. In the Subscriptions section in Azure, select the Subscription
2. In the Subscription pane, select “Access Control (IAM)”
3. Either Click :guilabel:`+ Add`, and then “Add Role Assignment” OR simply select “Add a role assignment”
4. In the right pane, select “Owner” or “Contributor” Role type
5. Search for the name of the App Registration used for the Morpheus integration
6. Select the App Registration in the search results
7. Select “Save”
You now have the required credentials and permissions to add an Azure Cloud integration into Morpheus. Continue on with the next sections of this guide to complete the integration from the Morpheus side.

**Complete the Add Cloud Process in Morpheus**

If you’ve followed this guide from the start, you will already have a Cloud integration modal open in Morpheus UI. If you still need to open that wizard, navigate to Infrastructure > Clouds > + ADD > Azure (Public) and click NEXT. Fill in the following fields with the information gathered in the steps above:

- Subscription ID
- Tenant ID
- Client ID
- Client Secret
- Location
- Resource Group
- Inventory Existing Instances
- Inventory Level
- Account Type

Once valid credentials are populated in the appropriate fields, the LOCATION dropdown menu will be populated. Select an available region, this is also a helpful check to ensure you’ve correctly provided working credentials. In addition, we can scope the cloud integration to all resource groups in the region (All) or can select a specific resource group to limit Morpheus resource inventorying and creation to just that resource group.

By checking INVENTORY EXISTING INSTANCES, Morpheus will automatically onboard existing cloud resources which are scoped to the region and resource group indicated. If this box is checked, we will also need to select either basic inventorying, which syncs name, IP addresses, platform types, power status, and sizing data (storage, CPU, and RAM) OR full (API heavy) inventorying which syncs resource utilization metrics (storage, CPU, and RAM) when available in addition to what we get with basic inventorying.

To move on, expand the “Advanced Options” section.

---

**Note:** CSP accounts will also need to enter CSP TENANT ID, CSP CLIENT ID, and CSP CLIENT SECRET in the Advanced Options section.

Within the “Advanced Options” drawer are additional configurations to consider for your first Cloud. Some of these won’t usable until they reference additional configured integrations. Common settings to consider are DOMAIN, STORAGE TYPE, APPLIANCE URL (overrides the Morpheus URL for external systems), GUIDANCE (setting “Manual” will make recommendations for rightsizing), COSTING, DNS INTEGRATION, CMDB, and AGENT INSTALL MODE.

Once you’re satisfied with your selections, click “NEXT”

We have now arrived at the “GROUP” tab. In this case, we will mark the radio button to “USE EXISTING” Groups if you wish to use the Group we configured earlier. Alternatively, you can create a new one here.
Once you’ve selected or created the Group, click “NEXT”.

On the final tab of the “CREATE CLOUD” wizard, you’ll confirm your selections and click “COMPLETE”. The new Cloud is now listed on the Cloud list page. After a short time, Morpheus will provide summary information and statistics on existing virtual machines, networks, and other resources available in the Cloud.

**Viewing Cloud Inventory**

Now that we’ve integrated our first Azure cloud, we can stop for a moment to review what Morpheus gives us from the Cloud detail page. We can see that Morpheus gives us estimated costs and cost histories, metrics on used resources, and also lists out resource counts in various categories including container hosts, hypervisors, and virtual machines. We can drill into these categories to see lists of resources in the various categories by clicking on the category tabs. We can link to the detail page for any specific resource by clicking on it from its resource category list.

**Configuring Resource Pools**

With our Azure Cloud configured, Morpheus will automatically sync in available resource pools and data stores.

For resource pools, once Morpheus has had time to ingest them, then will be visible from the cloud detail page. Navigate to *Infrastructure > Clouds > (your Azure cloud) > Resources tab*. In here, we are able to see and control access to the various resource pools that have been configured in Azure. For example, we can restrict access to a specific resource pool within Morpheus completely by clicking on the “ACTIONS” button, then clicking “Edit”. If we unmark the “ACTIVE” button and then click “SAVE CHANGES” we will see that the resource pool is now grayed out in the list. The resources contained in that pool will not be accessible for provisioning within Morpheus if it is not configured as active.
Often our clients will want to make specific blocks of resources available to their own customers. This can be easily and conveniently controlled through the same “EDIT RESOURCE POOL” dialog box we were just working in. If we expand the “Group Access” drawer, we are able to give or remove access to each pool to any Group we’d like. We can also choose to make some or all of our resource pools available to every Group. Specific resource pools can also be defined as the default for each Group when needed.
Additionally, we may choose to allow only certain service plans to be provisioned into a specific pool of resources. For example, perhaps a specific cluster is my SQL cluster and only specific services plans should be consumable within it. We can control that through this same dialog box.

**Configuring Data Stores**

To take a look at data stores, we’ll move from the “Resources” tab to the “Data Stores” tab on our Cloud detail page. Morpheus gives the user similar control with data stores to what we saw with our resources pools earlier. Just like with resource pools, we can disable access within Morpheus completely by clicking on “ACTIONS” and then “Edit”. If we unmark the “ACTIVE” checkbox and click “SAVE CHANGES”, you will see that specific data store has been grayed out.
Just like with resource pools, we are also able to scope data stores to specific Groups. This ensures that the members of each Group are only able to consume the data stores they should have access to.

### Configuring Network for Provisioning

When configuring networking, we can set global defaults by going to Infrastructure > Network > NETWORKS tab. Here we can add or configure networks from all Clouds integrated into Morpheus. Depending on the number of clouds Morpheus has ingested, this list may be quite large and may also be paginated across a large number of pages. In such a case, it may be easier to view or configure networks from the specific Cloud detail page so that networks from other Clouds are not shown.

Still in Infrastructure > Network, make note of the “INTEGRATIONS” tab. It’s here that we can set up any integrations that may be relevant, such as IPAM integrations. Generally speaking, when adding IPAM integrations, we simply need to name our new integration, give the API URL, and provide credentials. There’s more information in the IPAM integration section of Morpheus Docs.

In Infrastructure > Networking we can also set up IP address pools from the IP Pools tab. These pools can be manually defined, known as a Morpheus-type IP pool, or they can come from any IPAM integrations you’ve configured. As instances are provisioned, Morpheus will assign IP addresses from the pool chosen during provisioning. When the instance is later dissolved, Morpheus will automatically release the IP address to be used by another instance when needed. When adding or editing a network, we can opt to scope the network to one of these configured IP address pools. Edit an existing network by clicking the pencil icon on the Networks List Page (Infrastructure > Networks > Networks Tab) and fill in the “Network Pool” field to associate the IP Pool with the network.

Since this guide is focused on working within an Azure cloud that we integrated at the start, we will take a look at our
network configurations on the cloud detail page as well. Navigate to Infrastructure > Clouds > (your Azure cloud) > NETWORKS tab. Just as with resource pools and data stores, we have the ability to make certain networks inactive in Morpheus, or scope them to be usable only for certain Groups or Tenants.
Provisioning Your First Instance

At this point, the groundwork is laid and we are ready to attempt our first new provisioning. As a first Instance, we’ll provision an Apache web server to our Azure cloud. Morpheus includes a very robust catalog of pre-configured Instance types. We’ll use one of these included catalog items for this guide but you’ll likely also need to prep your own custom images and Instance types to make available to your users. Much more on this can be found elsewhere in Morpheus documentation.

Navigate to |ProIns|. If any Instances are currently provisioned, we will see them listed here. To start a new Instance we click + ADD to open the “CREATE INSTANCE” wizard. We’ll scroll down to and select the Apache instance type and click “NEXT”.

First, we’ll specify the Group to provision into which determines the Clouds available. If you’ve followed this guide to this point, you should at least have a Group that houses all of your Clouds which you can select here. This will allow us to select the Azure cloud from the “CLOUD” dropdown menu. Provide a unique name to this instance and then click “NEXT”.

From the “CONFIGURE” tab, we’re presented with a number of options. The options are cloud and layout-specific, more generalized information on creating Instances and available options is here. For our purposes, we’ll select the following options:

- **LAYOUT**: Includes options such as the base OS, custom layouts will also be here when available
- **PLAN**: Select the resource plan for your instance. Some plans have minimum resource limits, Morpheus will only show plans at or above these limits. User-defined plans can also be created in |AdmPla|.
- **VOLUMES**: The minimum disk space is set by the plan, this value may be locked if you’ve selected a custom plan that defines the volume size
• **NETWORKS**: Select a network

Under the “User Config” drawer, mark the box to “CREATE YOUR USER”. Click NEXT.

---

**Note:** “CREATE YOUR USER” will seed a user account into the VM with credentials set in your Morpheus user account settings. If you’ve not yet defined these credentials, you can do so by clicking on your username in the upper-right corner of the application window and selecting “USER SETTINGS”.

For now, we’ll simply click NEXT to move through the “AUTOMATION” tab but feel free to stop and take a look at the available selections here. There is more information later in this guide on automation and even more beyond that in the rest of Morpheus docs.

Review the settings for your first instance and click **COMPLETE**.

We are now dropped back onto the Instances list page. We can see a new entry in the list at this point with a status indicator that the new machine is being launched (rocket icon in the status field). We can double click on the Instance in the list to move to the Instance detail page. For now we will see a progress bar indicating that the Instance is being created and is starting up. The exact amount of time this process will take depends on selections made when provisioning the Instance. Initially, Morpheus will guess as to how long this will take and the progress bar may not be accurate. Over time, Morpheus will learn how long these processes take and progress bar accuracy will improve.
For more detailed information on the status of various provisioning processes, we can scroll down and select the “HISTORY” tab. The “STATUS” icon will change from the blue rocket to a green play button when the Instance is fully ready. Furthermore, we can click on the hyperlinked IP address in the “VMS” section of this page to view a default page in a web browser to confirm success.

Creating Your First Library Item

In the prior section, we manually provisioned our first Instance. However, Morpheus allows you to build a catalog of custom provisionable items to simplify and speed provisioning in the future. In this section, we’ll build a catalog item and show how that can translate into quick Instance provisioning after configuration.

Note: Before starting this process, it’s important to decide which virtual image you plan to use. If you’re not using a Morpheus-provided image, you’ll want to ensure it’s configured. You will not be able to complete this section without selecting an available image. In this example we will use a CentOS image that was previously configured in the Morpheus library. If you need to configure your own images prior to starting this section, navigate to Library > Virtual Images and click + ADD. A deeper dive into image prep and virtual image configuration goes beyond the scope of this guide.

Provisionable elements in Morpheus combine a Node Type(s), Layout(s), and an Instance Type. The Overview section of Morpheus docs discusses these objects and how they work together in greater detail. Our first step here will be to create a Node Type which wrap the image itself with additional configuration, templates, and scripts. While not strictly required, creating the Node Type, Instance Type, and then the Layout is often a good workflow for creating Library items. That is the order we will follow in this guide.

Navigate to Library > Blueprints > Node Types and click + ADD

In this example, I am going to set the following options in the “NEW NODE TYPE” wizard:

- **NAME**: Example Azure CentOS 7
- **SHORT NAME**: eac7 (Identifies the Node Type in Morpheus API/CLI)
- **VERSION**: 7 (Ensures the correct Node Types are used when tying Layouts with multiple images to the same Instance Type)
- **TECHNOLOGY**: Azure
- **VM IMAGE**: Azure-Centos-7

Click SAVE CHANGES
EDIT NODE TYPE

NAME
*Example Azure CentOS 7

SHORT NAME
eac7
The short name is a name with no spaces used for display in your container list.

VERSION
7

ENVIRONMENT VARIABLES
Name  Value  

Azure Options

VM IMAGE
Azure-Centos-7

LOG FOLDER

DEPLOY FOLDER
(Optional) If using deployment services, this mount point will be replaced with the contents of said deployments.

SERVICE PORTS
port  name  No LB  +

SCRIPTS
Search

FILE TEMPLATES
Search

Advanced Options

SAVE CHANGES
With the new Node Type created, we’ll now add a new Instance type which will be accessible from the provisioning wizard once created. Move from the “NODE TYPES” tab to the “INSTANCE TYPES” tab and click + ADD.

In the “NEW INSTANCE TYPE” wizard, I’ll simply enter a **NAME** and **CODE** value. Click **SAVE CHANGES**. You could also provide a description, icon, and category for easier identification from the provisioning wizard later.

![EDIT INSTANCE TYPE](image)

Now that we’ve created a new Instance type, access it by clicking on the name in the list of custom Instances you’ve created. In my case, I’ve given the name “**Example Azure CentOS 7**”.

Once we’ve opened the new Instance type, by default, we should be on the “LAYOUTS” tab. Click + **ADD LAYOUT**. I’ve set the following fields on my example layout:

- **NAME**: Example Azure CentOS 7
- **VERSION**: 7 (This is the version number of the layout itself, which is labeled 7 in the example)
- **TECHNOLOGY**: Azure
- **Nodes**: Select the Node Type we created earlier, if desired you can specify multiple nodes

Click **SAVE CHANGES**.
Morpheus Documentation

EDIT LAYOUT

NAME: Harker Azure CentOS 7

VERSION: 7

DESCRIPTION:

☐ CREATABLE

TECHNOLOGY: Azure

MINIMUM MEMORY: 1024 MB

This will override any memory requirement set on the virtual image

WORKFLOW: Select Workflow

☐ SUPPORTS CONVERT TO MANAGED

ENVIRONMENT VARIABLES:

Option Types

Search option types

Nodes

Search nodes

*Example Azure CentOS 7 (7)
At this point we’ve completed the setup work and can now provision the Instance we’ve created to our specifications. Navigate to |ProIns| and click + ADD. From the search bar we can search for the new Instance type we’ve created.

As before, we can select a Group and Cloud to provision this new Instance. Click NEXT. On the “CONFIGURE” tab, make note that the layout and plan are already selected because they were configured as part of creating the new Instance type. Select a network and click NEXT. Once again we will also click NEXT through the “AUTOMATION” tab. Finally, click COMPLETE.

As before when we provisioned a pre-existing Instance from the default catalog, Morpheus will now begin to spin up the new VM. How long this will take depends on the configuration and environmental factors but Morpheus will predict how long this process will take and represent that on a progress bar. Over time, Morpheus begins to learn how long these processes take and becomes more accurate in predicting spin-up time.

Once the provisioning process has completed, open the Instance detail page in Morpheus and click on the “CONSOLE” tab. You’ll be logged in with your user account and are then able to confirm the machine is ready and available, assuming the image and your custom catalog item were configured to seed user accounts and connect back to the Morpheus appliance.
Morpheus Documentation

Automation and Configuration Management

Morpheus automation is composed of Tasks and Workflows. A Task could be a script added directly, scripts or Blueprints pulled from the Morpheus Library, playbooks, recipes, or a number of other things. The complete list of Task types can be found in the Automation section of Morpheus docs. Tasks can be executed individually but they are often combined into workflows. We can opt to run a workflow at provision time or they can be executed on existing instances through the Actions menu.

In this guide we will set up an Ansible integration, create a Task, add the Task to a Workflow, and run the Workflow against a new and existing Instance. If you’ve worked through this guide to this point, you should already have an Apache instance running. If you don’t yet have that, provision one before continuing with this guide and ensure it’s reachable on port 80.

We’ll first set up the Ansible integration, you can integrate with the sample repository referenced here or integrate with your own. Go to ‘Administration > Integrations’. Click +NEW INTEGRATION and select Ansible from the dropdown menu. Fill in the following details:

- **NAME**
- **ANSIBLE GIT URL**: https://github.com/ncelebic/morpheus/-ansible-example, or enter the URL for your own Ansible git repository
- **PLAYBOOKS PATH**
- **ROLES PATH**
- Mark the box to “USE Morpheus AGENT COMMAND BUS”

**Note:** If your git repository requires authentication, you should create a keypair and use the following URL format: git@github.com:ncelebic/morpheus/-ansible-example.git.

Click **SAVE CHANGES**. You’ll now see our new Ansible integration listed among any other configured integrations. If we click on this new integration to view detail, a green checkmark icon indicates the git repository has been fully synced.

With the Ansible integration set up, we can now create a task that includes our playbook. Go to |LibAut|, click + ADD. We’ll first set our “TYPE” value to Ansible Playbook so that the correct set of fields appear in the “NEW TASK” wizard. Set the following options:

- **NAME**
- **ANSIBLE REPO**: Here we will choose the Ansible integration that we just created
- **PLAYBOOK**: In our example case, enter ‘playbook.yml’

Click “SAVE CHANGES” to save our new task. We can test the new task on our Apache VM now by going to |ProIns| and clicking into our VM. From the “ACTIONS” menu select “Run Task”. From the “TASK” dropdown menu, select the task we just added and click “EXECUTE”.

To see the progress of the task, click on the “HISTORY” tab and click on the (i) button to the right of each entry in the list. In this case, we can also see the results of the task by clicking on the link in the “LOCATION” column of the “VMS” section.

Now that our task is created, we can put it into a workflow. Back in |LibAut| we will click on the “WORKFLOWS” tab. Click “+ADD” and select Provisioning Workflow. We’ll give the new workflow a name and expand the Post Provision section. As we begin to type in the name of the task we’ve created, it should appear as a selection. Click “SAVE CHANGES”.

Now that we have a Workflow, return to |ProIns| and begin to provision another Apache instance. More detailed instructions on provisioning a new Apache instance are included earlier in this guide if needed. Now, when you...
reach the “AUTOMATION” section of the “CREATE INSTANCE” wizard, we have a workflow to select. From the “WORKFLOW” dropdown menu, select the workflow we just created and complete provisioning of the new instance.

As the instance is provisioning, we can go to the “HISTORY” tab and see Morpheus executing the tasks that were contained in our workflow.

This is just one example of using Morpheus to automate the process of configuring an instance to your needs. There are a number of other automation types that can be built into your Workflows as well. For further information, take a look at the [automation integrations](https://morpheusdocs.com) guide in Morpheus docs.

**Conclusion**

At this point you should be up and running in Morpheus, ready to consume Azure public cloud. This guide only scratches the surface, there is a lot more to see and do in Morpheus. Take a look at the rest of [Morpheus Docs](https://morpheusdocs.com) for more information on supported integrations and other things possible.

**12.4 Morpheus Virtual Desktops**

**12.4.1 VDI Pools Overview**

The VDI Pools section of Morpheus Tools provides a management area for defining VDI Pools and VDI Apps that a user can consume within the Virtual Desktop Persona.

Pools can be either persistent or non-persistent and have various controls pertaining to idle pools and minimum or maximum sizes. The idea here is to make sure a server is always quickly available to accommodate user demand.

Morpheus leverages its Instance Types concept for provisioning servers within the VDI Pool. All the options available during Instance provisioning is available for setting the base server configuration. This includes Workflows, domain joins, tagging, image selection and more.

A timeout setting can also be applied to release pool allocations from a user once they have disconnected their session. For non-persistent pools, a good recommendation is ten minutes whereas, for a persistent pool, a sensible recommendation would be around one hour.

Pool behavior changes depending on the pool type. In a non-persistent pool, when a timeout period expires, the VM is destroyed and a new one is allocated for use. This functionality will change based on the cloud technology in a future update allowing for potential recycling of the VMs. In a Persistent pool, when the lease timeout expires, the Instance will shutdown until the user requests it again in the future. It is important to note that lease timeouts auto-extend for as long as the user is logged into or browsing any area of the Morpheus application. Once the user closes their browser or logs out of their session, the timeouts will no longer auto-extend.

**12.4.2 Configuring Access to VDI Pools**

Access to the Virtual Desktop Persona and individual VDI pools is handled through the user Role and, where applicable, Tenant Role. When creating a new Role, access is restricted to the Virtual Desktop Persona and all VDI pools by default. To grant access:

1. Navigate to the Role (Administration > Roles > Selected Role)
2. Access the Personas tab
3. Toggle the Virtual Desktop permission to “Full” or “None”
4. Access the VDI Pool Access tab
5. Toggle access to selected VDI pools to “Full” or “None”, you can also toggle permission on all pools to “Full” or “None” with the Global Access selection

6. Role changes are saved automatically, there is no need to manually save

Additionally, users should have a Linux and/or Windows username and password configured in their user profiles in order for virtual desktop login to be as seamless as possible. User profiles are accessed by clicking on the user’s name in the upper-right corner of the application windows and clicking USER SETTNGS. The section to enter Windows and Linux account credentials is in the right column of the page.

12.4.3 Creating VDI Templates

**Note:** The following guide focuses on VMware and Windows but is applicable to most cloud environments. Morpheus also supports Linux virtual desktops.

1. Create a thin-provisioned VM in the VMware vCenter console. It’s recommended you allocate at least 50 GB of storage, at least 2 vCPU and at least 8 GB RAM on the template. Smaller VMs can be deployed from this template later.

2. Install a Windows operating system, there is no need to supply a license during deployment.

3. Supply the initial username and password

4. Install any updates, applications or optimizations. See the next section for recommended optimizations for the most performant virtual desktop experience

5. Shutdown the VM and convert to a template. Optionally, you can also use the Linked Clones (VMware) process which is described in a later section

**Suggested Optimizations**

Reducing display and input delays is key to providing the best virtual desktop experience for the user. Consider the following optimizations for VDI desktops and servers:

- Disable desktop wallpapers
- Implement Roaming Profiles
- Enforce WDDM remote display driver
- Re-enable local Administrator
- Delete the initial created user profile
- Clean up any unneeded installer packages

Additionally, there are a number of OS optimization tools available on the Internet which are specific to VDI use cases.
Linked Clones

Linked Clones are a feature of VMware which references snapshots of a VM to deploy from. This adds the advantage of quicker clone times and the ability to more easily share small modifications to a file system. Morpheus supports Linked Clones but recommends them for VDI workloads only.

**Note:** Linked Clones are not templates but rather powered down VMs.

1. Locate the VM you desire to have the Linked Clone in Morpheus. If it’s not currently managed by Morpheus, navigate to the appropriate Cloud (Infrastructure > Clouds), find the VM on the “VMs” tab, and click “Convert to Managed” from the ACTIONS menu

2. In the CONVERT TO INSTANCE modal, select “No Agent Install” in the AGENT field

3. If snapshots are already on the VM, these will now be synced by Morpheus. If you have not yet created a snapshot, do so in the vCenter console (and refresh the Cloud integration in Morpheus afterward) or from the ACTIONS menu in Morpheus itself. Be sure to take a snapshot of a powered-off VM and give the snapshot a name that will be identifiable for administrators

4. From the Instance detail page in Morpheus, navigate to the Backups tab to find the snapshot

5. Select “More” and create the Linked Clone

6. The Linked Clone will now appear in the Morpheus Virtual Image repository (Library > Virtual Images), ready to use with your custom Layouts

**Note:** You should modify the Virtual Image to “Force Guest Customization” unless you *sysprep* your VM at shutdown time

12.4.4 Creating or Editing a VDI Pool

VDI pools are configured from the Tools menu (VDI Pools selection). The following information is displayed in the VDI pools list view, bear in mind some fields may be hidden depending on how you’ve configured your VDI pools list view (gear icon):

- **TYPE:** An icon indicating the machine type associated with the pool. Morpheus includes many logos out of the box and also allows users to set their own custom icons

- **NAME:** The friendly name given to the VDI pool

- **PERSISTENT:** A check mark will appear when the VDI pool is configured for persistent virtual desktops

- **ENABLED:** A check mark will appear when the VDI pool is enabled and visible to users whose Role permissions allow them access

- **POOL USAGE:** A graph representing the usage of the VDI pool. The total length of the bar represents the maximum pool size based on the configuration. Green segments represent available virtual desktops, blue segments represent reserved virtual desktops, yellow segments represent virtual desktops which are being prepared, and gray segments represent additional pool capacity which could be made available depending on how many virtual desktops are currently reserved and how many idle machines you’ve configured the pool to keep available

- **DESCRIPTION:** A description of the virtual desktop type, if provided
Create a VDI pool by selecting + ADD from the VDI Pools tab or edit an existing one by clicking on the pencil icon from the appropriate row. Configure the following, fields containing a vertical blue bar along the left edge are required:

- **NAME**: A friendly name for the VDI pool in Morpheus
- **DESCRIPTION**: A description of the virtual desktop type
- **MIN IDLE**: The minimum number of virtual desktops that should remain idle and ready
- **INITIAL POOL SIZE**: The number of virtual desktops that will be prepared when the pool is created or enabled
- **MAX IDLE**: The maximum number of virtual desktops that remain idle and ready. Machines will be shut down as necessary when this number is exceeded due to users vacating their machines
- **MAX SIZE**: The total number of virtual desktops this pool can have. Additional users will not be able to access machines once this number is reached
- **LEASE TIMEOUT (MINUTES)**: The user lease time on a virtual desktop they’ve reserved. The lease will continue to auto-renew itself as long as the user is logged into Morpheus. Once the user has logged out and the lease timeout period has expired, the machine will be released as appropriate based on your configuration
- **PERSISTENT**: Pools with persistent virtual desktops will reserve a machine for each user in order to preserve settings, installed applications, work files and more. Machines in persistent pools will be shut down rather than destroyed when they are no longer in use
- **RECYCLABLE**: When enabled, the VDI Instance will revert back to a snapshot and become available once again after the user has logged out and the VDI session has expired. This behavior will not apply to VDI pools which are also configured to be persistent because in that configuration the Instance is merely stopped and saved for the user’s next session. This feature is currently only available for Cloud types which support snapshot management (VMware, Nutanix, and vCD)
- **ALLOW COPY** Enables or disables the ability for the VDI user to copy contents from the VDI instance to the local clipboard
- **ALLOW PRINTER** When enabled, users local system printers can be targeted from the VDI Instance
- **ALLOW HYPERVISOR CONSOLE**: When checked, native cloud console will be enabled (if available) rather than using Morpheus-native RDP/SSH capability
- **AUTO CREATE LOCAL USER UPON RESERVATION**: When marked, the user configured in Morpheus user settings will be created when the machine is initially accessed. If unchecked or if there is no user configured in Morpheus user settings, ensure the machine is joining a domain or there is a known user on the machine image in order to allow access
- **ENABLED**: When marked, the initial pool size will begin to deploy once the VDI pool is saved. The icon for this desktop environment will also be presented to Virtual Desktop Persona users
• **CONFIGURE:** Click this button to configure the deployment configuration each system will use. The wizard is identical to the Instance provisioning wizard meaning all available Instance Types, Workflows, and more are available to virtual desktop machine creation. Consult the steps above to see an example VDI image prep walkthrough.

• **LOGO:** Upload or select a logo to represent the virtual desktop type to users.

• **VDI APPS:** Optionally select one or more frequently-used applications the user can launch directly. Users will also have the option to launch into the desktop.

• **VDI GATEWAY** Select a configure VDI Gateway for VDI sessions to be redirected to. VDI sessions will be redirected to the gateway when a gateway is specified.

**Guest Console SSH Tunnel (optional)** A Jump Host can be configured for VDI session connections. Morpheus will tunnel through the Jump Host when connecting Guest Console sessions for VDI. This is not applicable for Hypervisor Console connections.

• **GUEST CONSOLE JUMP HOST** Jump Host IP address or hostname used to connect to the Jump Host for Guest Console sessions to VDI Instances.

• **GUEST CONSOLE JUMP USERNAME** Jump Host Username used to connect to the Jump Host for Guest Console sessions to VDI Instances.

• **GUEST CONSOLE JUMP PORT** Jump Host Port used to connect to the Jump Host for Guest Console sessions to VDI Instances.

• **GUEST CONSOLE JUMP PASSWORD** Jump Host Password used to connect to the Jump Host for Guest Console sessions to VDI Instances (optional if key specified).

• **GUEST CONSOLE KEYPAIR** Jump Host SSH Key used to connect to the Jump Host for Guest Console sessions to VDI Instances (optional if password specified).

**Note:** A Guest Console Keypair included here must be a local keypair, not a synced keypair.

---

**EDIT VDI POOL**

<table>
<thead>
<tr>
<th>NAME</th>
<th>Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>DESCRIPTION</td>
<td>Windows VDI Desktop</td>
</tr>
<tr>
<td>MIN SIZE</td>
<td>1</td>
</tr>
<tr>
<td>Sets the minimum number of idle instances on standby in the pool. The pool will always try to maintain this number of available instances on standby.</td>
<td></td>
</tr>
<tr>
<td>INITIAL POOL SIZE</td>
<td>1</td>
</tr>
<tr>
<td>The initial size of the pool to be allocated on creation.</td>
<td></td>
</tr>
<tr>
<td>MAX SIZE</td>
<td>1</td>
</tr>
<tr>
<td>Sets the maximum number of idle instances on standby in the pool. If the number of idle instances surpasses this, the pool will start removing instances.</td>
<td></td>
</tr>
<tr>
<td>MAX POOL SIZE</td>
<td>1</td>
</tr>
<tr>
<td>Max limit on number of allocations and instances within the pool.</td>
<td></td>
</tr>
<tr>
<td>LEASE TIMEOUT MINUTES</td>
<td>1</td>
</tr>
</tbody>
</table>

---

**12.4. Morpheus Virtual Desktops** 657
12.4.5 Creating or Editing a VDI Apps

VDI Apps allow users to launch directly into commonly-used apps rather than the OS desktop. Currently, VDI Apps only work with RDP Windows Instances, taking advantage of native Windows Remote Application functionality. Natively-hosted remote desktop applications can only be presented from Windows 10 Enterprise and Education. Other versions of Windows 10 can present remote applications using the procedure below:

1. Open the Windows Registry Editor
2. Locate the following entry: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\TSAppAllowList`
3. Navigate to `fDisabledAllowList` and set its value to “1” in the right-hand pane
4. Add a new key under `TSAppAllowList` and name it “Applications”
5. Add a new key under “Applications” using any name you’d like
6. Within this new key, create two new string values, one called “Name” and one called “Path”
7. The string value for “Name” should describe the application (ex. “Notepad”)
8. The string value for “Path” should be the absolute path to the executable for that application (ex. “C:\Windows\System32\notepad.exe”)

VDI Apps are created by selecting + ADD from the VDI Apps tab or edit an existing one by clicking on the pencil icon from the appropriate row. Configure the following, fields containing a vertical blue bar along the left edge are required:

- **NAME**: A friendly name for the VDI App in Morpheus
- **DESCRIPTION**: A description of the virtual app type
- **LAUNCH PREFIX**: A reference to the remote app registry prepended with two pipes (||). For example, we might create a registry “Chrome” for a Chrome browser VDI App and the associated launch prefix would be “||Chrome”
- **LOGO**: Upload or select a logo to represent the virtual app type to users

12.4.6 VDI Gateways

The Morpheus Worker is a light weight distributed worker daemon as well as a scalable VDI Gateway. Currently, the features center around VDI Gateway but will expand to support full plugin workloads as well as agent relay capabilities.

Adding VDI Gateways to Morpheus

VDI Gateways can be linked to a Morpheus appliance and then used in VDI Pool configurations. VDI sessions will be redirected to configured gateways instead of the Morpheus appliance when a VDI Gateway is specified for a VDI Pool.

**Note**: A VDI Gateway is a separate VM or container Instance used to route users to VDI Instances. The Morpheus VDI Gateway section is for configuring a connection to a VDI Gateway, not creating the gateway Instance itself.

- **NAME** Specify a name for the VDI Gateway in Morpheus. Note that the VDI Gateway Name is not used when connecting to the gateway
- **DESCRIPTION** Specify a description for the VDI Gateway in Morpheus. (optional)
• **GATEWAY URL** The url of the VDI Gateway. This url is used to connect to the gateway, and should match the worker url of the VDI Gateway.

Upon creation, the VDI Gateway record will produce an API KEY. This API KEY needs to be specified in the `morpheus-worker.rb` file on the API Gateway itself under `worker['apikey'] = '$API_KEY`

### VDI Gateway VM Install

A VDI Gateway VM is installed and configured similarly to a Morpheus appliance via **rpm** or **deb** package.

**Note:** VDI Gateway Package URLs are available at [https://morpheushub.com](https://morpheushub.com) in the downloads section.

### Requirements

**Table 1: Supported VDI Gateway Operating Systems**

<table>
<thead>
<tr>
<th>OS</th>
<th>Version(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Linux</td>
<td>2</td>
</tr>
<tr>
<td>CentOS</td>
<td>7.x, 8.x</td>
</tr>
<tr>
<td>Debian</td>
<td>10</td>
</tr>
<tr>
<td>RHEL</td>
<td>7.x, 8.x</td>
</tr>
<tr>
<td>SUSE SLES</td>
<td>12</td>
</tr>
<tr>
<td>Ubuntu</td>
<td>18.04, 20.04</td>
</tr>
</tbody>
</table>

- **Memory:** 4 GB RAM minimum recommended for default installations supporting up to 20 concurrent sessions. Add 50 MB RAM per additional concurrent session
- **Storage:** 10 GB storage minimum recommended. Storage is required for VDI Gateway Packages and log files
- **CPU:** 4-core minimum recommended
- Network connectivity to and from Morpheus appliance and from users to the VDI Gateway over TCP 443 (HTTPS)
- Superuser privileges via the **sudo** command for the user installing the Morpheus VDI Gateway package
- Access to base **yum** or **apt** repos. Access to Optional RPM repos may be required for RPM distros

1. Download the target distro & version package for installation in a directory of your choosing. The package can be removed after successful installation.

```bash
wget https://downloads.morpheusdata.com/path/to/morpheus-worker-$version.$distro
```

2. Validate the package checksum matches source checksums. For example:

```bash
sha256sum morpheus-worker-$version.$distro
```

3. Next install the package using your selected distribution’s package installation command and your preferred opts. Example, for RPM:

```bash
sudo rpm -ihv morpheus-worker-$version.$distro
```

(continues on next page)
Thank you for installing Morpheus Worker!
Configure and start the Worker by running the following command:

```
sudo morpheus-worker-ctl reconfigure
```

4. Configure the gateway by editing `/etc/morpheus/morpheus-worker.rb` and updating the following:

```ruby
worker_url 'https://gateway_worker_url' # This is the gateway URL the |morpheus| appliance can resolve and reach on 443
worker['appliance_url'] = 'https://morpheus_appliance_url' # The resolvable URL or IP address of |morpheus| appliance which the gateway can reach on port 443
worker['apikey'] = 'API KEY FOR THIS GATEWAY' # VDI Gateway API Key generated from |morpheus| Appliance VDI Pools > VDI Gateways configuration
```

**Note:** By default the worker_url uses the machine’s hostname, ie `https://your_machine_name`. The default worker_url value can be changed by editing `/etc/morpheus/morpheus-worker.rb` and changing the value of worker_url. Additional appliance configuration options are available below.

5. After all configuration options have been set, run `sudo morpheus-worker-ctl reconfigure` to install and configure the worker, nginx and guacd services:

```
sudo morpheus-worker-ctl reconfigure
```

The worker reconfigure process will install and configure the worker, nginx and guacd services and dependencies.

**Tip:** If the reconfigure process fails due to a missing dependency, add the repo that the missing dependency can be found in and run

```bash
Note: Configuration options can be updated after the initial reconfigure by editing `/etc/morpheus/morpheus-worker.rb` and running `sudo morpheus-worker-ctl reconfigure` again.
```

6. Once the installation is complete the morpheus worker service will automatically start and open a web socket with the specified Morpheus appliance. To monitor the startup process, run `morpheus-worker-ctl tail` to tail the logs of the worker, nginx and guacd services. Individual services can be tailed by specifying the service, for example `morpheus-worker-ctl tail worker`

**VDI Gateway Docker Install**

To Use VDI Gateway within a Docker container, a few pieces of information are needed.

Firstly, in Morpheus, go to **Tools > VDI Pools > VDI Gateways** and create a new VDI Gateway Record. Be sure to set the HTTPS URL as Morpheus will need to be able to redirect the user’s browser to that page. An API Key will be generated. Make note of this as you will need it later.

Now Simply run with:

```bash

---

660 Chapter 12. Guides
This will setup an HTTPS self-signed exposed port on 8443 for the vdi gateway. It is highly recommended to use valid certificates on your VDI Gateways. It could be terminated at the VIP or a p12 SSL File can be used and configured for the container.

If the docker entrypoint detects a file at /etc/certs/cert.p12, SSL Will be enabled on port 8443 instead. be sure to set environment variables MORPHEUS_SSL_ALIAS and MORPHEUS_SSL_PASSWORD when using p12 files.

If you wish to run in HTTP mode and SSL terminate at the VIP, you can run the container like so:

```
```

**VDI Gateway Helm Chart Installation**

First, configure the Helm repository:

```
helm repo add morpheusdata https://gomorpheus.github.io/helm-charts-morpheus/
```

Next, install the Morpheus worker using helm install. You can specify each parameter using --set key=value[,key=value] arguments as in the following example:

```
helm install morpheus-worker --set replicaCount="1" morpheusdata/morpheus-worker
```

Alternatively, you can create a values YAML file and pass an argument as in the following example:

```
helm install -f values.yaml morpheus-worker morpheusdata/morpheus-worker
```

Upgrading the workers node(s) is as simple as refreshing the repo and using helm upgrade:

```
helm repo update
helm upgrade -f values.yaml morpheus-worker morpheusdata/morpheus-worker
```

To uninstall, use one of the following:

```
helm uninstall morpheus-worker
```

or

```
helm delete morpheus-worker --purge
```

**Note:** helm delete removes all the Kubernetes components associated with the chart and deletes the release.

The following table lists the configurable parameters of the Sentry chart and their default values:
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>image.repository</td>
<td>Image repository</td>
<td>morpheusdata/morpheus-worker</td>
</tr>
<tr>
<td>image.tag</td>
<td>Image tag. Possible values listed here.</td>
<td>5.3.1-4</td>
</tr>
<tr>
<td>image.pullPolicy</td>
<td>Image pull policy</td>
<td>IfNotPresent</td>
</tr>
<tr>
<td>env.MORPHEUS_KEY</td>
<td>API Key for Morpheus Worker</td>
<td></td>
</tr>
<tr>
<td>env.MORPHEUS_URL</td>
<td>Morpheus FQDN with protocol</td>
<td></td>
</tr>
<tr>
<td>env.MORPHEUS_SELF_SIGNED</td>
<td>Is Morpheus using a Self Signed Certificate</td>
<td>false</td>
</tr>
<tr>
<td>service.type</td>
<td>Kubernetes service type for the GUI</td>
<td>ClusterIP</td>
</tr>
<tr>
<td>service.port</td>
<td>Kubernetes port where the GUI is exposed</td>
<td>8989</td>
</tr>
<tr>
<td>livenessProbe.initialDelaySeconds</td>
<td>Initial delay (seconds) for liveness monitoring</td>
<td>5</td>
</tr>
<tr>
<td>livenessProbe.timeoutSeconds</td>
<td>Timeout (seconds) before health check considered unhealthy</td>
<td>5</td>
</tr>
<tr>
<td>livenessProbe.periodSeconds</td>
<td>Poll interval (seconds) between health checks</td>
<td>10</td>
</tr>
<tr>
<td>livenessProbe.failureThreshold</td>
<td>Number of failed polls before restarting service</td>
<td>3</td>
</tr>
<tr>
<td>replicaCount</td>
<td>Number of Replicas if AutoScaling False</td>
<td>1</td>
</tr>
<tr>
<td>autoscaling.enabled</td>
<td>Enable AutoScaling</td>
<td>false</td>
</tr>
<tr>
<td>autoscaling.minReplicas</td>
<td>Minimum number of Replicas</td>
<td>1</td>
</tr>
<tr>
<td>autoscaling.maxReplicas</td>
<td>Maximum number of Replicas</td>
<td>100</td>
</tr>
<tr>
<td>autoscaling.targetCPUUtilizationPercentage</td>
<td>CPU Threshold for AutoScaling</td>
<td>80</td>
</tr>
<tr>
<td>autoscaling.targetMemoryUtilizationPercentage</td>
<td>Memory Threshold for AutoScaling</td>
<td></td>
</tr>
<tr>
<td>ingress.enabled</td>
<td>Enables Ingress</td>
<td>false</td>
</tr>
<tr>
<td>ingress.annotations</td>
<td>Ingress annotations</td>
<td>{}</td>
</tr>
<tr>
<td>ingress.path</td>
<td>Ingress path</td>
<td>/</td>
</tr>
<tr>
<td>ingress.hosts</td>
<td>Ingress accepted hostnames</td>
<td>chart-example.local</td>
</tr>
<tr>
<td>ingress.tls</td>
<td>Ingress TLS configuration</td>
<td>[]</td>
</tr>
<tr>
<td>resources</td>
<td>CPU/Memory resource requests/limits</td>
<td>{}</td>
</tr>
<tr>
<td>nodeSelector</td>
<td>Node labels for pod assignment</td>
<td>{}</td>
</tr>
<tr>
<td>tolerations</td>
<td>Toleration labels for pod assignment</td>
<td>[]</td>
</tr>
<tr>
<td>affinity</td>
<td>Affinity settings for pod assignment</td>
<td>{}</td>
</tr>
</tbody>
</table>

### 12.4.7 Virtual Desktop Persona Overview

The Morpheus VDI Persona provides a virtual desktop environment to grant users access to workstations and applications in a secure manner. Deploy pools of virtual machines on any supported Morpheus Cloud for users to reserve and use! Morpheus leverages open source client technologies, such as Apache Guacamole, to provide a performant and secure virtual desktop client for the end user while wrapping its frontend in a completely new framework. For information on configuring VDI pools for consumption in the Virtual Desktop Persona, see the Tools section of Morpheus docs.

**Note:** This is not an integration with existing VDI Pool Managers such as VMWare Horizon, Citrix VDI, or Nutanix XiFrame. It is a standalone Morpheus feature.
12.4.8 Key Features

- VDI Pool Management
- Virtual Desktop Persona
- RDP/SSH/VNC Console Support
- RDP Remote App Support
- Clipboard Copy/Paste
- HiDPI Support
- Auto Compression Scanning based on User Bandwidth
- Audio Playback (RDP)
- Local Printer (RDP)
- Auto-Resize
- Auto-Login based on Morpheus User Settings
Customizable User Background

12.4.9 Configuring Access to the Virtual Desktop Persona

Access to the Virtual Desktop Persona and individual VDI pools is handled through the user Role and, where applicable, Tenant Role. When creating a new Role, access is restricted to the Virtual Desktop Persona and all VDI pools by default. To grant access:

1. Navigate to the Role (Administration > Roles > Selected Role)
2. Access the Personas tab
3. Toggle the Virtual Desktop permission to “Full” or “None”
4. Access the VDI Pool Access tab
5. Toggle access to selected VDI pools to “Full” or “None”, you can also toggle permission on all pools to “Full” or “None” with the Global Access selection
6. Role changes are saved automatically, there is no need to manually save

12.4.10 Launching a VDI Instance

VDI Instances are launched from the Virtual Desktops Persona. Depending on Role permissions, your account may default to this view or may even restrict you solely to this view. To access the Virtual Desktops Persona from the standard view or from another Persona, click on the user’s name in the upper-right corner of the application window. When available, this dropdown menu will list the standard Morpheus Persona view as well as any other Personas the user has permission to access. Click on Virtual Desktop to access the Virtual Desktop Persona.

The Virtual Desktop Persona view lists out each of the virtual desktop types they can access. Click on the desired virtual desktop type to launch it. If there are virtual apps available for any listed desktop types, they are presented in a flyout menu alongside a “desktop” option to access the base OS over an individual app. Items categorized as “Desktops” are VDI pools configured in the Tools menu of the Standard Persona. Items categorized as “Instances” are Instances favorited by the current user in the Standard Persona (if they have access and they have favorited any Instances). Clicking on an Instance tile offers quick access to the Instance console.

Important: Virtual Desktops are launched in a pop-up window. Be sure your web browser is not blocking pop-ups or create an appropriate exception for Morpheus virtual desktop pop-ups.

12.4.11 Changing the Virtual Desktop Persona Background

The Morpheus Virtual Desktop Persona includes default backgrounds for an elegant look out of the box. If desired, users may change this background to suit personal taste or organizational branding. This change is unique to each individual account. At this time, there is no option for appliance-wide whitelabeling for Virtual Desktop Persona backgrounds.

1. Click on the user’s name in the far upper-right corner of the application window
2. Click USER SETTINGS
3. The section for “VDI Settings” is in the lower-right corner of the page
4. Mark the RESET box and click SAVE to reset the Virtual Desktop Persona to the default background
5. Click “Browse” and upload a local image to add a custom background
6. Click SAVE

12.5 Getting Started with Terraform Instance Types

Terraform is a common tool that allows IT administrators to map out infrastructure as code in configuration files and supports all of the popular providers used in the modern datacenter. Once configured, Terraform will plan, deploy, and manage the infrastructure as needed. Configuration files can be brought under version control so teams can easily make changes to environments. Infrastructure can also be monitored for drift and corrective action can easily be taken.

Morpheus allows users to on-board or even draft Terraform spec directly. With the configuration on-board, we can begin to piece together infrastructure constructs into the Morpheus Library as Layouts and Instance Types. With the Library items staged, users can deploy new infrastructure directly into the selected providers. Once deployed, infrastructure can be monitored for drift from within Morpheus UI. When needed, we can plan and take corrective action easily from the detail page of a Morpheus Terraform Instance.

In this section, we’ve discussed a high-level overview of Terraform and working with Terraform in the Morpheus context. In the next section, we’ll actually onboard Terraform spec, create Library items, and deploy real infrastructure to AWS with Morpheus.

12.5.1 Terraform Instance Types in Action

In this example, we’re going to deploy a VPC and three subnets to AWS using Terraform and Morpheus. I’ve created Spec Templates to onboard .tf configuration files which handle the AWS provider (with assume role for account flexibility), VPC creation, subnet creation, and variable injection.

We’ll onboard the Terraform configuration files as modular Spec Templates, create new Instance Types with custom Layouts for the Morpheus Library, and set up Inputs to inject variable values at provision time. Once deployed, we’ll take a look at the new infrastructure in Morpheus and go over the management capabilities for the new environment.

12.5.2 Spec Templates

Terraform configuration is stored as a Spec Template in Morpheus. You can store your configuration as one monolithic file for each Instance Type you intend to create or you can create individual Spec Templates for modular pieces which can be reused across multiple Instance Types. When added to the Layout later, we’ll be able to include as many Spec Templates as we wish which enables us to reuse smaller modular pieces if desired.

Spec Templates are added in the Morpheus Library (Library > Templates > Spec Templates tab). We can pull in the template from some type of repository, such as through a Github integration, or write new spec directly into the New Spec Template modal. In most cases, the spec will be pre-existing and pulled in from a version-controlled repository but here I have my Terraform spec entered locally. Click + ADD, complete the fields as I’ve done in the example below and click SAVE CHANGES.

In the VERSION field at the bottom of the TF Spec Template modal, enter a Terraform version number to force that version to be used. This version is only honored if the Terraform Runtime setting (Administration > Settings > Provisioning) is set to “auto”. When “manual” is selected as the Terraform Runtime setting, Morpheus will simply use the version installed on the appliance box.

**Tip:** When declaring variables, keep in mind that Morpheus expects users to follow Terraform best practices. For example, when a variable type is not defined, it defaults to string. See Terraform Documentation for additional resources on variable declaration.
• **AWS Subnet by Count**

```terraform
locals {
  bitCount = sum([tonumber(local.subnet_options.cidrMask),-tonumber(split("/",var.vpc_cidr))[1]])
}

resource "aws_subnet" "main" {
  count = tonumber(var.subnetCount)
  vpc_id = aws_vpc.main.id
  cidr_block = cidrsubnet(var.vpc_cidr, local.bitCount, count.index)
  tags = merge(
    local.default_tags,
    {
      Name = "${var.vpc_name}-subnet-0${count.index}"
    }
  )
}
```

(output continues on next page)
• AWS Terraform Default Vars

```hcl
variable "access_key" {
    type = string
}

variable "secret_key" {
    type = string
}

variable "subnetCount" {
    type = number
    default = "<%=customOptions.subnetCount%>"
}

variable "sensitive_thing" {
    type = string
    default = "this_var_is_sensitive"
    sensitive = true
}
```

• AWS Provider Role Assume

```hcl
terraform {
    required_providers {
        aws = {
            source = "hashicorp/aws"
            version = ">= 3.35.0"
        }
    }
}

provider "aws" {
    region = local.vpc_options.region
    access_key = var.access_key
    secret_key = var.secret_key

    assume_role {
        role_arn = "arn:aws:iam::${local.vpc_options.aws_account}:role/OrganizationAccountAccessRole"
    }
}
```

• AWS Terraform Locals

```hcl
locals {
    # Common tags to be assigned to all resources
    default_tags = {
        Owner = "<%=username%>"
        Group = "<%=groupName%>"
        Management_Tool = "Terraform"
        Management_Platform = "Morpheus"
    }
}
```
12.5.3 Inputs and Option Lists

In order to create the Layout later in the guide, I need to create four Inputs so the user can make certain selections at provision time. I wrote my Terraform Configuration with this flexibility in mind so that the same Instance Type can be reused in different scenarios. In this particular case, I’m populating the Inputs with manual Option Lists but they can also be populated through REST calls or calls to the Morpheus API when needed.

Option Lists are created in the Library (Library) under the Option Lists tab. These are lists of items which will be used to create dropdown selections at provision time. Click + ADD, complete the fields as I’ve done in the example below and click SAVE CHANGES. I’ve created one each for the AWS account selection, region selection, and CIDR mask input.
Inputs are also created in the Library under the Inputs tab. In this case, I’m creating four Inputs. Three of them will display as dropdown selections and will be tied to one of the Option Lists we just made. The other will be a simple text input where the user can indicate the total number of subnets that should be created. Click + ADD, complete the fields as I’ve done in the example below and click SAVE CHANGES.
12.5.4 Instance Type

At this point we’re ready to create a new Instance Type. We’ll give the Instance Type a name, which users will use to identify the Instance Type from the list in the provisioning wizard. We don’t need to set much else in this case, most of the pieces we’ve created in previous steps will be associated with the Layout that we create next. The Layout will also be tied to the Instance Type we’re creating now. Instance Types are also created in the Library (Library) under the Instance Types tab. Click + ADD, complete the fields as I’ve done in the example below and click SAVE CHANGES.

![NEW INSTANCE TYPE](image)

12.5.5 Layout

The Layout will bring together everything we’ve made to this point, the Spec Templates, Inputs and the Instance Type. We can add a new one from the Instance Type detail page (Library > Blueprints > Instance Types > Selected Instance Type) by clicking + ADD LAYOUT. We can also create one from the Layouts section (Library > Blueprints > Layouts) by clicking + ADD.

First, change the TECHNOLOGY value to Terraform and the fields will change to allow proper configuration. Next, provide a name for your Layout. If you’re creating the Layout through the Layout tab rather than from the Instance Type detail page, you’ll need to identify the Instance Type the Layout goes with. Using the typeahead fields at bottom of the modal window, add our four Inputs and our five Spec Templates to the Layout. Finally, point the layout to a TFVAR SECRET from Morpheus Cypher if needed. You can see a screenshot of my Layout configuration below.
12.5.6 Provisioning

Now, we’re ready to provision new infrastructure into AWS using Morpheus and Terraform. Just like any other Instance Type, we begin from the Instances list page (Provisioning > Instances) and click + ADD. Select the Instance Type we’ve just created and move on to the GROUP tab of the wizard. Here you’ll give the new instance a name and select your Group and Cloud. Once finished, you’ll move on to the CONFIGURE tab where we’ll see the Inputs we created and associated with the Layout. Once finished with this tab, step through the rest of the wizard to complete the process. You can see the options I’ve selected for this configuration in the image below.
12.5.7 Review the New Instance

After completing the wizard, from the History tab of the Instance detail page users can review the Terraform plan being executed and see the output while the resources are still being provisioned.

Once the provisioning process is complete, head to the State tab. Here we can see and link through to the associated Spec Templates. If needed, you can also edit the configuration spec by clicking on the pencil icon at the end of the row for any listed Spec Template.

By clicking APPLY STATE, the user can once again see the Input selections which were presented during the initial provisioning and make changes when needed. After making changes and clicking NEXT, Morpheus will show the plan output no different than if you’d run terraform plan. On clicking COMPLETE, the plan will be executed as if you’d run terraform apply. Back on the State tab you will see the output from the Apply process as well as an indicator of the success or failure of the operation.
Morpheus will also regularly check for drift from the Terraform configuration. On the State tab near the top is a “Drift Status” indicator. This will either show Drift or No Drift depending on the situation. Morpheus will automatically check for drift every few minutes but you can perform a manual check at any time by clicking \textit{REFRESH STATE}. Drift can be corrected when needed by reapplying state (\textit{APPLY STATE} button).

### 12.6 Backing Up and Restoring Morpheus Appliance

Morpheus includes built-in tools for backing up managed Instances as well as the appliance itself. Use this guide to configure a location and schedule for backing up your Morpheus appliance. This guide also includes steps for restoring or migrating your appliance from the created backup. The steps are the same whether your appliance is deployed in a single node or distributed architecture.

The built-in Morpheus appliance backup functionality backs up the MySql data. In addition to the database, it’s advisable to back up your shared storage (at \texttt{/var/opt/morpheus/morpheus-ui}) and the \texttt{morpheus.rb} configuration file.

\textbf{Note:} The destination Morpheus appliance must be running the same version as that which the backup was taken from.
12.6.1 Create A Backup Job

A Backup Job in Morpheus holds the schedule timing and retention count for automated backups. If you already have a Job configured, you can move on to the next section. By default, Morpheus includes two execution schedules: Daily at Midnight and Weekly on Sunday at Midnight. If currently-existing options do not make sense for your backup needs, create a new execution schedule:

1. Navigate to Library > Automation
2. Click on the “Execute Scheduling” tab
3. Click + ADD
4. Enter schedule timing using cron notation
5. Click SAVE

With the execution schedule created, we can move on to creating the Backup Job itself. A Backup Job includes both the backup retention count and an execution schedule (which we just created).

1. Navigate to Backups > Jobs
2. Click + ADD
3. Name the Job, then configure the retention count and the schedule
4. Click SAVE

12.6.2 Integrate a Bucket or File Share

When configuring a Morpheus appliance backup, a storage location is selected. If you already have the destination bucket or file share integrated with Morpheus, skip to the next section.

1. Navigate to Infrastructure > Storage
2. Click on the Buckets or File Shares tab depending on your chosen storage type
3. Click + ADD
4. Select the appropriate bucket or file share type
5. Complete the required fields and click SAVE CHANGES

Note: Additional guidance on integrating each of the supported bucket and file share types can be found elsewhere in Morpheus documentation.

12.6.3 Configuring Morpheus Appliance Backup

With the groundwork laid in the previous sections, we’re ready to enable and configure Morpheus appliance backup.

1. Navigate to Administration > Settings > Backups
2. Slide the switch labeled “Backup Appliance”
3. Click SAVE

On saving this change, a text link labeled “Backup” will be activated which will take you directly to the automatically-generated appliance backup job. Click this link to continue.

1. Click EDIT
2. Enter a name for the appliance backup job

3. Select an integrated storage bucket or file share

4. Choose a pre-created backup job. If you do not have an existing backup job that fits, a retention count and schedule can be manually created in this modal. If you manually configure retention counts and schedules in addition to associating a Job, the Job values will override any manual settings.

5. Click SAVE CHANGES

At this point, your appliance will be automatically backed up on the schedule you chose and stored in the selected location. An appliance backup will store backup copies of the appliance MySQL database. Should you need to restore or migrate your database from backup, follow the steps in the next section of this guide.

### 12.6.4 Restoring an Appliance from Backup

Begin by ensuring the Morpheus UI service is stopped on all of the application servers:

```
[root@app-server-new ~] morpheus-ctl stop morpheus-ui
```

To access the MySQL shell we will need the password for the Morpheus DB user. We can find this in the morpheus-secrets file:

```
[root@app-server-old ~] cat /etc/morpheus/morpheus-secrets.json | grep morpheus_
password
"morpheus_password": "451e122cr5d122asw3de5e1b", <---- this one
"morpheus_password": "9b5vdj4de5awf87d",
```

Make note of the first `morpheus_password` value as indicated above.

Copy the SQL database backup from the backup bucket or file share to an appliance node at `/tmp/morpheus_backup.sql`. Then, you can import the MySQL dump into the target database using the embedded MySQL binaries, specifying the database host, and entering the password for the morpheus user when prompted:

```
[root@app-server-new ~] /opt/morpheus/embedded/mysql/bin/mysql -u morpheus -h 10.1.2.
<2 morpheus -p < /tmp/morpheus_backup.sql
Enter password:
```

The data from the old appliance is now replicated on the new appliance. Simply start the UI to complete the process:

```
[root@app-server-new ~] morpheus-ctl start morpheus-ui
```

### 12.7 Cloud Resource Tagging with Morpheus

#### 12.7.1 Introduction

As organizations scale their cloud environments, they often need to devise methodologies for organizing those resources. Tags consist of key and optional value pairs which make it easier to search for or filter your cloud resources based on categories relevant to the organization. While each public or private cloud handles tagging slightly differently, Morpheus removes that complexity and differentiation by handling tags in a consistent way across clouds. In addition, the Morpheus policy engine gives administrators tools to set up guard rails and ensure cloud resource tagging is handled consistently with each provisioning.

This guide will go through Morpheus tagging features and best practices, as well as include provisioning examples from some of the most commonly integrated clouds.
Note: Tag syncing is bi-directional in Morpheus for supported clouds. Tag syncing is currently supported in Amazon, Azure, Google, VMware, and Alibaba Clouds.

12.7.2 Tagging on Provisioning

In the simplest use case, tags can be entered manually in most provisioning scenarios. For example, on the Configure tab of the Create Instance wizard, the user can expand the Tags section and enter as many Tags as he or she needs to comply with organization practices.

Once the resource is deployed, Tags are synced and applied to the provisioned machine in the relevant cloud. Tags are shown on the Instance detail page in Morpheus and can also be confirmed in the cloud console if desired. Tag syncing is also a two-way street in that any tag updates applied within Morpheus or within the cloud console will be reflected everywhere.
Note: Tag updates made in the cloud console may take up to five minutes to be reflected in Morpheus UI following the next sync of cloud data.

12.7.3 Custom Instance Types and Tagging

Manually tagging resources as described in the previous section will work in some cases but many administrators will likely need to pre-seed the provisioning wizards with tagging prompts or build dropdown lists for tag values. This is accomplished in Morpheus through the use of custom Instance Types, Inputs, and Option Lists.

To get started, first create an Option List to hold dropdown or typeahead sets of available key values if needed based on organizational tagging policy. If the tag value field should be manually entered at provision time or if the value field is to be left blank, this step can be skipped. Option Lists are created and stored in the Morpheus Library (Library). They can be populated manually by entering CSV or JSON datasets as shown in the example below. They can also be dynamically populated through Morpheus API or REST calls.

With the set of possible values defined (if needed), we next create an Input to prompt the user for tag input when provisioning relevant Instance types. Inputs are also housed in the Morpheus Library (Library).

It’s important to note the value entered for the FIELD NAME on the new Input will be set as the tag key. The EXPORT AS TAG box should also be marked. By default, the TYPE value is Text. This is appropriate when the user should be prompted with a free text field at provision time to enter a tag value. To tie this Input to the Option List that was
just created (if needed), change the TYPE value to Select List or Typeahead. Typeahead works best for very long lists while Select List is often a better user experience for lists of a more manageable size. Set the Option List we created in the previous step in the OPTION LIST value (if needed).

At this point, we are ready to add this Input to any custom Instance Types or Layouts. When those Instance Types
or Layouts are provisioned, the values input by the user become tags associated with the created cloud resources. By setting the Input on an Instance Type, the tag selection appears when provisioning all associated Layouts. Alternatively, if the Input is set on individual Layouts, it will only appear when those Layouts are provisioned.

Instance Types and Layouts are also stored in the Morpheus Library (Library). By opening up any custom Instance Type, we can add the Input we just created when editing the Instance Type. Additionally, we can drill into associated Layouts and apply the Input to selected Layouts if that’s more appropriate.
Going forward, each time the chosen Instance Type or Layout is provisioned, the user will be prompted to enter relevant tag selections. We can even require the user input these values or govern their inputs through tagging policies which will be discussed in the next section.
12.7.4 Instituting Tagging Policies

If needed, Morpheus allows cloud resource tagging to be governed through its native policy engine. Like other policies, tag policies are added from Administration > Policies. By creating a new policy and setting the TYPE to Tags, the relevant fields are revealed.

**Note:** At the time of this writing (Morpheus 4.2.1), tag policy scanning and enforcement is only functional in Azure, Amazon AWS, VMware, and Google Cloud Platform clouds.

With a tag policy, we can choose to enforce the policy on a strict or passive basis by marking or unmarking the STRICT ENFORCEMENT box. Strictly enforced tagging policies will not allow provisioning to proceed in supported clouds if the policy requirements are not met. If we opt to enforce the policy passively, a warning banner will appear on the detail page of any server that does not meet policy requirements. Additionally, existing servers in supported clouds will be scanned and those which do not meet policy requirements will also receive the warning banner.

A tag policy must be given a KEY value. If we define only a KEY value, the policy will look for a tag with that key and any (or no) value. Alternatively, we can select any pre-existing Option List as the VALUE LIST to require the tag contain a value that exists in that list.

Finally, like other Morpheus policies, we can choose to scope it globally, by group, by cloud, or by user. Master Tenant administrators can also choose to scope the policy to one or more Subtenants.
Tag Policy scanning and enforcement is only currently functional for three cloud types: Azure, Amazon, and VMware.

**Config**

**Strict Enforcement**

- **Key**: Tag Key
- **Value List**: Select

Choose from any configured Option List

**Filter**

- **Scope**: Global
12.7.5 Tagging in Action

With the prep work complete, we can take a look at our Inputs in action at provision time. In this example case, several Inputs have been created and applied to one custom Instance Type. The example Instance Type has three associated CentOS Layouts, one for AWS, one for VMware, and one for Azure. Regardless of the selected Layout, users are prompted to fill the same tag fields and our tagging remains consistent regardless of the user who is provisioning a new resource at the time.

12.7.6 Tagging and AWS

When provisioning my CentOS Instance Type with an Amazon Layout, the tag prompts are shown in the provisioning wizard.

In the AWS web console, we can see the same tags are applied. We also have two-way tag sync going forward. When tags are updated in Morpheus, the changed is synced to the AWS web console. The opposite is also true.
12.7.7 Tagging and VMware

When provisioning my CentOS Instance Type with a VMware Layout, the tag prompts are shown in the provisioning wizard.
In the VMware console, we can see the same tags are applied. We also have two-way tag sync going forward. When tags are updated in Morpheus, the changed is synced to VMware. The opposite is also true.

### 12.7.8 Tagging and Azure

When provisioning my CentOS Instance Type with an Azure Layout, the tag prompts are shown in the provisioning wizard.
In the Azure console, we can see the same tags are applied. We also have two-way tag sync going forward. When tags are updated in Morpheus, the changed is synced to Azure. The opposite is also true.

12.8 Configuring Access with Clouds, Groups, and Roles

As you get started, it’s vital to understand constructs such as Clouds and Groups as they are implemented in Morpheus. Deploying an effective strategy for dividing organizational resources and people groups under these constructs will ensure all parties have convenient access to the resources they need. Map currently-existing strategies for splitting resources and controlling costs into Morpheus and your teams will have access only to resources allocated to their department.

This guide discusses the constructs of Clouds, Groups, Roles, Users, and Policies while also presenting an example use case for allocating resources and distributing access under these umbrellas. We’ll end up with a permissions structure represented by the diagram below and step through each part of the implementation process.
12.8.1 Clouds

Clouds have broad meaning in Morpheus and can be integrations into public clouds, private clouds, or bare metal servers. You can read more about Clouds in Morpheus Docs here.

In our example case, the organization has an Azure account and three separate departmental projects consolidated under separate resource groups. The Morpheus integration with Azure public cloud allows users to scope the Cloud to one specific resource group, if desired. We will do so in this case because it will allow us to restrict our users to the appropriate Azure resource groups in a later step. In the screenshot below, note how I am scoping the Morpheus Azure Cloud to a specific resource group when adding or editing the Cloud. This process will be repeated two additional times to create the three Morpheus Clouds we need. Complete details on integrating Morpheus with Azure public cloud are here in Morpheus Docs.
Groups in Morpheus allow administrators to determine which Clouds their users have access to. Part of defining a Role, which we’ll see in the next section, is selecting which Groups are associated with the Role. One or multiple Clouds are added to each Group and passed to users through their assigned Roles.

When creating a Cloud, it must be added to a Group. Additionally, Clouds can be added to a Group at any time from the Clouds tab on the Group detail page (Infrastructure > Groups > Specific Group). In the example case diagrammed above, one Cloud (Azure cloud account scoped to a specific resource group) is associated with each Group but often Groups will contain many Clouds. In the screenshot below, I am adding an Azure Cloud to a Group that is currently empty.
12.8.3 Roles

Morpheus Roles determine user access to many things, including application features, Groups, configured Instance Types, configured Blueprints, Personas, and Catalog Item configurations for the Service Catalog Persona. It’s important to note that a user can have multiple Roles and will take the most permissive rights across all of these Roles. In many cases, this greatly simplifies Role configuration for administrators as it prevents the need to create highly-specific individual Roles that can suit every case. To illustrate this for our example case, I will create a set of Roles to handle Group access for my users and another set of Roles to give access to the correct feature permissions.

For this example case, I’ll start by creating one Role for each of the three Groups we created in the previous step. By default, a new Role will have all feature permissions set to “None” as shown below meaning we can skip directly to the Group Access tab.
On the Group Access tab, I will toggle the Global Access setting to Custom and give access only to one Group as shown in the next image. By doing this for each of our Groups created in the last section, we can easily control Group access for each user by applying one or more of our Group Roles to their user which we will do in the next section.

In addition to Roles for handling Group access, we need additional Role sets which will control our feature access. For example, we might have highly permissive feature access for administrators and more restrictive ones for developers or other users who have specific responsibilities requiring access to just a few specific areas of the UI. These additional
Roles are created in the same way as the Group Roles we just created but all Group access will be set to “None” and the appropriate feature access will be configured on the “Feature Access” tab.

### 12.8.4 Users

With the groundwork laid in the previous steps, we can easily configure permissions for any user accounts we might add to Morpheus. In the screenshot below, I’m adding a user account for a developer at my organization. I’ve applied one Role to handle correct Group access for this user and I’ve applied the “Developer” role to give only the feature access needed for this user to carry out his or her responsibilities.

![New User Form](image)

### 12.8.5 Policies

One final consideration for this example case is policy application. Morpheus enables administrators to place fine-grained governance scoped to specific users, Roles, Groups, Clouds, Tenants, or globally. You can read more about policies in Morpheus docs [here](#) but we will also create some that apply to the example case discussed in this guide.

Policies are created from the Administration menu in the Policies section. In the screenshot below, I’ve created a new policy and chosen to scope it to a Group. In this case, I’m creating a maximum VMs policy but there are many other types which are listed in our documentation linked above.
At this point, we've completed implementation of the access structure. As new users are added, we can easily give them the Group and feature access they need. We can also easily add or edit the policies that are in place or add new Clouds and distribute access to existing users. The key is understanding the relationship between the Morpheus constructs discussed in this guide. Armed with that understanding, the example case presented here can be expanded to suit the needs of large-scale enterprise.

12.9 Automation Integrations

12.9.1 Ansible

Overview

Ansible is a configuration management engine that is rapidly growing in popularity in the IT and DevOPS community. While it lacks some of the benefits at scale that solutions such as Salt, Chef, or Puppet offer. It is very easy to get started and allows engineers to develop tasks in a simplistic markup language known as YAML. Morpheus integrates with an existing repository of playbooks as the master in a master-slave Ansible architecture.

Morpheus not only supports Ansible but greatly enhances Ansible to do things that it could not do in its native form. For example, Ansible can now be configured to run over the Morpheus agent communication bus. This allows playbooks to be run against instances where SSH/WinRM access may not be feasible due to networking restrictions or other firewall constraints. Instead it can run over the Morpheus Agent which only requires port 443 access back to the Morpheus appliance URL.

This integration supports both Linux-based and Windows platforms for playbook execution and can also be configured to query secrets from Morpheus Cypher services (similar to Vault).
Requirements

- Minimum Ansible Version Requirement is 2.7.x
- For agentless non-commandbus, sshpass is required
- For Windows non-agent command bus, pywinrm is required
- **Integrations:** Ansible User Role Permission required for access to Ansible Details Pages and Ansible tabs in Groups and Clouds
- Calling Morpheus Cypher secrets into Ansible scripts requires the Python `requests` module which is not part of the Python standard library. For Ubuntu 18.04 or 20.04 run `sudo apt install python-requests` or `sudo apt install python3-requests`, respectively. For RHEL/CentOS, run `sudo yum install python2-requests`.

**Note:** Installing Ansible on the Morpheus appliance is a requirement. In some cases, this is handled automatically but in certain situations you may have to install manually. See the section below on troubleshooting Ansible for installation steps.

Add Ansible Integration

1. Navigate to Library > Integrations and select + New Integration
2. Select Integration Type “Ansible”
3. Populate the following fields:
   - **Name** Name of the Ansible Integration in Morpheus
   - **Enabled** Enabled by default
   - **Ansible Git URL** https or git url format of the Ansible Git repo to use
   - **Keypair** For private Git repos, a keypair must be added to Morpheus and the public key added to the git account.
   - **Playbooks Path** Path of the Playbooks relative to the Git url.
   - **Roles Path** Path of the Roles relative to the Git url.
   - **Group Variable Path** Path of the Group Variables relative to the Git url.
   - **Host Variables Path** Path of the Host Variables relative to the Git url.
   - **Use Ansible Galaxy** Install roles defined in requirements.yml
   - **Enable Verbose Logging** Enable to output verbose logging for Ansible task history
   - **Use Morpheus Agent Command Bus** Enable for Ansible Playbooks to be executed via Morpheus Agent Command Bus instead of SSH
4. Save Changes

Once you have completed this section and saved your changes you can set up a Cloud or Group to utilize this integration.
Ansible on Windows

When executing Ansible playbooks on Windows platforms, a few requirements must be met:

- `pywinrm` may need to be installed on the Morpheus Appliance via `pip install pywinrm`
- An Ansible Integration must be scoped to a Group or Cloud for Ansible to execute on Windows, as Morpheus assumes Ansible local when no group or cloud is scoped to Ansible. The playbooks do not need to be executed solely in the Group or Cloud, one just needs to be scoped to an Ansible Integration for Ansible Windows to run properly.

Scope Ansible Integration to a Cloud

1. Navigate to `Infrastructure > Clouds`
2. Edit the target Cloud
3. Expand the `Advanced Options` section
4. In the `Config Management` dropdown, select the Ansible Integration.
5. Save Changes

Once an Ansible integration is added to a Cloud, a new “ANSIBLE” tab will appear on the Cloud details page, populated with the Ansible integrations Playbook and Roles, as well as an editable Inventory list.

Scope Ansible Integration to a Group

1. Navigate to `Infrastructure > Groups`
2. Edit the target Group
3. Expand the `Advanced Options` section
4. In the `Config Management` dropdown, select the Ansible Integration.
5. Save Changes

Once an Ansible integration is added to a Group, a new “ANSIBLE” tab will appear on the Group details page, populated with the Ansible integrations Playbook and Roles, as well as an editable Inventory list.

Provisioning Options

When provisioning Instances into a Cloud or Group with a Ansible Integration added, an `Ansible` section will appear in the Config section of the provisioning wizard. By default, Ansible is enabled, but can be disabled by expanding the `Ansible` section and unchecking `Enable Ansible`.

Ansible Integration Provisioning options:

**Enable Ansible** Select to bootstrap

**Ansible Group** Ansible Inventory Group. Use existing group or enter a new group name to create a new group. Leaving this field blank will place instance in the “unassigned” inventory group.

**Note:** An instance can belong to multiple groups by separating group names with a comma

**Playbook** Playbook(s) to run. The .yml extension is optional.
Running Playbooks

Playbooks can also be run on all inventory groups, individual groups, or added as a task and ran with workflows.

To run Ansible on all or a single inventory group, in the Ansible tab of the Morpheus Group page, select the Actions dropdown and click Run.

In the Run Ansible modal, you can then select all or an individual group, and then all or a single Playbook, as well as add custom tags.

Playbook’s can also be added as tasks to workflows in the Library > Automation section, and then selected in the Automation pane during provisioning of new instances, when creating app blueprints, or ran on existing instances using the Actions > Run Workflow on the Instance or Host pages.

Using variables

Morpheus variables can be used in playbooks.

Use Case:

Create a user as instance hostname during provisioning.

Below is the playbook. Add this playbook to a task and run it as a workflow on the instance.

```yaml
---
- name: Add a user
  hosts: all
  gather_facts: false
  tasks:
    - name: Add User
      win_user:
        name: "{{ morpheus['instance']['hostname'] }}"
        password: "xxxxxxx"
        state: present
```

Note: `{{ morpheus['instance']['hostname'] }}` is the format of using Morpheus Variables

Create a user with a name which you enter during provisioning using a custom Instance type.

This instance type has a Text Input that provides a text box to enter a username. The fieldName of the Input in this case would be username.

```yaml
---
- name: Add a user
  hosts: all
  gather_facts: false
  tasks:
    - name: Add User
      win_user:
        name: "{{ morpheus['customOptions']['username'] }}"
        password: "xxxxxxx"
        state: present
```

Note: `{{ morpheus['customOptions']['username'] }}` will be the format.
Using Secrets

Another great feature with using Ansible and Morpheus together is the built-in support for utilizing some of the services that Morpheus exposes for automation. One of these great services is known as Cypher (please see documentation on Cypher for more details). Cypher allows one to store secret data in a highly encrypted way for future retrieval. Referencing keys stored in cypher in your playbooks is a matter of using a built-in lookup plugin for ansible.

```yaml
- name: Add a user
  win_user:
    name: "myusername"
    password: "{{ lookup('cypher','secret=password/myusername') }}"
    state: present
```

By using the `{{ lookup('cypher','secret=password/myusername') }}` syntax. One can grab the value directly out of the key for use. This lookup plugin also supports a few other fancy shortcuts. In this above example the `password/` mountpoint is capable of autogenerating passwords if they have not previously been defined and storing them within cypher for reference later.

Another capability is accessing properties from within a key in cypher. The value of a key can also be a JSON object which can be referenced for properties within. For example:

```yaml
{{ lookup('cypher','secret=secret/myjsonobject:value') }}
```

This would grab the `value` property off the nested json data stored within the key.

Cypher is very powerful for storing these temporary or permanent secrets that one may need to orchestrate various tasks and workflows within Ansible.

Custom Inventory Entries

With Morpheus it is possible to add custom inventory entries that exist outside of morpheus host/server entry. This is global across cloud or group and is done on the integration details page of the Ansible integration. To add a custom inventory entry navigate to Library > Integrations > (Your specific Ansible integration). Click on the ACTIONS button, then click EDIT INVENTORY. Inventory should be in the default Ansible ini format.
Using Ansible over the Morpheus Agent Command Bus

In many environments, there may be security restrictions on utilizing SSH or WinRM to run playbooks from an Ansible server on the appliance to a target machine. This could be due to being a customer network (in the environment of an MSP), or various security restrictions put in place by tighter industries (i.e. Government, Medical, Finance).

Ansible can get one in trouble in a hurry. It is limited in scalability due to its fundamental design decisions that seem to bypass concepts core to all other configuration management frameworks (i.e. SaltStack, Chef, and Puppet). Because of its lack of an agent, the Ansible execution binary itself has to handle all the load and logic of executing playbooks on all the machines in the inventory of an Ansible project. This differs from other tools where the workload is distributed across the agents of each vm. Because of this (reaching out) approach, Ansible is very easy to get started with, but can be quite a bit slower as well as harder to scale up. However, Morpheus offers some solutions to help mitigate these issues and increase scalability while, at the same time improving security.

How does the Morpheus Agent Command Bus Work?

One of the great things about Morpheus is its Agent Optional approach. This means that this functionality can work without the Agent, however the agent is what adds the security benefits being represented here. When an instance is provisioned (or converted to managed) within Morpheus, an agent can be installed. This agent opens a secure websocket back to the Morpheus appliance (over port 443). This agent is responsible for sending back logs, guest statistics, and a command bus for automation. Since it is a WebSocket, bidirectional communication is possible over a STOMP communication bus.

When this functionality is enabled on an Ansible integration, a connection_plugin is registered with Ansible of type morpheus and morpheus_win. These direct bash or powershell commands, in their raw form, from Ansible to run over a Morpheus api. The Ansible binary sends commands to be executed as an https request over the API utilizing a one time execution lease token that is sent to the Ansible binary. File transfers can also be enacted by this API interface. When Morpheus receives these commands, they are sent to the target instances agent to be executed. Once they have completed a response is sent back and updated on the ExecutionRequest within Morpheus. Ansible polls for the state and output on these requests and uses those as the response of the execution. This means Ansible needs zero knowledge of a machines target ip address, nor its credentials. These are all stored and safely encrypted within Morpheus.

It has also been pointed out that this execution bus is dramatically simpler than utilizing pywinrm when it comes to orchestrating Windows as the winrm configurations can be cumbersome to properly setup, especially in tightly secured Enterprise environments.

Using Ansible Galaxy

Morpheus can use a requirements.yml file to define Ansible roles to download prior to running your playbook. Place requirements.yml into the root of your Git repository and make sure Use Ansible Galaxy is checked in the integration. Roles will be installed in the root of the repository if a directory is not defined in Roles Path.

- Example requirements.yml:

```
- src: https://github.com/geerlingguy/ansible-role-java
  name: java
```

- Example playbook.yml:

```
- hosts: all
  gather_facts: true
  roles:
    - java
```
Troubleshooting Ansible

- When a workflow is executed manually, the Ansible run output is available in the Instance History tab. Select the i bubble next to the Ansible task to see the output. You can also see the run output in the ui logs in /var/log/morpheus/morpheus-ui/current which can be tailed by running morpheus-ctl tail morpheus-ui.

- Verify Ansible is installed on the Morpheus Appliance.

  Ansible should be automatically installed but certain OS or network conditions can prevent the automated install. You can confirm installation by running ansible --version in the Morpheus appliance, or by viewing the Ansible integration details page (Administration > Integrations > Select Ansible Integration). We also see it in the Ansible tab of a Group or Cloud scoped to Ansible, just run --version as ansible is already included in the command.

  If Ansible is not installed, follow these instructions to install, or use your preferred installation method:

  **Ubuntu:**

  ```
sudo apt-get install software-properties-common
sudo apt-add-repository ppa:ansible/ansible
sudo apt-get update
sudo apt-get install ansible
```

  **CentOS:**

  ```
sudo yum install epel-release
sudo yum install ansible
```

  Then create the working Ansible directory for Morpheus:

  ```
sudo mkdir /opt/morpheus/.local/.ansible
sudo chown morpheus-local.morpheus-local /opt/morpheus/.local/.ansible
```

- Validate the git repo is authorizing and the paths are configured correctly.

  The public and private ssh keys need to be added to the Morpheus appliance via “Infrastructure > Keys & Certs” and the public key needs to be added to the git repo via user settings. If both are set up right, you will see the playbooks and roles populate in the Ansible Integration details page.

- The Git Ref field on playbook tasks is to specify a different git branch than default. It can be left to use the default branch. If your playbooks are in a different branch you can add the brach name in the Git Ref field.

- When running a playbook that is in a workflow, the additional playbooks fields do not need to be populated, they are for running a different playbook than the one set in the Ansible task in the Workflow, or using a different Git Ref.

- If you are manually running Workflows with Ansible tasks on existing Instances through Actions > Run Workflow and not seeing results, set the Provision Phase on the Ansible task to Provision as there may be issues with executing tasks on other phases when executing manually.
12.9.2 Ansible Tower

Overview

Morpheus supports Ansible Tower for configuration management. Morpheus accomplishes this by integrating with an existing instance running Ansible Tower (AT) 3.3.0-1 and earlier. The username and password required for integration can be a user with admin access or a user with project admin access.

Morpheus will import the current Inventory, Templates, Hosts, Groups and Projects. In the integration view it will add a Job tab which will have information of all the jobs executed from Morpheus.

**Note:** This integration will not import data of the jobs which are not executed from Morpheus.

Add Ansible Tower Integration

1. Navigate to \AdmInt\ and select + New Integration
2. Select Integration Type “Ansible Tower”
3. Populate the following fields:
   - Name: Name of the Ansible Tower Integration in Morpheus
   - Enabled: To disable the integration, uncheck this option
   - Ansible Tower URL: An HTTPS or HTTP Ansible Tower URL
   - Username: The user Morpheus would use to communicate with Ansible Tower
   - Password: Enter the password. Password is encrypted and saved in DB
   - API Version: This drop down has one option (v2) for now but may have others in future
4. Save Changes

Once you have completed this section and saved your changes you can set up a Cloud or Group to utilize this integration.

Scope Ansible Tower Integration to a Cloud

All instances provisioned in this cloud will have the Ansible Tower config option during provisioning. See below the Provisioning Options for more details about the options.

1. Navigate to Infrastructure > Clouds
2. Edit the target Cloud
3. Expand the Advanced Options section
4. In the Config Management dropdown, select the Ansible Tower Integration.
5. Save Changes
Scope Ansible Tower Integration to a Group

All instances provisioned in this Group will have the Ansible Tower config option during provisioning in any cloud part of the Group. See below the Provisioning Options for more details about the options.

1. Navigate to Infrastructure > Groups
2. Edit the target Group
3. Expand the Advanced Options section
4. In the Config Management dropdown, select the Ansible Tower Integration.
5. Save Changes

Provisioning Options

When provisioning Instances into a Cloud or Group with a Ansible Tower Integration added, an Ansible Tower section will appear in the Config section of the provisioning wizard. By default, Ansible Tower is enabled, but can be disabled by expanding the Ansible Tower section and unchecking Enable Ansible Tower.

Ansible Integration Provisioning options:

**Enable Ansible Tower** Select to bootstrap

**Inventory** A list of Inventory available in Ansible Tower will appear in the drop down. Select an existing inventory.

The instance will be added to the inventory selected.

**Ansible Group** Enter the name of an existing Group in the inventory selected above.

**Template**

Select an existing template or select the option ‘Create New Template’. If ‘Create New Template’ is selected below fields will appear and are mandatory

- **Template Name** Enter the template name
- **Project** Select an existing project from the drop down options
- **Playbook** Select a playbook from the dropdown to be associated with the template. Note: Morpheus doesn’t store a local copy of the playbooks visible in Ansible Tower. SCM or local path for playbooks should be maintained in Ansible Tower.

**Execute Mode**

Select one of the options from the dropdown

- **Limit to instance** This will execute the template on the instance provisioned.
- **Limit to Group** This will execute the template on all hosts attached to the group entered in the ‘Ansible Group’ field.
- **Run for all** This will execute the template on all hosts in the inventory
- **Skip execution** This will skip the execution of the template on the instance provisioned.
Scoping Ansible Tower Jobs to Tenant-Default Inventories

Users in the Primary Tenant have an additional Inventory execution option when creating Ansible Tower Job-type Tasks. When making a selection in the Inventory field, “Use Tenant Default” may be selected rather than a specific Inventory. This is because Ansible Tower Jobs created in the Primary Tenant may be shared publicly to other Tenants through public Workflows or when associated with public Library items.

When this option is selected and the Task is run in a Subtenant, it will automatically be run against the default Inventory which is configured for the Subtenant. The next section includes steps for associating Tenants and default Inventories.

Important: An Ansible Tower Job configured to run against a Tenant-default Inventory will fail when run by a user whose Tenant does not have a default Inventory set.

Setting Default Inventories for Tenants

When creating or editing Ansible Tower integrations, navigate to the Inventory tab to view all Inventories synced from the selected integration. Click “Permissions” inside the “MORE” action menu at the end of a row for the selected Inventory. Within the PERMISSIONS modal, there is a single typeahead field where a Tenant can be selected. Once the Tenant is selected, click SAVE CHANGES. Now back on the Inventory list view, you’ll see the default Tenant which is associated with each Inventory.

Note: Tenants may only be associated with one Inventory, though an Inventory can have multiple Tenant associations. If a Tenant is selected to be associated with a new Inventory, its association with a previous Inventory will automatically be removed.
When provisioning or when running Ansible Tower Jobs as Morpheus Tasks, you may pass the extra_vars stack to the Tower Job. First, ensure the Job Template has extra variables “Prompt on Launch” enabled as shown below:

The sample Playbook below is associated with the Tower Job Template.

```yaml
---
- hosts: all
  vars:
    Opensource_Team: "Customer"
  tasks:
    - name: Print Hello World
      debug:
        msg: "Hello World {{ Opensource_Team }}. Here are Morpheus extra_vars: {{ morpheus }}
```
After executing the Tower Job, we can see the variable stack surfaced into the results as defined in the Playbook:

```
4 5 TASK [Gathering Facts] ******************************************** 04:12:59
  **********
6  ok: [ctspcen1001.localdomain]
7
8 TASK [Print Hello World] ******************************************** 04:33:01
  **********
9  ok: [ctspcen1001.localdomain] => {}
10   "msg": {
11      "Hello World Customer. Here are Morpheus extra_vars: (u'platform': u'linux', u'sshKey': None, u'maxCpu': None, u'sequence': 1, u'isDocker': False, u'ansibleTowerExecuteMode': u'executeHost', u'isEC2': False, u'ansibleTowerJobTemplateId': u'66', u'nutanixUser': None, u'variables': {u'HOST_INTERNAL': u'container357', u'INSTANCE_HOSTNAME': u'ctspcen1001', u'IP_INTERNAL': u'10.30.20.105', u'IP_PUBLIC': u'10.30.20.10', u'HOST_EXTERNAL': u'ctspcen1001', u'PORT_22': 22}, u'groupName':
```

**Use Case**

You have Job template(s) in Ansible Tower to do post build config after the OS is deployed. The playbook with roles and tasks to do post build will add specific users and groups, install required packages, remove packages, disable services, change config for ntp, resolv, hosts etc. You want to add the instance to an existing Group/Inventory in Tower.

You can achieve this by adding the Ansible Tower Integration and then scope it to a Cloud or Group. While provisioning an instance, in the config stage you have the Ansible Tower section with option to select the post build job template, select the Inventory and provide an existing Group Name or if the Group doesn’t exist Morpheus will create it and submit for provisioning.

Morpheus will provision the instance, once it is in the finalize state where the instance has an ip and has completed domain join if required, added user(s) or User Groups if specified then Morpheus will add the instance to the inventory and Group and run the Template which will do all the post build of the server.

The output of the post build template execution can be see under Instance history.

**12.9.3 Chef**

**Overview**

Morpheus integrates with one or multiple Chef servers to be used for bootstrapping while provisioning or as tasks in workflows in the Automation section. These workflows can then be run during provisioning in the provisioning wizard Automation pane, or on an existing Instance by selecting Run Workflows from the Actions menu on the Instance detail page. Workflows can also be added to Instances in the blueprint and app sections.
Add Chef Integration

1. Navigate to Administration > Integrations and select + New Integration
2. Select Integration Type “Chef”
3. Populate the following fields:
   - Name: Name of the Chef Integration in Morpheus
   - Chef Endpoint: url of chef server api endpoint in https://api.example.com format. Do not add /organization/xxxx here, which is populated in the Chef Organization field
   - Chef Version: 12.3.0 by default, can be changed to use a different/more recent version of chef
   - Chef Organization: Chef Server Organization
   - Chef User: Chef Server User
   - User Private Key: The private key of the user with access to this chef server
   - Organization Validator: Validator key for the organization
4. Save Changes

The added Chef Integration is now available for use in Morpheus. The Chef Integration can be added to Clouds or Groups to auto-bootstrap nodes and specify Environment, Node ID, Runlist, Attributes and Tags when creating instances. The Chef integration can also be selected in the Chef Server dropdown when creating a Chef Bootstrap-type Task.

Note: Integrating Chef with Morpheus enables a user to bootstrap a node using Chef Bootstrap-type Tasks or Chef associations with Clouds or infrastructure Groups. It does not enable users to update run-lists on the Chef server for nodes which have already been bootstrapped.

Scope Chef Integration to a Cloud

1. Navigate to Infrastructure > Clouds
2. Edit the target Cloud
3. Expand the Advanced Options section
4. In the Config Management dropdown, select the Chef Integration.
5. Save Changes

Scope Chef Integration to a Group

1. Navigate to Infrastructure > Groups
2. Edit the target Group
3. Expand the Advanced Options section
4. In the Config Management dropdown, select the Chef Integration.
5. Save Changes
Provisioning Options

When provisioning Instances into a Cloud or Group with a Chef Integration added, a Chef section will appear in the Config section of the provisioning wizard. By default, Chef is enabled, but can be disabled by expanding the Chef section and unchecking Enable Chef.

Chef Integration Provisioning options:

**Enable Chef** Select to bootstrap

**Chef Environment** Populate Chef environment, or leave as _default_

**Chef Node ID** Defaults to instance name, configurable.

**Chef Runlist** Add Runlist

**CHEF ATTRIBUTES** Add Chef Attributes

**CHEF TAGS** Add Chef tags

12.9.4 Puppet

Each Morpheus Puppet integration ties to a specific Puppet Master and makes it easy to install the Puppet Agent onto target Instances and Servers. Once integrated, we can trigger the agent installation by creating Puppet Agent Install Tasks through Morpheus automation or at provision time when spinning up instances in Clouds associated with a Puppet integration.

Add Puppet Integration

1. Navigate to Administration > Integrations
2. Click + NEW INTEGRATION
3. Select Integration type “Puppet”
4. Populate the following fields
   - Name: A friendly name for this Puppet integration in Morpheus
   - Enabled: When marked, this Puppet integration will be available to users at provision time and when creating Tasks
   - Puppet Master (Hostname): The resolvable DNS name to the Puppet Master, communicating on port 443 by default
   - Allow Immediate Execution: Yes or No (See additional details below)
5. Click SAVE CHANGES
Allow Immediate Execution

When adding or editing a Puppet integration, users have the option to “Allow Immediate Execution”. Using this feature will connect to the Puppet Master after the Puppet Agent is installed and force configuration application immediately. This is an optional convenience feature, if it’s not used, the Puppet Master will still apply configuration to the node on its own schedule. Using this feature requires supplying SSH credentials. If you do not wish to provide SSH credentials to Morpheus select “No” to opt out of this feature and they do not need to be provided.

Associating a Puppet Integration with a Cloud

By associating a Puppet Integration with a Cloud, users are able to automatically install the Puppet Agent, select a Puppet environment, and supply a Puppet Node Name at provision time. The integration association is made when adding or editing a Cloud integration in Morpheus.

1. Navigate to Infrastructure > Clouds
2. Identify the Cloud to associate with Puppet and edit it by clicking on the pencil icon at the right end of the row
3. In the EDIT CLOUD modal, expand the Advanced Options section
4. In the CONFIG MANAGEMENT dropdown, choose the Puppet integration
5. Save changes to the Cloud integration
Creating Puppet Agent Install Tasks

Puppet Agent Install Tasks automate the process of installing the Puppet Agent, selecting the Puppet environment, and supplying the Puppet Node Name. We can run this Task on-demand as needed for individual Instances or servers or add them to workflows to build a Puppet Agent installation step into larger automation suites.

1. Navigate to Library > Automation
2. Select the Tasks tab
3. Click + ADD
4. From the “Type” field, select Puppet Agent Install
5. Complete the fields as needed to target a specific Puppet Master and to identify Puppet environment and node names
6. Save changes
Installing Puppet Agent at Provision Time

With a Puppet integration associated with a Cloud (as described above), users can opt to install the Puppet Agent at provision time. When provisioning into an associated Cloud, a new “Puppet” section will appear on the CONFIGURE tab of the provisioning wizard. Here users can select a specific Puppet Master, select the Puppet environment, and select a Puppet node name. During provisioning, the Puppet Agent will be automatically installed and configured for the selected Master.

12.9.5 Salt

Overview

Morpheus integrates with an existing Salt Master for seamless deployment of Salt States to Minions provisioned from Morpheus.

Add Salt Integration

To get started browse to Admin > Integrations from within Morpheus.

Once there simply add a New Integration

And then scope the integration to your existing Salt Master by ip address. Make sure that the username entered is one with proper escalation privileges for running Salt, and point the Working Directory at the directory on your Master where your States live.

Note: Morpheus will allow you to run States from a git backend, but in v2.10 you will not see states from a git
backend within Morpheus
Scope Salt Integration to Group Or Cloud

Configuration Management integrations like Saltstack apply to the Infrastructure Group abstraction in Morpheus. To tie yours in, browse to Infrastructure > Groups in Morpheus and select the group that you would like to tie to your Salt Master.

From here select Edit.

And from the options toggle Advanced Options and select your Saltstack integration in the Config Management drop-down.
After a page refresh you should see your Saltstack tab in your group page.

Clicking on it will reveal a page that includes:

**12.9. Automation Integrations**
1. An interface to run Salt Master commands
2. Parsed Top File
3. Available States

The classic example of running

```
salt '*' test.ping
```

will return empty unless there are existing Minions with accepted keys on the Master. However, provisioning Minions via Morpheus is extremely easy.
Provisioning with Saltstack

To do so, provision as usual and Instances within the Group tied to the Saltstack Integration will now show additional options on the Configure pane.

Minion ID defaults to the hostname, and a State can be applied directly at provision time.
Note: Only States served from the Master’s Working Directory can be applied at provision, not States from a git backend.

Once your instance is provisioned and key negotiation has completed you will be able to access it and run commands via the integrated Salt command center in your Group.

If you did not apply a state at provision time now you will be able to run State commands through Morpheus.
In our example the Apache State from a git backend was applied successfully to our newly created vm.
12.9.6 Terraform

Requirements

Role Access

- In order to see the Terraform Blueprint type option and create Terraform App Blueprints in Library > Blueprints > App Blueprints, the Morpheus user must have Role permissions for Provisioning: Blueprints - Terraform set to Full.
- In order to provision Terraform Apps in Provisioning > Apps, the Morpheus user must have Role permissions for Provisioning: Blueprints > Terraform set to Provision or Full.
- Existing Terraform Blueprints must be added before they can be provisioned from Provisioning > Apps.

Github/Git Repo

- To use .tf files from a Git repo a Git or Github integration needs to be configured in Administration > Integrations. If one is not configured .tf or .tf.json files can be manually added to Terraform App Blueprints.

Supported App Provisioning Targets

- VMware
- Amazon AWS
- Microsoft Azure
- Oracle Cloud

Note: Additional clouds will be available in later releases.

Terraform Installation

Morpheus will automatically install Terraform locally upon the first Terraform App provision. It is possible on some operating system configurations for the automated terraform installation to fail, in which case it can be manually installed (run `terraform --version` to verify).

To manually install and configure terraform on the Morpheus Appliance:

1. Run the following cURL on the Morpheus Appliance to install Terraform:

   ```bash
curl -k -s "https://applianceServerUrl/api/server-script/terraform-install?local=true" | bash
   ```

   Note: Replace applianceServerUrl with your Morpheus appliance URL or IP address.

2. Copy the Terraform directory at `/usr/local/bin/terraform` to `/usr/sbin/terraform`

   ```bash
cp /usr/local/bin/terraform /usr/sbin/terraform
   ```

   Terraform is now installed and configured, and Terraform apps can be provisioned from Morpheus.
Creating Terraform App Blueprints

In order to provision Terraform apps, Terraform App Blueprints must be created first.

**Important:** In Morpheus version 4.2.0, VMware and AWS Cloud types are supported for Terraform App provisioning targets. Additional clouds will be available in later releases.

1. Navigate to Library > Blueprints > App Blueprints
2. Select + ADD
3. Name the Blueprint and select *Terraform* type.

**Note:** In order to see the Terraform Blueprint type option, the Morpheus user must have Role permissions for *Provisioning: Blueprints - Terraform* set to *Full*.

4. Select NEXT
5. Configure the following:

   **NAME**  Name of the
   **DESCRIPTION**  Description for you App Blueprints shown in the Apps list (optional)
   **CATEGORY**  App Category (optional)
   **IMAGE**  Add reference image/picture for your App Blueprint (optional)
   **CONFIG TYPE** (select Terraform, Terraform.json, or Git Repository)

   **Terraform (.tf)**
   - **CONFIG**  Paste in the .tf contents in the config section. Variables will be presented as input fields during App provisioning, or auto-populated with matching values if contained in a selected TFVARM Secret file added to the Cypher service.

   **Terraform JSON (.tf.json)**  Paste in .tf.json contents in the config section. Variables will be presented as input fields during App provisioning, or auto-populated with matching values if contained in a selected TFVARM Secret file added to the Cypher service.

   **Git Repository**
   - **SCM Integration**  Select a Github SCM integration that has been added in Administration - Integrations. If using a Git Repository integration from Administration - Integrations this filed can be skipped.
   - **Repository**  Select repository from selected SCM integration, or Git Repository integration from Administration - Integrations if no SCM/Github Integration is selected.
   - **BRANCH OR TAG**  i.e. master (default)
   - **WORKING PATH**  Enter the repo path for the .tf files (s). . / is default.
   - **CONFIG**  .tf files found in the working path will populate in the CONFIG section.

   **Note:** If no files are found please ensure your Github or Git integration is configured properly (Private repos need to have a key pair added to Morpheus, the keypair selected on the integration in Morpheus, and the keypair’s public key added to the GitHub users SSH keys in github or to the git repo).
TFVAR SECRET  Select a tfvars secret for .tf variables. Tfvars secrets can be added in Services > Cypher using the tfvars/name mountpoint. This allows sensitive data and passwords to be encrypted and securely used with Terraform Blueprints.

OPTIONS example -var 'instanceName=sampleTfApp'

6. Select SAVE

Your Terraform App is ready to be provisioned from |ProApp|.

Provisioning Terraform Apps

Note: An existing Terraform App Blueprints must be added to Library > Blueprints > App Blueprints before it can be provisioned.

Note: In order to provision Terraform Apps in |ProApp|, the Morpheus user must have Role permissions for Provisioning: Blueprints - Terraform set to Provision or Full.

1. Navigate to |ProApp|
2. Select + ADD
3. Choose and existing Terraform App Blueprint
4. Select NEXT
5. Enter a NAME for the App and select the Group, Default Cloud and Environment (optional)
6. Select NEXT
7. Populate any required variables in the Terraform Variables section. ..TIP:: If the tf CONFIG data needs to be edited, select the RAW section, edit, and then select the BUILDER section again. The CONFIG changes from the RAW edit will be updated in the CONFIG section.
8. Select COMPLETE

The Terraform App will begin to provision.

Once provisioning is completed, note the TERRAFORM tab in the App details page (|ProApp| > select the App). This section contains State and Plan output:
12.9. Automation Integrations
12.9.7 vRealize Orchestrator

The vRealize Orchestrator (vRO) Integration provided for Morpheus enables users to easily trigger existing workflows that may already exist in vRealize Orchestrator. Not only can the user trigger these workflows, but they can also be chained easily into non-vRO workflows and process both output and input parameters of a workflow.

Adding the Integration

Setting up the vRO integration involves some steps which vary depending on the authentication model being used. When using OAUTH, the Client ID must be gathered first. This can be found by browsing a file on the actual VRA server using SSH. On the vRA server, run the following command:

```
grep -i cafe_cli= /etc/vcac/solution-users.properties | sed -e 's/cafe_cli=//' 
```

Secondly, you will need the username, password, and host API URL. Typically, the API URL is run on port 8283. A sample API URL may look like the following example: `https://vrahost.com:8283/`

Be sure to fill in the tenant token as the domain or tenant ID, for example: `vsphere.local`, with a username of `administrator@vsphere.local`.

Note: At times, this can vary depending on how authentication and role assignments for the user have been set up for vRO.

vRA auth uses vRA identity Bearer tokens for API consumption. The only real difference in field requirements when using this authentication mode is that the `Client ID` is no longer needed.

Using vRealize Orchestrator

One of the first things Morpheus does when it is tied into a vRO integration is sync all available workflows by category. These workflows become available when creating a new Morpheus task in Library > Automation. Morpheus allows a user to map these vRO workflows into the task engine. The task engine allows users to design workflows that chain tasks in order or operate at different phases of a provisioning request. For more information on tasks, please read the Automation documentation.

Creating a task for VRO is simple. First, go to Library > Automation and create a new task. Choose a task type of `vRealize Orchestrator Workflow`. A dropdown will appear allowing one to first select the active vRO Integration you would like to use. Once that is selected, a list of workflows becomes available.

Note: The next part is where things can get a bit tricky. The parameter body (expected in JSON) format can be a bit difficult to track down. One way is to use the Network Chrome inspector when kicking off a sample workflow from the vRO HTML5 client and grabbing the parameter JSON. Another is to query the API yourself and look at the samples from historical run history.

An example payload for the `SSH / Run SSH Command` Workflow would look like this:

```json
{
   "parameters": [
   {
      "name": "hostNameOrIP",
      "type": "string",
      "value": 
```
"string": {  
  "value": "x.x.x.x"
}
},
{
  "name": "port",
  "type": "number",
  "value": {
    "number": {
      "value": 22
    }
  }
},
{
  "name": "cmd",
  "type": "string",
  "value": {
    "string": {
      "value": "echo \"Hello <%=instance.name%>\"
    }
  }
},
{
  "name": "encoding",
  "type": "string",
  "value": {
    "string": {
      "value": ""
    }
  }
},
{
  "name": "username",
  "type": "string",
  "value": {
    "string": {
      "value": "myuser"
    }
  }
},
{
  "name": "passwordAuthentication",
  "type": "boolean",
  "value": {
    "boolean": {
      "value": true
    }
  }
},
{
  "name": "password",
  "type": "string",
  "value": {
    "string": {
      "value": "password"
    }
  }
}
"name": "path",
  "type": "string",
  "value": {
  "string": {
    "value": "/var/lib/vco/app-server/conf/vco_key"
  }
}
},
{
  "name": "passphrase",
  "type": "string",
  "value": {
    "string": {
      "value": ""
    }
  }
}
]

Note that all Morpheus variables can be injected into the parameter body. In the above example we inject the instance name into the sample command with <%=instance.name%>.

Adding this task to a workflow allows the result parameters to be referenced in subsequent tasks called throughout the workflow. For example, a local script task type could reference the output text of the above ssh command by injecting the following results map: echo "results.vro: <%=results.vro.find{it.name == 'outputText'}?.value?.string?.value%>"

There are very powerful options available for chaining results and injecting variables relevant to the instance being provisioned or even custom inputs from an operational workflow. Please reference the rest of the Automation documentation for examples.

12.10 Backups

12.10.1 Commvault

Morpheus integrates with Commvault for selection as a Cloud backup target. Compatible Clouds include VMware and OpenStack. Morpheus integrates with your existing Commvault appliance, which can then be set as the preferred backup solution for any existing Clouds. From there, easily schedule backup routines during Instance provisioning and restore Instances when needed. This section discusses the process for integrating Commvault with Morpheus, sharing a Commvault integration with multiple Tenants, setting backup during Instance provisioning, and restoring Instances from backup.
Features

- Share one backup provider across multiple Tenants
- Apply Commvault integration as the default backup target for compatible clouds
- Select Commvault integrations as backup provider at Instance provision time
- Automate backups with Morpheus Backup Jobs
- When needed, easily restore Instance backups

Adding Commvault Integration

1. Navigate to Backups > Services
2. Select + ADD
3. Select Commvault
4. Fill in the following:
   - **Name** Name of the Integration in Morpheus
   - **Enabled** Enable the Commvault integration
   - **Host** IP or Hostname of the Commvault server.
   - **Port** Port number configured to access the Commvault server.
   - **Username** Admin Username for Commvault
   - **Password** Password for Username provided (encrypted in Morpheus).
   - **Visibility**
     - **Private** Only Available to the Tenant the Integration is added by
     - **Public** Available to Sub-Tenants (master tenant option only)
5. SAVE

Tip: Enter the port to connect with the Commvault web server, by default this is port 81. For more, see Commvault port requirement documentation.

Set Commvault as Cloud Backup Target

Once the initial integration is made, set this integration as the backup provider for as many supported Clouds as needed. Commvault integrations are supported as backup target for VMware and OpenStack Clouds at this time.

1. Navigate to Infrastructure > Clouds
2. Select an existing VMware or OpenStack Cloud
3. Click EDIT
4. Expand the Advanced Options section
5. Under “Backup Provider”, select the relevant Commvault integration
6. Click SAVE CHANGES
Configure Backup at Provision Time

When provisioning an Instance into a Cloud where Commvault is set as the backup provider, Commvault will be selectable as the “Backup Type” on the Automation tab of the provisioning wizard. Expand the Backups section on this tab and enter the following:

- **Backup Type**: Select the desired Commvault backup type
- **Backup Server**: Select the desired server synced from the Commvault backup provider associated with the Cloud
- **Backup Set**: Select a configured backup set synced from the Commvault backup provider associated with the Cloud
- **Storage Policy**: Gold, Silver, or Bronze. Select the applicable SLA or retention policy for the workload being provisioned. The meanings of these retention tiers are configurable in Commvault
- **Backup Name**: A name for the backup in Morpheus, this field is pre-populated with the Instance name but can be overwritten
- **Backup Job Type**: Clone an existing backup job (Backups > Jobs) or add this backup to an existing job. A job contains a retention count and backup frequency schedule and can have as many Instances backing up under it as needed
- **Backup Job**: Select the job which will be cloned or have a backup added to it depending on your selection in the prior field
• **Job Name:** A name for the new cloned job (if you are cloning and not creating a new Backup Job)

Viewing Backups

After provisioning, users can review backup details from the Instance detail page (Provisioning > Instances > Selected Instance > Backups tab). Additionally, backups can be configured here if this was not done during provision time by clicking *ADD BACKUP*. Users can also run one-off backups from this page by opening the ACTIONS menu and clicking Backup. Backups will still continue to run based on the schedule configured in their job but additional runs can be made on-demand this way.

Within the Backups section (Backups > Backups) users can also view all currently-configured backups and whether or not recent backup runs have succeeded.
For Instances with current backups, the Backup Results section will be populated on the Instance detail page (Provisioning > Instances > Selected Instance > Backup tab). If the Instance needs restored, simply click Actions (within the Backup Results area, not the main actions menu for the Instance itself) and then click Restore. The status icon at the top of the Instance detail page will turn green once this process is finished and the Instance will be fully restored from your selected backup.

12.10.2 Veeam

Veeam is a backup and replication platform designed to work with popular on-prem cloud providers, including VMware, Microsoft Hyper-V, and vCloud Director. Morpheus integrates with your existing Veeam appliance which can then be set as the preferred backup solution for any existing Clouds. From there, easily schedule backup routines during Instance provisioning and restore Instances when needed. This section discusses the process for integrating Veeam with Morpheus, sharing a Veeam integration with multiple Tenants, setting backup during Instance provisioning, and restoring Instances from Veeam backup.
Features

- Share one backup provider across multiple Tenants
- Apply Veeam integration as the default backup target for compatible clouds
- Select Veeam integrations as backup provider at Instance provision time
- Automate backups with Morpheus Backup Jobs
- When needed, easily restore Instance backups

Adding Veeam Integration

1. Navigate to Backups > Integrations
2. Select + ADD
3. Select Veeam
4. Fill in the following:
   - **Name** Friendly name for the integration in Morpheus
   - **Enabled** When marked, this integration will be active and available for use
   - **API URL** IP or Hostname of the Veeam Enterprise Manager, must be HTTPS for VEEAM 10
   - **Port** Port number configured to access the Veeam server, must be 9398 for VEEAM 10
   - **Username** Username for an admin service account in Veeam
   - **Password** Password for Username provided (encrypted in Morpheus)
   - **Visibility**
     - **Private** Only available to the Tenant that added the integration
     - **Public** Available to Subtenants (primary tenant option only)
5. Click SAVE

**Note:** Veeam Backup Enterprise Manager must be installed in order to successfully integrate Morpheus with Veeam.

**Important:** Once Veeam service has been integrated with Morpheus, Veeam server(s) will be available to select as the backup provider for VMware, Hyper-V, and vCloud Director cloud integrations (Infrastructure > Clouds > Edit a compatible Cloud). To enable Veeam backups, select the appropriate Veeam server as the “backup provider” for your cloud integrations as needed. Failure to do so will result in blank Backup Repositories and Backup Job Templates options when configuring Veeam Backups during provisioning.
Set Veeam as Cloud Backup Target

Once the initial integration is made, set this integration as the backup provider for as many supported Clouds as needed. Veeam integrations are supported as backup target for VMware, Hyper-V, and vCloud Director Clouds at this time.

1. Navigate to Infrastructure > Clouds
2. Select an existing VMware, Hyper-V, or vCD Cloud
3. Click EDIT
4. Expand the Advanced Options section
5. Under “Backup Provider”, select the relevant Veeam integration
6. Click SAVE CHANGES

Configure Backup at Provision Time

When provisioning an Instance into a Cloud where Veeam is set as the backup provider, Veeam will be selectable as the “Backup Type” on the Automation tab of the provisioning wizard. Expand the Backups section on this tab and enter the following:

- **Backup Type**: Select the desired Veeam backup type
- **Repository**: Select a repository synced from the Veeam backup provider associated with the Cloud
- **Managed Server**: Select a managed server associated with the backup server selected in the previous step
• **Backup Name:** A name for the backup in Morpheus, this field is pre-populated with the Instance name but can be overwritten

• **Backup Job Type:** Clone an existing backup job (Backups > Jobs) or add this backup to an existing job. A job contains a retention count and backup frequency schedule and can have as many Instances backing up under it as needed

• **Backup Job:** Select the job which will be cloned or have a backup added to it depending on your selection in the prior field

• **Job Name:** A name for the new cloned job (if you are cloning and not creating a new Backup Job)

---

**Viewing Backups**

After provisioning, users can review backup details from the Instance detail page (Provisioning > Instances > Selected Instance > Backups tab). Additionally, backups can be configured here if this was not done during provision time by clicking **ADD BACKUP**. Users can also run one-off backups from this page by opening the ACTIONS menu and clicking Backup. Backups will still continue to run based on the schedule configured in their job but additional runs can be made on-demand this way.

Within the Backups section (Backups > Backups) users can also view all currently-configured backups and whether or not recent backup runs have succeeded.
Restore an Instance from Veeam

For Instances with current backups, the Backup Results section will be populated on the Instance detail page (Provisioning > Instances > Selected Instance > Backup tab). If the Instance needs restored, simply click Actions (within the Backup Results area, not the main actions menu for the Instance itself) and then click Restore. The status icon at the top of the Instance detail page will turn green once this process is finished and the Instance will be fully restored from your selected backup.

12.10.3 Rubrik

Adding Rubrik Integration

Note: The Rubrik backup service is currently only supported on the VMware cloud type.

1. Navigate to Backups > Services
2. Select + ADD
3. Select Rubrik
4. Fill in the following:
**Name** Name of the Integration in Morpheus

**Enabled** Enable the Integration

**Host** IP or Hostname of the Rubrik api server.

**Username** Admin Username for Rubrik

**Password** Password for Username provided (encrypted in Morpheus).

**Visibility**

Sets Multi-Tenant Visibility

**Private** Only Available to the Tenant the Integration is added by

**Public** Available to Sub-Tenants (master tenant option only)

5. **SAVE**

### 12.10.4 Zerto

**Adding Zerto Integration**

1. Navigate to **Backups > Integrations**
2. Select **+ ADD**
3. Select Zerto
4. Fill in the following:
   - **Name** Name of the Integration in Morpheus
   - **Enabled** Enable the Integration
   - **API URL**
     - **API URL for Zerto Virtual Manager** Example `API URL: https://zvm_IP:9669`
   - **Username** Admin Username for Zerto
   - **Password** Password for Username provided (encrypted in Morpheus).
   - **Visibility**
     - **Sets Multi-Tenant Visibility**
       - **Private** Only Available to the Tenant the Integration is added by
       - **Public** Available to Sub-Tenants (master tenant option only)

5. **SAVE**
12.10.5 Avamar

IMPORTANT: Avamar API must be installed on Avamar server (not installed by default)

Adding Avamar Integration

1. Navigate to Backups > Services
2. Select + ADD
3. Select Avamar
4. Fill in the following:
   - **Name**: Name of the Integration in Morpheus
   - **Enabled**: Enable the Integration
   - **Host**: IP or Hostname of the Avamar api server.
   - **Port**: Port number configured to access the Avamar server
   - **Username**: Admin Username for Avamar
   - **Password**: Password for Username provided (encrypted in Morpheus).
   - **Tenant**: Avamar Tenant/Domain to scope Integration to
   - **Hypervisor**: Avamar Hypervisor to scope Integration to
   - **Visibility**:
     - **Private**: Only Available to the Tenant the Integration is added by
     - **Public**: Available to Sub-Tenants (master tenant option only)
5. SAVE

12.11 Build

12.11.1 Jenkins

The Morpheus Jenkins Integration is easy to add and will allow you to see all jobs, builds, statuses of those builds, commits notes, and links to artifacts.
Adding Jenkins Integration

1. Navigate to Administration > Integrations
2. Select + NEW INTEGRATION
3. Select Jenkins
4. Fill in the following:
   - **Name**: Name of the Integration in Morpheus
   - **Enabled**: Enable the Integration. Uncheck to disable the Jenkins Integration sync Job.
   - **Jenkins URL**: Jenkins URL or IP address. ex: https://jenkins.morpheus.com
   - **Username**: Jenkins service account username
   - **Password**: Jenkins service account password
5. SAVE CHANGES

**Important**: By default Jenkins is configured to run on port 8080. If this has been modified you will need to append the alternate port to the Jenkins URL.
Viewing Jobs in Jenkins Integration

In the Morpheus Jenkins integration you can view all of your jobs.

Viewing Builds and Build Statuses

In the Morpheus Jenkins integration you can view recent builds with ID, Status, Date, Duration, Artifacts, Commit Notes and Run By user data. Artifacts will automatically link to the Artifact url in Jenkins, and the urls can be used in Morpheus Deployments (dependent on Jenkins configuration).
12.12 Clouds

12.12.1 AWS

Overview

AWS is the Amazon public cloud, offering a full range of services and features across the globe in various datacenters. AWS provides businesses with a flexible, highly scalable, and low-cost way to deliver a variety of services using open standard technologies as well as proprietary solutions. This section of documentation will help you get Morpheus and AWS connected to utilize the features below:
Features

• Instance, Service, Infrastructure Provisioning & Synchronization
• EKS Cluster Creation & Synchronization
• Morpheus Kubernetes, Docker & KVM Cluster Creation
• ELB Classic Load Balancer Creation & Synchronization
• ELB Application Load Balancer (ALB) Creation & Synchronization
• Security Group Creation & Synchronization
• Security Group Rule Creation & Synchronization
• Network Synchronization
• VPC Creation & Synchronization
• CloudFormation Provisioning & Resource Synchronization
• Terraform Provisioning & Resource Synchronization
• Pricing & Costing Synchronization
• MetaData Tag Creation & Synchronization
• S3 Bucket Creation & Synchronization
• Route53 Automation & Synchronization
• IAM Profile Synchronization and Assignment
• RDS Support
• Backups / Snapshots
• Migrations
• Auto Scaling
• Remote Console (SSH & RDP)
• Lifecycle Management and Resize
• Restore from Snapshots
• Elastic IP Assignment
• Network Pools
• Enhanced Invoice Costing

Requirements

**AWS IAM Security Credentials**  Access Key Secret Key Sufficient User Privileges (see MinimumIAMPolicies section for more info)

**Security Group Configuration for Agent Install, Script Execution, and Remote Console Access**

• Typical Inbound ports open from Morpheus Appliance: 22, 5985, 3389 (22 & 3389 required for Console. 22 & 5985 required for agent-less comms)
• Typical Outbound to Morpheus Appliance: 443 (Required for Agent install & comms)
Note: These are required for Morpheus agent install, communication, and remote console access for windows and linux. Other configurations, such as docker instances, will need the appropriate ports opened as well. Cloud-init Agent Install mode does not require incoming access for port 22.

Network(s) IP assignment required for Agent install, Script Execution, and Console if the Morpheus Appliance is not able to communicate with AWS instances private ip’s.

Adding an AWS Cloud

1. Navigate to Infrastructure > Clouds
2. Select + Create Cloud
3. Select AWS
4. Enter the following:

Cloud Configuration

NAME Name of the Cloud in Morpheus
CODE Unique code used for api/cli, automation and policies.
LOCATION Description field for adding notes on the cloud, such as location.
VISIBILITY For setting cloud permissions in a multi-tenant environment. Not applicable in single tenant environments.
TENANT If Visibility is set to Private, select the Tenant the Cloud resources will assigned to.
ENABLED When disabled, automatic Cloud sync is paused and the Cloud will not be selectable for provisioning.
AUTOMATICALLY POWER ON VMS When enabled, Morpheus will maintain the expected power state of managed VMs. Morpheus will power on any managed VMs in the Cloud that have been shut down for unknown reasons (not powered off by Morpheus) to ensure availability of services.

Note: When “AUTOMATICALLY POWER ON VMS” is enabled, the power state of managed VMs should be maintained in Morpheus. This setting is not applicable to discovered/unmanaged resources.

Details

REGION Select AWS Region for the Cloud
ACCESS KEY Access Key ID from AWS IAM User Security Credentials.
SECRET KEY Secret Access Key associated with the Access Key ID.
USE HOST IAM CREDENTIALS Check to use use Host IAM Credentials
ROLE ARN Supports security token service (STS) to AssumeRole by entering an AWS Role ARN
INVENTORY
Basic Morpheus will sync information on all EC2 Instances in the selected VPC the IAM user has access to, including Name, IP Addresses, Platform Type, Power Status, and overall resources sizing for Storage, CPU and RAM, every 5 minutes. Inventoried EC2 Instances will appear as Unmanaged VM's.

Full In addition to the information synced from Basic Inventory level, Morpheus will gather Resource Utilization metrics for Memory, Storage and CPU utilization per VM.

Off Existing EC2 Instances will not be inventoried

Note: Cloud Watch must be configured in AWS for Morpheus to collect Memory and Storage utilization metrics on inventoried EC2 instances.

USE VPC Specify if the target account is using EC2-VPC or EC2-Classic Platform. In almost all cases, VPC should be selected, and then select the target VPC from the synced available VPC's list, or All VPC's.

5. The AWS cloud is ready to be added to a group and saved. Additional configuration options available:

IMAGE TRANSFER STORE S3 bucket for Image transfers, required for migrations into AWS.

EBS ENCRYPTION Enable or disable encryption of EBS Volumes

COSTING KEY For Gov Cloud pricing only, key for standard managing cost account

COSTING SECRET For Gov Cloud pricing only, secret for standard managing cost account

Advanced Options

DOMAIN Specify a default domain for instances provisioned to this Cloud.

SCALE PRIORITY Only affects Docker Provisioning. Specifies the priority with which an instance will scale into the cloud. A lower priority number means this cloud integration will take scale precedence over other cloud integrations in the group.

APPLIANCE URL Alternate Appliance url for scenarios when the default Appliance URL (configured in admin > settings) is not reachable or resolvable for Instances provisioned in this cloud. The Appliance URL is used for Agent install and reporting.

TIME ZONE Configures the time zone on provisioned VM’s if necessary.

DATACENTER ID Used for differentiating pricing among multiple datacenters. Leave blank unless prices are properly configured.

NETWORK MODE Unmanaged or select a Network Integration (NSX, ACI etc)

LOCAL FIREWALL On or Off. Enable to managed Host and VM firewall/IP Table rules (linux only)

SECURITY SERVER Security Server setting is for Security Service Integrations such as ACI

TRUST PROVIDER Select Internal (Morpheus) or an existing Trust Provider Integration

STORAGE MODE Single Disk, LVM or Clustered

BACKUP PROVIDER Select Internal Backups (Morpheus) or a Backup Integration

REPLICATION PROVIDER Sets the default Replication Provider for the Cloud. Select an existing Replication Provider Integration

GUIDANCE Enable Guidance recommendations on cloud resources.

COSTING Enable for Morpheus to sync Costing data from the Cloud provider, when available. For on-prem Clouds, enabling costing activates a costing service designed to mirror the live costing experience of public clouds, including invoicing with line items and real-time cost data (Operations > Costing > Invoices). If your organization
utilizes reserved instances and you want to pull in related pricing data, select *Costing and Reservations*. If this is not relevant, select *Costing* to save money on additional calls to the AWS Cost Explorer API or similar service for other clouds.

**DNS INTEGRATION**  Records for instances provisioned in this cloud will be added to selected DNS integration.

**SERVICE REGISTRY**  Services for instances provisioned in this cloud will be added to selected Service Registry integration.

**CONFIG MANAGEMENT**  Select a Chef, Salt, Ansible or Puppet integration to be used with this Cloud.

**CMDB**  Select CMDB Integration to automatically update selected CMDB.

**CMDB DISCOVERY**  When checked, any automatically discovered (unmanaged) servers onboarded into Morpheus from this Cloud will also have CMDB records created for them.

**CHANGE MANAGEMENT**  Select an existing Change Management Integration to set on the Cloud. ex: Cherwell

**AGENT INSTALL MODE**
- SSH / WINRM: Morpheus will use SSH or WINRM for Agent install.
- Cloud Init / Unattend (when available): (DEFAULT) Morpheus will utilize Cloud-Init or Cloudbase-Init for agent install when provisioning images with Cloud-Init/Cloudbase-Init installed. Morpheus will fall back on SSH or WINRM if cloud-init is not installed on the provisioned image. Morpheus will also add Agent installation to Windows unattend.xml data when performing Guest Customizations or utilizing syspreped images.

**API PROXY**  Set a proxy for outbound communication from the Morpheus Appliance to the Cloud endpoints. Proxies can be added in the *Infrastructure > Networks > Proxies* tab.

**INSTALL AGENT**  Enable to have Agent Installation on by default for all provisioning into this Cloud. Disable for Agent Installation to be off by default for all provisioning into this Cloud.

**Provisioning Options**

**PROXY**  Set a proxy for inbound communication from Instances to the Morpheus Appliance. Proxies can be added in the *Infrastructure > Networks > Proxies* tab.

**Bypass Proxy for Appliance URL**  Enable to bypass proxy settings (if added) for Morpheus Agent communication to the Appliance URL.

**NO PROXY**  Include a list of IP addresses or name servers to exclude from proxy traversal


**KMS KEY ID**  For specify an AWS KMS key for encrypting EBS Volumes when volume encryption is enabled

**Enhanced Invoice Costing Configuration**

AWS cloud integrations in Morpheus will sync highly-granular costing data through the use of AWS Costing & Utilization Reports (CUR). If desired, users can turn on costing in the Morpheus Cloud configuration without linking a CUR to use AWS Cost Explorer instead. Morpheus version 4.2.3 also simplified the way CUR reports can be selected or created in order to sync costing data. The section below discusses setting up enhanced costing through CUR reports both in 4.2.3 and versions prior. For additional details on setting up costing with AWS GovCloud, see the next section.

**Note:**  Even with a costing report configured in the Cloud integration as described below, the COSTING value must also be set to “Costing and Reservations” in order for enhanced invoice data to be brought into Morpheus. Confirm
this setting by editing the Amazon Cloud integration, and checking the COSTING value in the Advanced Options panel before continuing.

**v4.2.3 and Above**

In Morpheus 4.2.3+, edit the Amazon cloud integration or create a new Amazon Cloud to get started. On the Create/Edit Cloud modal, open the advanced options section. The relevant fields for configuring invoice costing are shown below:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>COSTING REPORT</td>
<td>New Report</td>
</tr>
<tr>
<td>COSTING REPORT NAME</td>
<td>test_report</td>
</tr>
<tr>
<td>COSTING FOLDER</td>
<td>reports</td>
</tr>
<tr>
<td>COSTING BUCKET</td>
<td>New Report Bucket</td>
</tr>
<tr>
<td>COSTING BUCKET NAME</td>
<td>new_bucket</td>
</tr>
<tr>
<td>COSTING BUCKET REGION</td>
<td>US West (N. California)</td>
</tr>
<tr>
<td>COSTING KEY</td>
<td></td>
</tr>
<tr>
<td>COSTING SECRET</td>
<td></td>
</tr>
<tr>
<td>LINKED ACCOUNT ID</td>
<td></td>
</tr>
</tbody>
</table>

In the example case above, a new report and a new S3 bucket are created but Morpheus will also sync in buckets and reports that meet the required parameters if they already exist. For reports to be synced they must meet the requirements listed below:

- Hourly time granularity
- Include resource IDs
- GZIP compression
- CSV format

If you don’t currently have a report meeting those criteria, you can create one by selecting “New Report” from the
REPORT NAME dropdown menu. A new S3 bucket can be created in similar fashion if needed. You may also want to review the section below on configuration for Morpheus 4.2.2 and below to note policies that will be applied to your selected bucket and Cost Explorer permissions required for the AWS cloud user associated with the Morpheus Cloud integration.

In the end, the following fields must be filled in order to complete the process:

- **COSTING BUCKET**: The S3 bucket name
- **COSTING REGION**: The region the bucket was created in
- **COSTING FOLDER**: This is the report path prefix if you configured one earlier
- **COSTING REPORT NAME**: The name given to your CUR report
- **COSTING KEY**: If the IAM user for this AWS cloud integration does not have access to the S3 bucket with the CUR data, enter the AWS Key ID for an IAM user with access
- **COSTING SECRET**: If the IAM user for this AWS cloud integration does not have access to the S3 bucket with the CUR data, enter the AWS Secret Key for the IAM account whose Key ID you entered in the previous field
- **LINKED ACCOUNT ID**: If the IAM user for this AWS cloud integration does not have access to the S3 bucket with the CUR data, enter the AWS account number that the IAM user from the above step resides in

**Note**: If the AWS cloud account is a GovCloud account, enter the COSTING KEY, COSTING SECRET, and LINKED ACCOUNT ID for the master commercial account your GovCloud account is associated with.

v4.2.2 and Below

Begin by logging into the AWS Billing Console, then click *Create report.*
AWS Cost and Usage Reports

AWS Cost and Usage reports provide access to detailed data, enabling you to better analyze and understand your AWS usage amounts underlying those costs. You can customize the content and delivery of your reports and manage them.

Create report

Other Reports

You will be able to see your spend data within 24 hours of enabling reports.

Enable Reports

- Analyze your cost and usage using AWS Cost Explorer
  - AWS Cost Explorer lets you dive deeper into your cost and usage data to identify trends, pinpoint cost drivers, and view cost breakdowns by resource.

- Monitor your Reserved Instance (RI) utilization using AWS Cost Explorer
  - This report allows you to visualize your RI utilization, providing insight into opportunities for increasing your RI utilization.

AWS Usage Report

A CSV report that provides usage data for select AWS services.

Include a name for your report and mark the box to “Include resource IDs”. Morpheus uses these resource IDs to map costs to various resources. Click Next.
On the following page, begin by identifying an S3 bucket to house reports. Click *Configure* near the top of the page and select an existing bucket or create a new one.
After identifying the bucket, you must mark the box to accept the default policy being applied to the bucket. Click "Save."

The default policy applied to the bucket is below:
After choosing a bucket, accepting the default policy, and saving the change, you're brought back to the report delivery page. By default, CUR reports are saved to a folder at the path `my-report-name/date-folder`. If this bucket already contains CUR reports, you may want to specify a prefix path in the "Report path prefix" field. Outside of this field, use the default values as shown in the screenshot below, then click Next.
On the following page, make your final review and click Review and Complete. Following this, you will see your newly configured report in the list of CUR report(s).

In addition, the AWS cloud user associated with the integration in Morpheus needs IAM policy permission to access Cost Explorer. Attach a policy like the one below to this cloud user:

```json
{
    "Version": "2012-10-17",
    "Id": "SomeID",
    "Statement": [
        {
            "Sid": "SomeStmtID",
            "Effect": "Allow",
            "Action": [
                "ce:DescribeReportDefinitions",
                "ce:DescribeCostCategoryDefinition",
                "ce:ListCostCategoryDefinitions"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```
**Note:** If the Cost Explorer permissions are granted at the master account level, the user will see all costs for each member account; if granted at the member account, only the costs for that member account are available.

With the AWS console configuration steps complete, we can move back into Morpheus. Keep in mind it is only necessary to set up one AWS cloud for Costing since we process all records in the CUR report.

Once back in Morpheus, add or edit the relevant AWS cloud integration (Infrastructure > Clouds > + ADD OR click the pencil icon in the row for the chosen AWS integration). Expand the Advanced Options drawer and complete the following fields:

- **COSTING BUCKET:** The S3 bucket name
- **COSTING REGION:** The region the bucket was created in
- **COSTING FOLDER:** This is the report path prefix if you configured one earlier
- **COSTING REPORT NAME:** The name given to your CUR report
- **COSTING KEY:** If the IAM user for this AWS cloud integration does not have access to the S3 bucket with the CUR data, enter the AWS Key ID for an IAM user with access
- **COSTING SECRET:** If the IAM user for this AWS cloud integration does not have access to the S3 bucket with the CUR data, enter the AWS Secret Key for the IAM account whose Key ID you entered in the previous field
- **LINKED ACCOUNT ID:** If the IAM user for this AWS cloud integration does not have access to the S3 bucket with the CUR data, enter the AWS account number that the IAM user from the above step resides in

**Note:** If the AWS cloud account is a GovCloud account, enter the COSTING KEY, COSTING SECRET, and LINKED ACCOUNT ID for the master commercial account your GovCloud account is associated with.
**Costing and AWS GovCloud**

AWS GovCloud delivers Amazon public cloud infrastructure and features in a way that complies with U.S. government standards for security. GovCloud accounts are applied for and must be associated with a pre-existing standard AWS account and the usage and billing data for the GovCloud account is rolled up into that of the standard AWS account. For that reason, Amazon recommends creating a new standard account solely to house the GovCloud account if usage and billing must be tracked separately.

Since GovCloud accounts do not have access to billing data directly, Morpheus must be able to access it through the associated standard account. You could do this by creating the Morpheus cloud integration through the standard account itself or by integrating the GovCloud account and supplying an Access Key and Secret Key for the standard account when configuring costing. When needed, add the additional credentials for the standard commercial account as described below:

1. Add a new AWS Cloud or edit an existing one
2. Expand the Advanced Options section
3. Complete the following fields in addition to other required fields needed to set up costing as described in the previous section:
   - **COSTING KEY**: The AWS Key ID for an IAM user with sufficient access who is associated with the standard commercial account
• **COSTING SECRET:** The AWS Secret Key for an IAM user with sufficient access who is associated with the standard commercial account

• **LINKED ACCOUNT ID:** The AWS account number for the standard commercial account in which the IAM user referenced in the prior bullets resides

4. Save the changes to the AWS Cloud integration

When credentials are configured correctly, you will be able to select an existing Costing and Usage Report (CUR) from the appropriate S3 bucket if it already exists. If not, you can create one directly from the add/edit AWS Cloud modal in Morpheus.

**AWS Reserved Instances and Savings Plans**

Amazon AWS public cloud offers Reserved Instances (RI) and Savings Plans, which allow organizations with consistent use patterns to reduce cloud spend significantly. Morpheus analyzes AWS cloud usage and spend, which allows it to make intelligent recommendations that can lead to significant savings. This data can be reviewed in the Reservation Recommendations and Savings Plan Recommendations tables on any AWS Cloud detail page (Infrastructure > Clouds > Selected Amazon Cloud).

Savings Plans potentially offer greater than 70% savings in exchange for a commitment to consistent usage levels for a 1- or 3-year term. Morpheus provides Savings Plan guidance based on learned analytics; allowing you to analyze Savings Plans based on different term commitments and upfront costs to choose the best savings plan.
Reserved Instances (RI) provide a discounted hourly rate and optional capacity reservation for EC2 instances. AWS billing automatically applies your RI-discounted rate when the attributes of EC2 instance usage match attributes of an active RI. Morpheus provides RI guidance based on learned analytics.

### Reservation Recommendations

<table>
<thead>
<tr>
<th>ITEM</th>
<th>CURRENT USAGE</th>
<th>RECOMMENDATION</th>
<th>TERM COST</th>
</tr>
</thead>
<tbody>
<tr>
<td>SERVICE</td>
<td>TYPE</td>
<td>AVG TOTAL/MONTH</td>
<td>RESERVED</td>
</tr>
<tr>
<td>EC2</td>
<td>T2.NANO</td>
<td>16.9 $71.55</td>
<td>17</td>
</tr>
<tr>
<td>EC2</td>
<td>M4.LARGE</td>
<td>3 $256.23</td>
<td>3</td>
</tr>
<tr>
<td>EC2</td>
<td>T2.NANO</td>
<td>387.97 $1,954.22</td>
<td>346</td>
</tr>
<tr>
<td>EC2</td>
<td>T2.NANO</td>
<td>1.99 $59.87</td>
<td>2</td>
</tr>
<tr>
<td>TOTAL</td>
<td></td>
<td>$2,291.87</td>
<td>50.00</td>
</tr>
</tbody>
</table>

### Minimum AWS IAM Policies

Below are the AWS IAM Permissions covering the minimum access for Morpheus applying to all resources and services.


### Morpheus Sample AWS IAM Policy

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "autoscaling:DescribeAutoScalingGroups",
                "ce:*",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:GetMetricStatistics",
                "ec2:AllocateAddress",
                "ec2:AssignPrivateIpAddresses",
                "ec2:AssociateAddress",
                "ec2:AttachInternetGateway",
                "ec2:AttachNetworkInterface",
                "ec2:AttachVolume",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CancelExportTask",
                "ec2:CancelImportTask",
                "ec2:CopyImage",
                "ec2:CopySnapshot",
                "ec2:CreateEgressOnlyInternetGateway",
                "ec2:CreateImage",
                "ec2:CreateInstanceExportTask",
                "ec2:CreateInternetGateway"
            ]
        }
    ]
}  
(continues on next page)
"ec2:CreateKeyPair",
"ec2:CreateNatGateway",
"ec2:CreateNetworkAcl",
"ec2:CreateNetworkAclEntry",
"ec2:CreateNetworkInterface",
"ec2:CreateSecurityGroup",
"ec2:CreateSnapshot",
"ec2:CreateTags",
"ec2:CreateVolume",
"ec2:DeleteEgressOnlyInternetGateway",
"ec2:DeleteInternetGateway",
"ec2:DeleteKeyPair",
"ec2:DeleteNatGateway",
"ec2:DeleteNetworkAcl",
"ec2:DeleteNetworkAclEntry",
"ec2:DeleteNetworkInterface",
"ec2:DeleteSecurityGroup",
"ec2:DeleteSnapshot",
"ec2:DeleteTags",
"ec2:DeleteVolume",
"ec2:DeregisterImage",
"ec2:DescribeAccountAttributes",
"ec2:DescribeAddresses",
"ec2:DescribeAvailabilityZones",
"ec2:DescribeClassicLinkInstances",
"ec2:DescribeConversionTasks",
"ec2:DescribeEgressOnlyInternetGateways",
"ec2:DescribeExportTasks",
"ec2:DescribeImageAttribute",
"ec2:DescribeImages",
"ec2:DescribeImportImageTasks",
"ec2:DescribeImportSnapshotTasks",
"ec2:DescribeInstances",
"ec2:DescribeInstanceStatus",
"ec2:DescribeInternetGateways",
"ec2:DescribeKeyPairs",
"ec2:DescribeNatGateways",
"ec2:DescribeNetworkAcls",
"ec2:DescribeNetworkInterfaceAttribute",
"ec2:DescribeNetworkInterfaces",
"ec2:DescribeRegions",
"ec2:DescribeSecurityGroupReferences",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSnapshotAttribute",
"ec2:DescribeSnapshots",
"ec2:DescribeStaleSecurityGroups",
"ec2:DescribeSubnets",
"ec2:DescribeTags",
"ec2:DescribeVolumeAttribute",
"ec2:DescribeVolumes",
"ec2:DescribeVolumeStatus",
"ec2:DescribeVpcAttribute",
"ec2:DescribeVpcClassicLink",
"ec2:DescribeVpcClassicLinkDnsSupport",
"ec2:DescribeVpcEndpoints",
"ec2:DescribeVpcEndpointServices",
"ec2:DescribeVpcPeeringConnections",

(continues on next page)
"ec2:DescribeVpcs",
"ec2:DetachInternetGateway",
"ec2:DetachNetworkInterface",
"ec2:DetachVolume",
"ec2:DisassociateAddress",
"ec2:GetPasswordData",
"ec2:ImportImage",
"ec2:ImportInstance",
"ec2:ImportKeyPair",
"ec2:ImportSnapshot",
"ec2:ImportVolume",
"ec2:ModifyImageAttribute",
"ec2:ModifyInstanceAttribute",
"ec2:ModifyNetworkInterfaceAttribute",
"ec2:ModifySnapshotAttribute",
"ec2:ModifyVolumeAttribute",
"ec2:RebootInstances",
"ec2:RegisterImage",
"ec2:ReleaseAddress",
"ec2:ReplaceNetworkAclAssociation",
"ec2:ReplaceNetworkAclEntry",
"ec2:ResetImageAttribute",
"ec2:ResetInstanceAttribute",
"ec2:ResetNetworkInterfaceAttribute",
"ec2:ResetSnapshotAttribute",
"ec2:RevokeSecurityGroupEgress",
"ec2:RevokeSecurityGroupIngress",
"ec2:RunInstances",
"ec2:StartInstances",
"ec2:StopInstances",
"ec2:TerminateInstances",
"ec2:UnassignPrivateIpAddresses",
"ec2:UpdateSecurityGroupRuleDescriptionsEgress",
"eks:*",
"iam:ListGroups",
"iam:ListInstanceProfiles",
"iam:ListRoles",
"rds:AddRoleToDBCluster",
"rds:AddTagsToResource",
"rds:ApplyPendingMaintenanceAction",
"rds:AuthorizeDBSecurityGroupIngress",
"rds:CopyDBClusterSnapshot",
"rds:CopyDBParameterGroup",
"rds:CopyDBSnapshot",
"rds:CreateDBCluster",
"rds:CreateDBClusterSnapshot",
"rds:CreateDBInstance",
"rds:CreateDBInstanceReadReplica",
"rds:CreateDBSecurityGroup",
"rds:CreateDBSnapshot",
"rds:DeleteDBCluster",
"rds:DeleteDBInstance",
"rds:DeleteDBSecurityGroup",
"rds:DeleteDBSnapshot",
"rds:DescribeAccountAttributes",
"rds:DescribeCertificates",
"rds:DescribeDBClusterParameterGroups", 
(continues on next page)
"rds:DescribeDBClusterParameters",
"rds:DescribeDBClusters",
"rds:DescribeDBClusterSnapshotAttributes",
"rds:DescribeDBClusterSnapshots",
"rds:DescribeDBEngineVersions",
"rds:DescribeDBInstances",
"rds:DescribeDBLogFiles",
"rds:DescribeDBParameterGroups",
"rds:DescribeDBParameters",
"rds:DescribeDBSecurityGroups",
"rds:DescribeDBSnapshots",
"rds:DescribeDBSubnetGroups",
"rds:DescribeEngineDefaultClusterParameters",
"rds:DescribeEngineDefaultParameters",
"rds:DescribeEventCategories",
"rds:DescribeEvents",
"rds:DescribeOptionGroupOptions",
"rds:DescribeOptionGroups",
"rds:DescribeOrderableDBInstanceOptions",
"rds:ListTagsForResource",
"rds:ModifyDBCluster",
"rds:ModifyDBClusterParameterGroup",
"rds:ModifyDBClusterSnapshotAttribute",
"rds:ModifyDBInstance",
"rds:ModifyDBParameterGroup",
"rds:ModifyDBSnapshotAttribute",
"rds:PromoteReadReplica",
"rds:RebootDBInstance",
"rds:RemoveTagsFromResource",
"rds:RestoreDBClusterFromSnapshot",
"rds:RestoreDBClusterToPointInTime",
"rds:RestoreDBInstanceFromDBSnapshot",
"rds:RestoreDBInstanceToPointInTime",
"rds:RevokeDBSecurityGroupIngress",
"route53:GetHostedZone",
"route53:ListHostedZones",
"route53:ListResourceRecordSets",
"s3:AbortMultipartUpload",
"s3:CreateBucket",
"s3:DeleteBucket",
"s3:DeleteObject",
"s3:DeleteObjectVersion",
"s3:GetBucketLocation",
"s3:GetObject",
"s3:GetObjectVersion",
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:ListBucketMultipartUploads",
"s3:ListBucketVersions",
"s3:ListMultipartUploadParts",
"s3:PutObject"
],
"Resource": "+"
Resource Filter

If you need to limit actions based on filters you have to pull out the action and put it in a resource based policy since not all the actions support resource filters.


Resource filter example:

```json
{
    "Effect": "Allow",
    "Action": [
        "ec2:StopInstances",
        "ec2:StartInstances"
    ],
    "Resource": *
},
{
    "Effect": "Allow",
    "Action": "ec2:TerminateInstances",
    "Resource": "arn:aws:ec2:us-east-1:123456789012:instance/*",
    "Condition": {
        "StringEquals": {
            "ec2:ResourceTag/purpose": "test"
        }
    }
}
```

12.12.2 Azure (Public)

Overview

Morpheus offers a complete Integration with Microsoft Azure including the following:

- Virtual Machine Sync, Create, Delete, Manage, RBAC, Tenant Permissions, Policies
- Resource Group Sync, Create, Delete, RBAC, Tenant Permissions
- Network Sync, Create, Delete, RBAC, Tenant Permissions
- Subnet Sync, Create, Delete, RBAC, Tenant Permissions
- Security Group Sync, Create, Delete, Tenant Permissions
- Security Group Rule Sync, Create, Delete, Tenant Permissions
- ARM Blueprints, Spec Templates, Deployment Logs Sync, Git/GitHub Integration
- MSSQL Service Sync, Create, Delete, Manage, RBAC, Tenant Permissions
- AKS Sync, Sync, Create, Delete, Manage, RBAC, Tenant Permissions
- Backup Create, Delete, Manage, RBAC, Policies
- Storage Sync, Create, Delete, Manage, Browse, RBAC, Tenant Permissions, Policies
- Marketplace Sync
- Private Image Sync & Upload
- Azure Marketplace Custom Library Item Support
• Remote Console (SSH & RDP)
• Lifecycle Management
• Availability Set Support
• Scale Set Sync, Create, Assign, Manage, Delete
• Azure Load Balancer Create, Assign, Manage, Delete, RBAC, Tenant Permissions
• Docker (VM) Cluster Sync, Create, Delete, Manage, RBAC, Tenant Permissions
• Kubernetes (VM) Cluster Sync, Create, Delete, Manage, RBAC, Tenant Permissions
• Service Plan Sync, Tenant Permissions, RBAC
• Pricing Sync RBAC, Tenant Permissions, Markup
• Costing Sync, Reporting, Invoicing
• Reservations Sync, Guidance Recommendations
• Azure Stack Support
• Tag Bi-Directional Sync, Creation, Deletion Policy Enforcement
• Cost Estimator
• Azure US Gov Support
• Azure China Support
• Azure Germany Support
• CSP Account Support

Requirements

Morpheus Azure Integration requires Owner or Contributor access to subscription via App Registration. Adding an Azure Cloud or Clouds to Morpheus will require the following:

• Azure Subscription ID
• Directory (tenant) ID
• Application (client) ID
• Application (client) Secret
• Application (client) must be Owner or Contributor of Subscription

CSP Accounts require the additional following input:

• CSP Directory (tenant) ID
• CSP Application (client) ID
• CSP Application (client) SECRET
Credentials & Permissions

Morpheus authenticates with Azure via an App Registration with an Owner or Contributor Role on a Subscription. Use the steps below to create and collect the required credentials and assign the required permissions to integrate Azure with Morpheus.

**Warning:** Using an App Registration (service principal) that has selective resource permissions and is not an Owner or Contributor of the Subscription is not supported and will cause failures/issues. Please confirm the App Registration you use to integrate Azure with Morpheus has Owner or Contributor permissions on the specified Subscription before contacting support.

Create an App Registration

If you do not have an existing Azure Active Directory App Registration, or you wish to use an new one for Morpheus, you will need to create one.

1. Log into the Azure portal
2. Select “Azure Active Directory”
3. Select “App Registrations”
4. Select “New Registration”
5. Next, give app a name, specify Web app / API for the type (default) and enter any url for the Sign-on URL:
6. Click Create and your new App Registration will be created.
Now that we have (or already had) our App Registration, we will gather the credentials required for the Morpheus Azure integration.

**Copy Directory (tenant) and Application (client) IDs**

The App Registration Directory (tenant) and Application (client) ID are required for the Morpheus Azure integration. Both can be found in the overview section of the App Registration.

1. Go to the Overview section of your App Registration
2. Copy the Directory (tenant) ID
3. Store/Paste for use as the Tenant ID when Adding your Azure cloud in Morpheus
4. Copy the Application (client) ID
5. Store/Paste for use as the Client ID when Adding your Azure cloud in Morpheus
Generate a Client Secret

While still in your App Registration:

1. Select Certificates & secrets in the Manage Section
2. Select + New client secret
3. The “Add a client secret” modal will come up
4. Add a description to help identify the secret in the future
5. Select a duration
6. Select Add

7. Copy the newly generated Client Secret Value. It is important to copy the Client Secret Value now as it will not be displayed/available

**Important:** Copy the key value before continuing as it will not be displayed/available again.

8. Store/Paste for use as the Client Secret when Adding your Azure cloud in Morpheus

You now have 3 or the 4 credentials required for Morpheus Azure cloud integration. The last credential required is the Azure Subscription ID.
Subscription ID

To get the Azure Subscription ID:

1. Navigate to the main Subscriptions section. One way is to search for “Subscriptions” and select Subscriptions in the search results

2. In the main “Subscriptions” section, copy the Subscription ID

3. Store/Paste for use as the Subscription ID when Adding your Azure cloud in Morpheus
Make App Registration owner or contributor of Subscription

The App Registration created/used needs to be an owner of the Azure Subscription used for the Morpheus cloud integration. If lesser permissions are given or permissions are assigned at individual resource levels, Morpheus will not be able to properly inventory/sync, create and/or remove resources.

1. In the main “Subscriptions” section in Azure, select the Subscription
2. In the Subscription pane, select “Access Control (IAM)”
3. Either Click “+ Add”, and the “Add Role Assignment”, or simply select “Add a role assignment”
4. In the right pane, select “Owner” or “Contributor” Role type
5. Search for the name of the App Registration used for the Morpheus integration
6. Select the App Registration in the search results
7. Select “Save”
You now have the required Credentials and permissions to add an Azure Cloud Integration(s) into Morpheus.

**Add an Azure Cloud Integration**

To add a new Azure Cloud integration into Morpheus using the credentials created/collected from the previous section, perform the following:

1. In Morpheus, navigate to **Infrastructure > Clouds** and select **+ ADD**

2. Select “AZURE (PUBLIC)” from the Cloud Types list and click **NEXT**
3. Populate the Following Cloud Configuration

**NAME**  Name of the Cloud in Morpheus

**CODE**  Unique code used for api/cli, automation and policies.

**LOCATION**  Description field for adding notes on the cloud, such as location.

**VISIBILITY**  For setting cloud permissions in a multi-tenant environment. Not applicable in single tenant environments.

**TENANT**  If Visibility is set to Private, select the Tenant the Cloud resources will assigned to.

**ENABLED**  When disabled, automatic Cloud sync is paused and the Cloud will not be selectable for provision-
AUTOMATICALLY POWER ON VMS  When enabled, Morpheus will maintain the expected power state of managed VMs. Morpheus will power on any managed VMs in the Cloud that have been shut down for unknown reasons (not powered off by Morpheus) to ensure availability of services.

**Note:** When “AUTOMATICALLY POWER ON VMS” is enabled, the power state of managed VMs should be maintained in Morpheus. This setting is not applicable to discovered/unmanaged resources.

**Details**

**CLOUD TYPE**
- Standard (Azure Cloud)
- US Gov (Azure US Government)
- German (Azure German Cloud)
- China (Azure China Cloud)

**SUBSCRIPTION ID**  The target Azure Subscription ID obtained from the previous section

**TENANT ID**  The Directory (tenant) ID obtained from the previous section

**CLIENT ID**  The Application (client) ID obtained from the previous section

**CLIENT SECRET**  The Application (client) Secret obtained from the previous section

**LOCATION**  Once valid credentials are populate above and Morpheus is able to successfully authenticate with Azure, the available locations/regions will populate.

**RESOURCE GROUP**
- Select “All” to scope the Cloud to all available Resource Groups in the specified location/region.
- Select a single Resource Group to limit Morpheus resource creation, selection and discovery to just this Resource Group.

**INVENTORY EXISTING INSTANCES**  Check to enable discovery/inventory of existing VM's in the scoped Region and Resource Group(s)

**INVENTORY LEVEL**
- **Basic**  Morpheus will sync information on all resources in the selected Resource Group(s), including Name, IP Addresses, Platform Type, Power Status, and overall resources sizing for Storage, CPU and RAM, every 5 minutes. Inventoried VM’s will appear as Unmanaged VM’s.
- **Full (API Heavy)**  In addition to the information synced from Basic Inventory level, Morpheus will gather Resource Utilization metrics for Memory, Storage and CPU utilization per VM when available.
- **Off**  Existing VM’s will not be inventoried

**ACCOUNT TYPE**  Standard, EA or CSP

**Note:**  For CSP Accounts, also enter CSP TENANT ID, CSP CLIENT ID and CSP CLIENT SECRET in the Advanced Options section. In order to enable cost sync for CSP accounts, the “CSP CUSTOMER” checkbox must be marked and “COSTING” should be set to “Costing” rather than “Costing and Reservations”.
### CREATE CLOUD

- **NAME**: newAzureCloud
- **CODE**: codeIsUsefulForPoliciesAndAPI
- **LOCATION**: West Central US

#### Details

- **CLOUD TYPE**: Global
- **SUBSCRIPTION ID**: eccf-b998
- **TENANT ID**: c99-0686
- **CLIENT ID**: db7-13f
- **CLIENT SECRET**: Password123
- **LOCATION**: West Central US
- **RESOURCE GROUP**: All

- **INVENTORY EXISTING INSTANCES**
- **INVENTORY LEVEL**: Full (API Heavy)
- **ACCOUNT TYPE**: Standard

- **Advanced Options**
- **Provisioning Command**
Advanced Options

**DOMAIN**  Specify a default domain for instances provisioned to this Cloud.

**SCALE PRIORITY**  Only affects Docker Provisioning. Specifies the priority with which an instance will scale into the cloud. A lower priority number means this cloud integration will take scale precedence over other cloud integrations in the group.

**APPLIANCE URL**  Alternate Appliance url for scenarios when the default Appliance URL (configured in admin > settings) is not reachable or resolvable for Instances provisioned in this cloud. The Appliance URL is used for Agent install and reporting.

**TIME ZONE**  Configures the time zone on provisioned VM’s if necessary.

**DATACENTER ID**  Used for differentiating pricing among multiple datacenters. Leave blank unless prices are properly configured.

**NETWORK MODE**  Unmanaged or select a Network Integration (NSX, ACI etc)

**LOCAL FIREWALL**  On or Off. Enable to managed Host and VM firewall/IP Table rules (linux only)

**SECURITY SERVER**  Security Server setting is for Security Service Integrations such as ACI

**TRUST PROVIDER**  Select Internal (Morpheus) or an existing Trust Provider Integration

**STORAGE MODE**  Single Disk, LVM or Clustered

**BACKUP PROVIDER**  Select Internal Backups (Morpheus) or a Backup Integration

**REPLICATION PROVIDER**  Sets the default Replication Provider for the Cloud. Select an existing Replication Provider Integration

**GUIDANCE**  Enable Guidance recommendations on cloud resources.

**COSTING**  Enable for Morpheus to sync Costing data from the Cloud provider, when available. For on-prem Clouds, enabling costing activates a costing service designed to mirror the live costing experience of public clouds, including invoicing with line items and real-time cost data (Operations > Costing > Invoices). If your organization utilizes reserved instances and you want to pull in related pricing data, select Costing and Reservations. If this is not relevant, select Costing to save money on additional calls to the AWS Cost Explorer API or similar service for other clouds.

**DNS INTEGRATION**  Records for instances provisioned in this cloud will be added to selected DNS integration.

**SERVICE REGISTRY**  Services for instances provisioned in this cloud will be added to selected Service Registry integration.

**CONFIG MANAGEMENT**  Select a Chef, Salt, Ansible or Puppet integration to be used with this Cloud.

**CMDB**  Select CMDB Integration to automatically update selected CMDB.

**CMDB DISCOVERY**  When checked, any automatically discovered (unmanaged) servers onboarded into Morpheus from this Cloud will also have CMDB records created for them.

**CHANGE MANAGEMENT**  Select an existing Change Management Integration to set on the Cloud. ex: Cherwell

**AGENT INSTALL MODE**

- SSH / WINRM: Morpheus will use SSH or WINRM for Agent install.
- Cloud Init / Unattend (when available): (DEFAULT) Morpheus will utilize Cloud-Init or Cloudbase-Init for agent install when provisioning images with Cloud-Init/Cloudbase-Init installed. Morpheus will fall back on SSH or WINRM if cloud-init is not installed on the provisioned image. Morpheus
will also add Agent installation to Windows unattend.xml data when performing Guest Customizations or utilizing syspreped images.

**API PROXY**  Set a proxy for outbound communication from the Morpheus Appliance to the Cloud endpoints. Proxies can be added in the *Infrastructure > Networks > Proxies* tab.

**INSTALL AGENT**  Enable to have Agent Installation on by default for all provisioning into this Cloud. Disable for Agent Installation to be off by default for all provisioning into this Cloud.

**Provisioning Options**

**PROXY**  Set a proxy for inbound communication from Instances to the Morpheus Appliance. Proxies can be added in the *Infrastructure > Networks > Proxies* tab.

**Bypass Proxy for Appliance URL**  Enable to bypass proxy settings (if added) for Morpheus Agent communication to the Appliance URL.

**NO PROXY**  Include a list of IP addresses or name servers to exclude from proxy traversal.


4. Once done configuring the Cloud, select *NEXT*. NOTE all specified values except the Subscription ID can be changes after the Cloud is created.

5. Next select an existing Group to add the Azure Cloud to, or create a new Group, then select *NEXT*
6. Review the configuration and then select *COMPLETE*

Your new Azure Cloud integration will be created and begin to sync.

**Note:** The initial sync of an Azure Cloud can take some time due to Marketplace data sync.
12.12.3 Azure Stack

Overview

Azure Stack is Microsoft’s Azure Cloud for on-premises environments. Azure Stack contains the core Azure services, allowing organizations to take advantage of Azure’s offerings with the security, compliance, and financial benefits of hosting it in their own data-centers.

- Virtual Machine Provisioning
- Backups / Snapshots
- Resource Group Sync & Selection
- Network Sync & Selection
- Security Group Sync & Selection
- Storage Account Sync & Selection
- Marketplace Search and Provisioning
- Remote Console
- Periodic Synchronization
- Lifecycle Management and Resize
- Availability Set Support
- Azure Load Balancers
- Azure Storage
Morpheus Documentation

- Docker Host Provisioning & Management
- Service Plan Sync
- Pricing Sync with markup options
- Cost Estimator

Combine these features with public Azure and Morpheus can provide a single pane of glass and self service portal for managing instances scattered across both Azure offerings.

Requirements

Azure Stack Accessibility

By default, the Azure Stack management url’s are not accessible from an external network. Port mappings and DNS must be configured for communication between the Morpheus Appliance and Azure Stack.

Important: In order to communicate with Azure Stack, Morpheus must be able to reach the internal Azure Stack network. The Azure Stack Portal needs to be exposed to the Morpheus Appliances’ network with corresponding entries added to DNS.

One option to expose the Internal Azure Stack network to the Morpheus Appliances network is to use the Expose-AzureStackPortal.ps1 powershell script from https://gallery.technet.microsoft.com/scriptcenter/Expose-the-Azure-Stack-7ef68b19. An Azure Stack Port Mapping Tool is also available.

Below is a sample output from the script for reference:

```
[Admin Portal] Created port mappings on 10.30.23.120 to 192.168.102.8
[Admin Portal] Ports: 13011 30015 13001 13010 13020 443 13003 12646 12647 12648
   12649 12650 12495 13026 12499
[Admin Portal] DNS: 10.30.23.120 - adminportal.local.azurestack.external
   --adminmanagement.local.azurestack.external

[Tenant Portal] Created port mappings on 10.30.23.121 to 192.168.102.10
[ Tenant Portal] Ports: 13011 30015 13001 13010 13020 443 13003 12646 12647
   12648 12649 12650 12495 13026 12499
   --azurestack.external

[Blob Storage] Created port mappings on 10.30.23.122 to 192.168.102.4
[Blob Storage] Ports: 80 443

VERBOSE: DNS delegation/forwarding is optional, change the DNS records on MAS-DC01 manually (dnsmgmt.msc from Host).
[DNS Delegation] Created port mappings on 10.30.23.120 to 192.168.200.224
[DNS Delegation] Ports: 53 (TCP/UDP)
[DNS Delegation] DNS: local.azurestack.external NS 10.30.23.120
[DNS Delegation] Change records on MAS-DC01 manually ‘if’ you plan to use DNS forwarding.
[DNS Delegation] Change records back to the original internal IPs before running this script again.

VERBOSE: App Service detected and external IPs specified, creating mappings.
[App Service API] Created port mappings on 10.30.23.123 to 192.168.102.17
```
Azure Stack Resources

The following resources need to be created and configured inside Azure Stack for successful provisioning:

- Resource Group(s)
- Virtual Network(s)
- Storage Account(s)
- Network Security Group(s)
  - Inbound ports open from Morpheus Appliance: 22, 5985, 3389
  - Outbound ports open to Morpheus Appliance: 80, 443

**Note:** Proper Network and Network Security Group configuration is required for Morpheus agent install, communication, and remote console access. Other configurations, such as docker instances, will need the appropriate ports opened as well.

Required Credentials & Permissions

Credentials to integrate Morpheus with Azure Stack are located in both the public Azure Portal and the Private Azure Stack Portal. The Azure Active Directory Application used must be an owner of the Azure Stack subscription.

**Azure Portal:**

- Azure Active Directory Application Credentials
- Directory ID
- Management URL
- Identity Resource URL
- Application ID
- Key Value

**Azure Stack Portal:**

- Azure Stack Subscription ID
- Active Directory App from Azure portal added as owner of the Azure Stack Subscription in Azure Stack.
Adding an Azure Stack Cloud

Configure

1. In the Morpheus UI, navigate to **Infrastructure > Clouds** and Select + **CREATE CLOUD**

2. Select **AZURE STACK (PRIVATE)** from the Clouds list and select **NEXT**

3. In the Configure section, enter:

   **Cloud Configuration**

   NAME   Name of the Cloud in Morpheus

   CODE   Unique code used for api/cli, automation and policies.

   LOCATION Description field for adding notes on the cloud, such as location.

   VISIBILITY For setting cloud permissions in a multi-tenant environment. Not applicable in single tenant environments.

   TENANT If Visibility is set to Private, select the Tenant the Cloud resources will assigned to.

   ENABLED When disabled, automatic Cloud sync is paused and the Cloud will not be selectable for provisioning.

   AUTOMATICALLY POWER ON VMS When enabled, Morpheus will maintain the expected power state of managed VMs. Morpheus will power on any managed VMs in the Cloud that have been shut down for unknown reasons (not powered off by Morpheus) to ensure availability of services.

   

   **Note:** When “AUTOMATICALLY POWER ON VMS” is enabled, the power state of managed VMs should be maintained in Morpheus. This setting is not applicable to discovered/unmanaged resources.

   **Details**

   IDENTIT Y URL  https://login.microsoftonline.com

   MANAGEMENT URL* Azure AD Azure Stack Administrator app or Microsoft Azure Stack Administrator app url. Example: https://adminmanagement.local.azurestack.external/

   IDENTIT Y RESOURCE URL Azure AD Azure Stack Administrator App ID URI Example: https://adminmanagement.xxxxx.onmicrosoft.com/4a80e607-4259-4ac6-83e2-2fabeaf2eh83

   BASE DOMAIN This should match the base domain in your Management url. Example: local.azurestack.external

   SUBSCRIPTION ID Subscription ID from Azure Stack portal (this is different from the Subscription ID in you Azure portal used when configuring Azure Stack)

   TENANT ID This is the Directory ID from the Azure AD directory

   CLIENT ID Application ID of Azure AD app with Azure Stack permissions granted, and has been added as an owner of the Azure Stack subscription (in the Azure Stack portal).

   CLIENT SECRET Key Value of Application ID used above

   **Note:** Once all credentials are entered and validated, the Location and Resource Group fields will populate.

   **Location** Select an Azure Stack region for the cloud to scope to. This typically will be “local”.
**Resource Group**  Select All or a single Resource Group to scope the cloud to. Selecting a single Resource Group will only sync resources in that Resource Group and disable Resource Group selection during provisioning. All will sync all resources and allow specifying the Resource Group during provisioning.

**Inventory Existing Instances** If enabled, existing Virtual Machines will be inventoried and appear as unmanaged Virtual Machines in Morpheus.

4. The Azure Stack cloud is ready to be added to a group and saved. Additional configuration options available:

**Note:** All fields and options can be edited after the Cloud is created.

### Advanced Options

**DOMAIN** Specify a default domain for instances provisioned to this Cloud.

**SCALE PRIORITY** Only affects Docker Provisioning. Specifies the priority with which an instance will scale into the cloud. A lower priority number means this cloud integration will take scale precedence over other cloud integrations in the group.

**APPLIANCE URL** Alternate Appliance url for scenarios when the default Appliance URL (configured in `admin > settings`) is not reachable or resolvable for Instances provisioned in this cloud. The Appliance URL is used for Agent install and reporting.

**TIME ZONE** Configures the time zone on provisioned VM’s if necessary.

**DATACENTER ID** Used for differentiating pricing among multiple datacenters. Leave blank unless prices are properly configured.

**NETWORK MODE** Unmanaged or select a Network Integration (NSX, ACI etc)

**LOCAL FIREWALL** On or Off. Enable to managed Host and VM firewall/IP Table rules (linux only)

**SECURITY SERVER** Security Server setting is for Security Service Integrations such as ACI

**TRUST PROVIDER** Select Internal (Morpheus) or an existing Trust Provider Integration

**STORAGE MODE** Single Disk, LVM or Clustered

**BACKUP PROVIDER** Select Internal Backups (Morpheus) or a Backup Integration

**REPLICATION PROVIDER** Sets the default Replication Provider for the Cloud. Select an existing Replication Provider Integration

**GUIDANCE** Enable Guidance recommendations on cloud resources.

**COSTING** Enable for Morpheus to sync Costing data from the Cloud provider, when available. For on-prem Clouds, enabling costing activates a costing service designed to mirror the live costing experience of public clouds, including invoicing with line items and real-time cost data (Operations > Costing > Invoices). If your organization utilizes reserved instances and you want to pull in related pricing data, select Costing and Reservations. If this is not relevant, select Costing to save money on additional calls to the AWS Cost Explorer API or similar service for other clouds.

**DNS INTEGRATION** Records for instances provisioned in this cloud will be added to selected DNS integration.

**SERVICE REGISTRY** Services for instances provisioned in this cloud will be added to selected Service Registry integration.

**CONFIG MANAGEMENT** Select a Chef, Salt, Ansible or Puppet integration to be used with this Cloud.

**CMDB** Select CMDB Integration to automatically update selected CMDB.
CMDB DISCOVERY When checked, any automatically discovered (unmanaged) servers onboarded into Morpheus from this Cloud will also have CMDB records created for them.

CHANGE MANAGEMENT Select an existing Change Management Integration to set on the Cloud. ex: Cherwell

AGENT INSTALL MODE
- SSH / WINRM: Morpheus will use SSH or WINRM for Agent install.
- Cloud Init / Unattend (when available): (DEFAULT) Morpheus will utilize Cloud-Init or Cloudbase-Init for agent install when provisioning images with Cloud-Init/Cloudbase-Init installed. Morpheus will fall back on SSH or WINRM if cloud-init is not installed on the provisioned image. Morpheus will also add Agent installation to Windows unattend.xml data when performing Guest Customizations or utilizing syspreped images.

API PROXY Set a proxy for outbound communication from the Morpheus Appliance to the Cloud endpoints. Proxies can be added in the Infrastructure > Networks > Proxies tab.

INSTALL AGENT Enable to have Agent Installation on by default for all provisioning into this Cloud. Disable for Agent Installation to be off by default for all provisioning into this Cloud.

Provisioning Options

PROXY Set a proxy for inbound communication from Instances to the Morpheus Appliance. Proxies can be added in the Infrastructure > Networks > Proxies tab.

Bypass Proxy for Appliance URL Enable to bypass proxy settings (if added) for Morpheus Agent communication to the Appliance URL.

NO PROXY Include a list of IP addresses or name servers to exclude from proxy traversal


5. Once all options are configured, select NEXT to add the cloud to a Group.

GROUP A Group must be specified or created for the new Cloud to be added to. Clouds can be added to additional Groups or removed from Groups after being created.

USE EXISTING Add the new Cloud to an exiting Group in Morpheus.

CREATE NEW Creates a new Group in Morpheus and adds the Cloud to the Group.

6. Confirm all settings are correct and select COMPLETE. The Azure Stack Cloud will be added, and Morpheus will perform the initial cloud sync of:
- Virtual Machines (if Inventory Existing Instances is enabled)
- Networks
- Virtual Images/Blueprints
- Network Security Groups
- Storage Accounts
- Marketplace Catalog
- Availability Sets

Tip: Synced Networks can be configured or deactivated from the Networks section in this Clouds detail page, or in the Infrastructure > Networks section.
12.12.4 Cloud Foundry

Configuration

Adding PCF Cloud From Infrastructure > Clouds

1. Navigate to Infrastructure > Clouds
2. Select + ADD
3. Select CLOUD FOUNDRY from the Clouds list
4. Select NEXT
5. Populate the following:

   Cloud Configuration

   NAME Name of the Cloud in Morpheus
   CODE Unique code used for api/cli, automation and policies.
   LOCATION Description field for adding notes on the cloud, such as location.
   VISIBILITY For setting cloud permissions in a multi-tenant environment. Not applicable in single tenant environments.
   TENANT If Visibility is set to Private, select the Tenant the Cloud resources will assigned to.
   ENABLED When disabled, automatic Cloud sync is paused and the Cloud will not be selectable for provisioning.

   AUTOMATICALLY POWER ON VMS When enabled, Morpheus will maintain the expected power state of managed VMs. Morpheus will power on any managed VMs in the Cloud that have been shut down for unknown reasons (not powered off by Morpheus) to ensure availability of services.

   Note: When “AUTOMATICALLY POWER ON VMS” is enabled, the power state of managed VMs should be maintained in Morpheus. This setting is not applicable to discovered/unmanaged resources.

Details

API URL Cloud Foundry API Url
CLIENT ID Typically cf
CLIENT SECRET Typically blank
USERNAME Enter Username. If using an API Key, enter apikey for username, and the API Key as the password.
PASSWORD Enter Password. If using an API Key, the API Key as the password.
ORGANIZATION Select Organization. Dropdown populates upon successful authorization.

Advanced Options

DOMAIN Specify a default domain for instances provisioned to this Cloud.

SCALE PRIORITY Only affects Docker Provisioning. Specifies the priority with which an instance will scale into the cloud. A lower priority number means this cloud integration will take scale precedence over other cloud integrations in the group.
**APPLIANCE URL** Alternate Appliance url for scenarios when the default Appliance URL (configured in `admin > settings`) is not reachable or resolvable for Instances provisioned in this cloud. The Appliance URL is used for Agent install and reporting.

**TIME ZONE** Configures the time zone on provisioned VM’s if necessary.

**DATACENTER ID** Used for differentiating pricing among multiple datacenters. Leave blank unless prices are properly configured.

**NETWORK MODE** Unmanaged or select a Network Integration (NSX, ACI etc)

**LOCAL FIREWALL** On or Off. Enable to managed Host and VM firewall/IP Table rules (linux only)

**SECURITY SERVER** Security Server setting is for Security Service Integrations such as ACI

**TRUST PROVIDER** Select Internal (Morpheus) or an existing Trust Provider Integration

**STORAGE MODE** Single Disk, LVM or Clustered

**BACKUP PROVIDER** Select Internal Backups (Morpheus) or a Backup Integration

**REPLICATION PROVIDER** Sets the default Replication Provider for the Cloud. Select an existing Replication Provider Integration

**GUIDANCE** Enable Guidance recommendations on cloud resources.

**COSTING** Enable for Morpheus to sync Costing data from the Cloud provider, when available. For on-prem Clouds, enabling costing activates a costing service designed to mirror the live costing experience of public clouds, including invoicing with line items and real-time cost data (Operations > Costing > Invoices). If your organization utilizes reserved instances and you want to pull in related pricing data, select Costing and Reservations. If this is not relevant, select Costing to save money on additional calls to the AWS Cost Explorer API or similar service for other clouds.

**DNS INTEGRATION** Records for instances provisioned in this cloud will be added to selected DNS integration.

**SERVICE REGISTRY** Services for instances provisioned in this cloud will be added to selected Service Registry integration.

**CONFIG MANAGEMENT** Select a Chef, Salt, Ansible or Puppet integration to be used with this Cloud.

**CMDB** Select CMDB Integration to automatically update selected CMDB.

**CMDB DISCOVERY** When checked, any automatically discovered (unmanaged) servers onboarded into Morpheus from this Cloud will also have CMDB records created for them.

**CHANGE MANAGEMENT** Select an existing Change Management Integration to set on the Cloud. ex: Cherwell

**AGENT INSTALL MODE**

- SSH / WINRM: Morpheus will use SSH or WINRM for Agent install.
- Cloud Init / Unattend (when available): (DEFAULT) Morpheus will utilize Cloud-Init or Cloudbase-Init for agent install when provisioning images with Cloud-Init/Cloudbase-Init installed. Morpheus will fall back on SSH or WINRM if cloud-init is not installed on the provisioned image. Morpheus will also add Agent installation to Windows unattend.xml data when performing Guest Customizations or utilizing sysprepped images.

**API PROXY** Set a proxy for outbound communication from the Morpheus Appliance to the Cloud endpoints. Proxies can be added in the `Infrastructure > Networks > Proxies` tab.

**INSTALL AGENT** Enable to have Agent Installation on by default for all provisioning into this Cloud. Disable for Agent Installation to be off by default for all provisioning into this Cloud.
Provisioning Options

**PROXY** Set a proxy for inbound communication from Instances to the Morpheus Appliance. Proxies can be added in the *Infrastructure > Networks > Proxies* tab.

**Bypass Proxy for Appliance URL** Enable to bypass proxy settings (if added) for Morpheus Agent communication to the Appliance URL.

**NO PROXY** Include a list of IP addresses or name servers to exclude from proxy traversal


6. Select NEXT

7. Select an existing or create a new Group to add the Cloud to. The Cloud can be added to additional Groups in a Groups Clouds tab.

8. Select NEXT

9. Review and then Select COMPLETE

Adding PCF Cloud From *Infrastructure > Groups*

1. Navigate to *Infrastructure > Groups*
2. Select a Group
3. Select the CLOUDS tab
4. Scroll down to CLOUD FOUNDRY and select + ADD
5. Populate the following:
   - **Name** Name of the Cloud in Morpheus
   - **Location** Description field for adding notes on the cloud, such as location.
   - **Visibility** For setting cloud permissions in a multi-tenant environment. Not applicable in single tenant environments.
   - **TENANT** Select a Tenant if Visibility is set to Private to assign to Cloud to that Tenant. Multiple Tenants can be added by editing the cloud after creation.
   - **API URL** Cloud Foundry API Url. Example https://api.cf.morpheusdata.com
   - **CLIENT ID** Typically cf
   - **CLIENT SECRET** Typically blank
   - **USERNAME** Enter Username. If using an API Key, enter apikey for username, and the API Key as the password.
   - **PASSWORD** Enter Password. If using an API Key, the API Key as the password.
   - **ORGANIZATION** Select Organization. Dropdown populates upon successful authorization.

Advanced Options

- **DOMAIN** Specify a default domain for instances provisioned to this Cloud.
- **SCALE PRIORITY** Only affects Docker Provisioning. Specifies the priority with which an instance will scale into the cloud. A lower priority number means this cloud integration will take scale precedence over other cloud integrations in the group.

12.12. Clouds 777
**APPLIANCE URL**  Alternate Appliance url for scenarios when the default Appliance URL (configured in `admin > settings`) is not reachable or resolvable for Instances provisioned in this cloud. The Appliance URL is used for Agent install and reporting.

**TIME ZONE**  Configures the time zone on provisioned VM’s if necessary.

**DATACENTER ID**  Used for differentiating pricing among multiple datacenters. Leave blank unless prices are properly configured.

**NETWORK MODE**  Unmanaged or select a Network Integration (NSX, ACI etc)

**LOCAL FIREWALL**  On or Off. Enable to managed Host and VM firewall/IP Table rules (linux only)

**SECURITY SERVER**  Security Server setting is for Security Service Integrations such as ACI

**TRUST PROVIDER**  Select Internal (Morpheus) or an existing Trust Provider Integration

**STORAGE MODE**  Single Disk, LVM or Clustered

**BACKUP PROVIDER**  Select Internal Backups (Morpheus) or a Backup Integration

**REPLICATION PROVIDER**  Sets the default Replication Provider for the Cloud. Select an existing Replication Provider Integration

**GUIDANCE**  Enable Guidance recommendations on cloud resources.

**COSTING**  Enable for Morpheus to sync Costing data from the Cloud provider, when available. For on-prem Clouds, enabling costing activates a costing service designed to mirror the live costing experience of public clouds, including invoicing with line items and real-time cost data (Operations > Costing > Invoices). If your organization utilizes reserved instances and you want to pull in related pricing data, select Costing and Reservations. If this is not relevant, select Costing to save money on additional calls to the AWS Cost Explorer API or similar service for other clouds.

**DNS INTEGRATION**  Records for instances provisioned in this cloud will be added to selected DNS integration.

**SERVICE REGISTRY**  Services for instances provisioned in this cloud will be added to selected Service Registry integration.

**CONFIG MANAGEMENT**  Select a Chef, Salt, Ansible or Puppet integration to be used with this Cloud.

**CMDB**  Select CMDB Integration to automatically update selected CMDB.

**CMDB DISCOVERY**  When checked, any automatically discovered (unmanaged) servers onboarded into Morpheus from this Cloud will also have CMDB records created for them.

**CHANGE MANAGEMENT**  Select an existing Change Management Integration to set on the Cloud. ex: Cherwell

**AGENT INSTALL MODE**

- SSH / WINRM: Morpheus will use SSH or WINRM for Agent install.
- Cloud Init / Unattend (when available): (DEFAULT) Morpheus will utilize Cloud-Init or Cloudbase-Init for agent install when provisioning images with Cloud-Init/Cloudbase-Init installed. Morpheus will fall back on SSH or WINRM if cloud-init is not installed on the provisioned image. Morpheus will also add Agent installation to Windows unattend.xml data when performing Guest Customizations or utilizing sysprep-ed images.

**API PROXY**  Set a proxy for outbound communication from the Morpheus Appliance to the Cloud endpoints. Proxies can be added in the `Infrastructure > Networks > Proxies` tab.

**INSTALL AGENT**  Enable to have Agent Installation on by default for all provisioning into this Cloud. Disable for Agent Installation to be off by default for all provisioning into this Cloud.
Provisioning Options

**PROXY** Set a proxy for inbound communication from Instances to the Morpheus Appliance. Proxies can be added in the Infrastructure > Networks > Proxies tab.

**Bypass Proxy for Appliance URL** Enable to bypass proxy settings (if added) for Morpheus Agent communication to the Appliance URL.

**NO PROXY** Include a list of IP addresses or name servers to exclude from proxy traversal

**USER DATA (LINUX)** Add cloud-init user data. Morpheus 4.1.0 and earlier assumes bash syntax. Morpheus 4.1.1 and later supports all User Data formats. Refer to [https://cloudinit.readthedocs.io/en/latest/topics/format.html](https://cloudinit.readthedocs.io/en/latest/topics/format.html) for more information.

6. Select **NEXT**

7. Review and then Select **COMPLETE**

Adding Spaces

Cloud Foundry Spaces are referred to as Resource Pools in Morpheus. You can add a new Space by:

1. Navigating to the Cloud and selecting the Resources tab.
3. Give the Resource a Name
4. Expand the Managers, Developers, and Auditors section to add specific Cloud Foundry users to the roles. When adding a user to these sections, use their Cloud Foundry email addresses.

Provisioning

Morpheus automatically seeds MySQL, Redis and RabbitMQ PCF Instance Types, as well as a generic Cloud Foundry Instance Type that will create a shell app used in conjunction with deployments. PCF Marketplace items can also be added to the Provisioning Library in the Cloud detail view Marketplace tab. The Marketplace item will be added to the selected Instance Type and available when selecting the Cloud Foundry Cloud during Instance or App Template creation.

Deployments

The Cloud Foundry App Instance Type is used in conjunction with deployments. Users do not have to pick deployment when creating a Cloud Foundry App Instance Type, but then Instance will only be a shell of a Cloud Foundry Application.

A deployment in Morpheus can either point to a git hub repository or contain the actual manifest.yml and associated artifacts required for a Cloud Foundry deployment. During the deployment, Morpheus will gather up the files required. Therefore, if the deployment points to a git hub repository, Morpheus will fetch the files from git hub. Once the files are obtained, Morpheus will deploy the artifacts in a similar fashion to the Cloud Foundry cli. This includes parsing the manifest to obtain the parameters to create or update the Cloud Foundry application. Morpheus will ignore certain fields such as memory and disk size because they are dictated by the selected plan. Other fields are utilized such as routes. After parsing the manifest.yml file (including overwriting certain fields), Morpheus is ready to update or create the App in Cloud Foundry.

After the App is configured, the artifacts references in the Morpheus deployment are uploaded to Cloud Foundry for the App. Note that when paths are referenced in the manifest.yml file, the paths continue to be relative to the manifest. So, a jar file under build/libs would need to be found under the build/libs directory.
Morpheus Documentation

If Cloud Foundry services are specified in the manifest, they must already exist within Cloud Foundry. Morpheus App templates can be utilized to wire up Cloud Foundry services created by Morpheus. In this case, Morpheus will add all of the included service names defined in the App template to the manifest.yml services section. Therefore, multiple services can be used and wired up by Morpheus.

Example

To better understand how Morpheus parses the manifest.yml file, lets take a closer look at the Cloud Foundry ‘spring-music’ project. The project can be found here (https://github.com/cloudfoundry-samples/spring-music).

The project contains the required manifest.yml file as well as the source code and build.gradle file to define how the project is to be built. After downloading the project to your local machine, build the project to generate the jar.

Now, let’s take a look at the manifest.yml file:

```
---
applications:
- name: spring-music
  memory: 1G
  random-route: true
  path: build/libs/spring-music.jar
```

Using the Cloud Foundry docs (https://docs.cloudfoundry.org/devguide/deploy-apps/manifest.html), we can gain a better understanding of how this file is utilized by Cloud Foundry.

- The `-name` parameter defines the name that will be given to the application in Cloud Foundry. Morpheus will overwrite this value with the name given to the Instance being created in Morpheus.
- The `-memory` parameter (as well as the disk_quota parameter if specified) will be overwritten by Morpheus based on the plan specified for the Instance.
- The `-path` parameter defines, where relative to the manifest.yml file, your Cloud Foundry application can be found.
- The `-random-route` parameter, as well as all other parameters described in the Cloud Foundry documentation will simply be passed through to Cloud Foundry.

Adding Marketplace Items

1. Navigate to Infrastructure > Clouds and select your Cloud Foundry Cloud
2. Select the MARKETPLACE tab
3. Select + ADD MARKETPLACE ITEM
4. Select the Morpheus Instance Type to add the Marketplace Item to.
5. Enter version
6. Search for and select Marketplace Item
7. Select SAVE CHANGES

A Node Type and layout will be created in the Library section and the layout will be automatically added to the Instance Type selected when adding the Marketplace Item.
Provisioning Instances

Seeded and Marketplace Items

Morpheus automatically seeds MySQL, Redis and RabbitMQ PCF Instance Types, and PCF Marketplace items can also be easily added to the Provisioning Library in the Cloud detail view Marketplace tab. The Marketplace item will be added to the selected Instance Type and available when selecting the Cloud Foundry Cloud during Instance or App Template creation.

1. Navigate to Provisioning > Instances and select an Instance Type with a Cloud Foundry layout (MySQL, Redis and RabbitMQ plus Marketplace additions)
2. Select NEXT
3. Select a Group and PCF Cloud
4. Add an Instance Name
5. Optionally select and Environment Tag and/or add a custom Tag
6. Select NEXT
7. Select Version and Instance Configuration for a Cloud Foundry layout, ex: Cloud Foundry MySQL
8. Select a Plan and available options for the Plan, or use the custom Plan
9. Select a Space to add the Instance to
10. Optionally configure advanced options
11. Select NEXT
12. Optionally configure Automation options
13. Select NEXT
14. Select COMPLETE

Note: Compute, Memory, and CPU stats will be pulled, and a Cloud Foundry monitoring health check will be automatically configured for the instance.

Cloud Foundry App Instance Type

Important: Add Deployments in Provisioning > Code > Deployments to be used when provisioning a Cloud Foundry App Instance Type.

Note: Minimal options are outlined below.

1. Navigate to Provisioning > Instances and select the Cloud Foundry App Instance Type
2. Select NEXT
3. Select a Group and PCF Cloud
4. Add an Instance Name
5. Optionally select and Environment Tag and/or add a custom Tag
6. Select NEXT

7. Select a Plan and available options for the Plan, or use the custom Plan

8. Select a Space to add the Instance to

9. Select NEXT

10. In the Deployments section, select a Deployment and Version to be deployed. These can be git repos or files added in Provisioning > Code > Deployments

   **Important:** If services are specified in a git repo manifest, Morpheus assumes they are already exist in the PCF cloud with matching names.

11. Select NEXT

12. Select COMPLETE

This will quickly create the Cloud Foundry Application, and then the deployment will follow which may take longer depending on the app configuration. The location will be updated with the route once it is configured.

**Note:** Compute, Memory, and CPU stats will be pulled, and a Cloud Foundry monitoring health check will be automatically configured for the instance.

### 12.12.5 Digital Ocean

#### Add a Digital Ocean Cloud

DigitalOcean Cloud Integration Detail fields:

**Cloud Configuration**

**NAME** Name of the Cloud in Morpheus

**CODE** Unique code used for api/cli, automation and policies.

**LOCATION** Description field for adding notes on the cloud, such as location.

**VISIBILITY** For setting cloud permissions in a multi-tenant environment. Not applicable in single tenant environments.

**TENANT** If Visibility is set to Private, select the Tenant the Cloud resources will assigned to.

**ENABLED** When disabled, automatic Cloud sync is paused and the Cloud will not be selectable for provisioning.

**AUTOMATICALLY POWER ON VMS** When enabled, Morpheus will maintain the expected power state of managed VMs. Morpheus will power on any managed VMs in the Cloud that have been shut down for unknown reasons (not powered off by Morpheus) to ensure availability of services.

**Note:** When "AUTOMATICALLY POWER ON VMS" is enabled, the power state of managed VMs should be maintained in Morpheus. This setting is not applicable to discovered/unmanaged resources.
Details

**Username**  DigitalOcean Username

**API Key**  Personal access tokens/Key from the DigitalOcean API > Tokens/Keys section.

**Data Center**  Select DigitalOcean DataCenter Region

The Cloud can now be added to a Group or configured with additional Advanced options.

**Advanced Options**

**DOMAIN**  Specify a default domain for instances provisioned to this Cloud.

**SCALE PRIORITY**  Only affects Docker Provisioning. Specifies the priority with which an instance will scale into the cloud. A lower priority number means this cloud integration will take scale precedence over other cloud integrations in the group.

**APPLIANCE URL**  Alternate Appliance url for scenarios when the default Appliance URL (configured in admin > settings) is not reachable or resolvable for Instances provisioned in this cloud. The Appliance URL is used for Agent install and reporting.

**TIME ZONE**  Configures the time zone on provisioned VM's if necessary.

**DATACENTER ID**  Used for differentiating pricing among multiple datacenters. Leave blank unless prices are properly configured.

**NETWORK MODE**  Unmanaged or select a Network Integration (NSX, ACI etc)

**LOCAL FIREWALL**  On or Off. Enable to managed Host and VM firewall/IP Table rules (linux only)

**SECURITY SERVER**  Security Server setting is for Security Service Integrations such as ACI

**TRUST PROVIDER**  Select Internal (Morpheus) or an existing Trust Provider Integration

**STORAGE MODE**  Single Disk, LVM or Clustered

**BACKUP PROVIDER**  Select Internal Backups (Morpheus) or a Backup Integration

**REPLICATION PROVIDER**  Sets the default Replication Provider for the Cloud. Select an existing Replication Provider Integration

**GUIDANCE**  Enable Guidance recommendations on cloud resources.

**COSTING**  Enable for Morpheus to sync Costing data from the Cloud provider, when available. For on-prem Clouds, enabling costing activates a costing service designed to mirror the live costing experience of public clouds, including invoicing with line items and real-time cost data (Operations > Costing > Invoices). If your organization utilizes reserved instances and you want to pull in related pricing data, select Costing and Reservations. If this is not relevant, select Costing to save money on additional calls to the AWS Cost Explorer API or similar service for other clouds.

**DNS INTEGRATION**  Records for instances provisioned in this cloud will be added to selected DNS integration.

**SERVICE REGISTRY**  Services for instances provisioned in this cloud will be added to selected Service Registry integration.

**CONFIG MANAGEMENT**  Select a Chef, Salt, Ansible or Puppet integration to be used with this Cloud.

**CMDB**  Select CMDB Integration to automatically update selected CMDB.

**CMDB DISCOVERY**  When checked, any automatically discovered (unmanaged) servers onboarded into Morpheus from this Cloud will also have CMDB records created for them.

**CHANGE MANAGEMENT**  Select an existing Change Management Integration to set on the Cloud. ex: Cherwell

**AGENT INSTALL MODE**
• SSH / WINRM: Morpheus will use SSH or WINRM for Agent install.

• Cloud Init / Unattend (when available): (DEFAULT) Morpheus will utilize Cloud-Init or Cloudbase-Init for agent install when provisioning images with Cloud-Init/Cloudbase-Init installed. Morpheus will fall back on SSH or WINRM if cloud-init is not installed on the provisioned image. Morpheus will also add Agent installation to Windows unattend.xml data when performing Guest Customizations or utilizing sysprepped images.

API PROXY  Set a proxy for outbound communication from the Morpheus Appliance to the Cloud endpoints. Proxies can be added in the Infrastructure > Networks > Proxies tab.

INSTALL AGENT  Enable to have Agent Installation on by default for all provisioning into this Cloud. Disable for Agent Installation to be off by default for all provisioning into this Cloud.

Provisioning Options

PROXY  Set a proxy for inbound communication from Instances to the Morpheus Appliance. Proxies can be added in the Infrastructure > Networks > Proxies tab.

Bypass Proxy for Appliance URL  Enable to bypass proxy settings (if added) for Morpheus Agent communication to the Appliance URL.

NO PROXY  Include a list of IP addresses or name servers to exclude from proxy traversal


12.12.6 ESXi

The ESXi Cloud type enables managing and provisioning to ESXi hosts, even without the ESXi API enabled.

Important:  The VMware ESXi integration is for adding a single ESXi / vSphere Hypervisor host. If you have vCenter please use the VMWare vCenter cloud type for full vSphere integraiton features.

To get started with VMware ESXi, simply add a VMware ESXi Cloud in either the Infrastructure > Clouds or Infrastructure > Groups section.

1. Select + Create Cloud Button
2. Select ESXi from the Add Cloud modal
3. Select NEXT
4. Provide the following information.

Cloud Configuration

NAME  Name of the Cloud in Morpheus

CODE  Unique code used for api/cli, automation and policies.

LOCATION  Description field for adding notes on the cloud, such as location.

VISIBILITY  For setting cloud permissions in a multi-tenant environment. Not applicable in single tenant environments.

TENANT  If Visibility is set to Private, select the Tenant the Cloud resources will assigned to.

ENABLED  When disabled, automatic Cloud sync is paused and the Cloud will not be selectable for provision-
AUTOMATICALLY POWER ON VMS  When enabled, Morpheus will maintain the expected power state of managed VMs. Morpheus will power on any managed VMs in the Cloud that have been shut down for unknown reasons (not powered off by Morpheus) to ensure availability of services.

Note: When “AUTOMATICALLY POWER ON VMS” is enabled, the power state of managed VMs should be maintained in Morpheus. This setting is not applicable to discovered/unmanaged resources.

Details

• ESXi Host name or IP address
• Username ( This is normally root )
• Password

Note: If you receive the message “Error! Invalid cloud config” Please ensure you have ssh enabled on the ESXi host.

Advanced Options

DOMAIN  Specify a default domain for instances provisioned to this Cloud.

SCALE PRIORITY  Only affects Docker Provisioning. Specifies the priority with which an instance will scale into the cloud. A lower priority number means this cloud integration will take scale precedence over other cloud integrations in the group.

APPLIANCE URL  Alternate Appliance url for scenarios when the default Appliance URL (configured in admin > settings) is not reachable or resolvable for Instances provisioned in this cloud. The Appliance URL is used for Agent install and reporting.

TIME ZONE  Configures the time zone on provisioned VM’s if necessary.

DATACENTER ID  Used for differentiating pricing among multiple datacenters. Leave blank unless prices are properly configured.

NETWORK MODE  Unmanaged or select a Network Integration (NSX, ACI etc)

LOCAL FIREWALL  On or Off. Enable to managed Host and VM firewall/IP Table rules (linux only)

SECURITY SERVER  Security Server setting is for Security Service Integrations such as ACI

TRUST PROVIDER  Select Internal (Morpheus) or an existing Trust Provider Integration

STORAGE MODE  Single Disk, LVM or Clustered

BACKUP PROVIDER  Select Internal Backups (Morpheus) or a Backup Integration

REPLICATION PROVIDER  Sets the default Replication Provider for the Cloud. Select an existing Replication Provider Integration

GUIDANCE  Enable Guidance recommendations on cloud resources.

COSTING  Enable for Morpheus to sync Costing data from the Cloud provider, when available. For on-prem Clouds, enabling costing activates a costing service designed to mirror the live costing experience of public clouds, including invoicing with line items and real-time cost data (Operations > Costing > Invoices). If your organization utilizes reserved instances and you want to pull in related pricing data, select Costing and Reservations. If this is not relevant, select Costing to save money on additional calls to the AWS Cost Explorer API or similar service for other clouds.

DNS INTEGRATION  Records for instances provisioned in this cloud will be added to selected DNS integration.
SERVICE REGISTRY  Services for instances provisioned in this cloud will be added to selected Service Registry integration.

CONFIG MANAGEMENT  Select a Chef, Salt, Ansible or Puppet integration to be used with this Cloud.

CMDB  Select CMDB Integration to automatically update selected CMDB.

CMDB DISCOVERY  When checked, any automatically discovered (unmanaged) servers onboarded into Morpheus from this Cloud will also have CMDB records created for them.

CHANGE MANAGEMENT  Select an existing Change Management Integration to set on the Cloud. ex: Cherwell

AGENT INSTALL MODE
- SSH / WINRM: Morpheus will use SSH or WINRM for Agent install.
- Cloud Init / Unattend (when available): (DEFAULT) Morpheus will utilize Cloud-Init or Cloudbase-Init for agent install when provisioning images with Cloud-Init/Cloudbase-Init installed. Morpheus will fall back on SSH or WINRM if cloud-init is not installed on the provisioned image. Morpheus will also add Agent installation to Windows unattend.xml data when performing Guest Customizations or utilizing sysprepped images.

API PROXY  Set a proxy for outbound communication from the Morpheus Appliance to the Cloud endpoints. Proxies can be added in the Infrastructure > Networks > Proxies tab.

INSTALL AGENT  Enable to have Agent Installation on by default for all provisioning into this Cloud. Disable for Agent Installation to be off by default for all provisioning into this Cloud.

Provisioning Options

PROXY  Set a proxy for inbound communication from Instances to the Morpheus Appliance. Proxies can be added in the Infrastructure > Networks > Proxies tab.

Bypass Proxy for Appliance URL  Enable to bypass proxy settings (if added) for Morpheus Agent communication to the Appliance URL.

NO PROXY  Include a list of IP addresses or name servers to exclude from proxy traversal


Important:  ESXi provisioning require a vmx file, which is not included in an OVF/OVA export from vCenter. A proper vmx file must be included when adding a vmdk/ovf/ova image to Virtual Images in Morpheus for successful provisioning.

12.12.7 Google Cloud Platform (GCP)

Integration Features
- Provisioning Virtual Machines
- Network tagging
- Private and Local Images
- Google VM Snapshots
- Brownfield Inventory
- Costing
• Right-sizing
• Shared Network Support

Requirements for Integration with Morpheus

To integrate Morpheus with Google Cloud Platform, you will need the following. APIs are enabled in “APIs & Services” and must be enabled for all projects or the selected project (depending on your GCP Cloud integration settings):

• The Compute Engine API enabled
• The Cloud Resource Manager API enabled
• The Cloud Billing API
• The Identity and Access Management (IAM) API enabled
• The BigQuery API enabled
• The BigQuery Data Transfer API enabled
• The Kubernetes Engine API enabled (required to provision GKE clusters)
• Credentials for an IAM service account with Owner or Compute Admin role permissions
• The private key and client email for the service account

This integration guide goes through the process of configuring your account and obtaining the information necessary to integrate with Morpheus.

Enabling the Compute Engine API

1. Log into the Google Cloud Platform web console
2. Hover over the “APIs & Services” menu and click on Dashboard
3. Click + ENABLE APIS AND SERVICES

4. In the search bar, search for “Compute Engine API”
5. Select “Compute Engine API” and click *ENABLE*. It may take a few moments for the API to be fully enabled.

**Note:** If the button is labeled *MANAGE* rather than *ENABLE*, the API is already enabled. When enabling Compute Engine API, you may be prompted to also enable Cloud Billing API. It’s also required this API is enabled so go ahead and enable it at this point and you won’t have to do so later.

6. Head back to the API library and search for “Cloud Resource Manager API”
7. Select “Cloud Resource Manager API” and click *ENABLE*. It may take a few moments for the API to be fully enabled.
8. If you haven’t already enabled Cloud Billing API, head back to the API library and search for “Cloud Billing API”
9. Select “Cloud Billing API” and click *ENABLE*. It may take a few moments for the API to be fully enabled.

**Creating a Service Account**

1. From the landing page of the GCP web console, hover over the “IAM & Admin” menu and click on “Service Accounts”
2. Click + *CREATE SERVICE ACCOUNT*
3. Enter at least a name for your new service and click CREATE

4. After creating the service account, you’ll be prompted to set a role for the account. In order to fully integrate with Morpheus, you must use an account in the Owner role or the Compute Admin role

5. Click CONTINUE

6. Following creation of the service account, you’ll be taken back to the list of existing service accounts
Generating Keys and Integrating with Morpheus

1. From the list of service accounts, click the ellipsis button (…)
2. Click “Manage Keys”

3. On the Keys page, click “Add Key” and then “Create New Key”
4. Select JSON format and click CREATE
5. A JSON-formatted document will be downloaded, this document contains the Project ID, private key, and client email values needed to complete the integration process in the next step

Add a GCP Cloud

Note: The JSON-formatted document downloaded when creating a key for your service account contains all of the required values for completing the integration. Consult the above section on generating keys if needed.

1. Navigate to Infrastructure > Clouds
2. Select + CREATE CLOUD, select Google Cloud, and then click NEXT.
3. Enter the following into the Create Cloud modal:
   **Cloud Configuration**
   - **NAME** Name of the Cloud in Morpheus
   - **CODE** Unique code used for api/cli, automation and policies.
   - **LOCATION** Description field for adding notes on the cloud, such as location.
   - **VISIBILITY** For setting cloud permissions in a multi-tenant environment. Not applicable in single tenant environments.
   - **TENANT** If Visibility is set to Private, select the Tenant the Cloud resources will assigned to.
   - **ENABLED** When disabled, automatic Cloud sync is paused and the Cloud will not be selectable for provisioning.
   - **AUTOMATICALLY POWER ON VMS** When enabled, Morpheus will maintain the expected power state of managed VMs. Morpheus will power on any managed VMs in the Cloud that have been shut down for unknown reasons (not powered off by Morpheus) to ensure availability of services.
Note: When “AUTOMATICALLY POWER ON VMS” is enabled, the power state of managed VMs should be maintained in Morpheus. This setting is not applicable to discovered/unmanaged resources.

Details

PRIVATE KEY The service account private key. Paste in the entire value between (but not including) the quotation marks in your downloaded JSON document, formatted like the following example: 

```
-----BEGIN PRIVATE KEY------
(your_key)------END PRIVATE KEY------
```

CLIENT EMAIL The service account client email, ex: morpheus@morpheus.iam.gserviceaccount.com

PROJECT ID Projects will auto-populate upon successful entry of the private key and client email. You can opt to scope the GCP integration to a single Project or select “All” to instead select the Project from the Resource Pool dropdown at provision time

REGION Regions will auto-populate upon successful entry of the private key and client email. Select the appropriate region for this Cloud, if applicable. You can also opt to scope the GCP integration to all regions to allow users to select from any region at provision time

INVENTORY EXISTING INSTANCES If checked, existing GCP resources will be inventoried and appear as unmanaged virtual machines in Morpheus.

If advanced options are not needed, click NEXT to advance to the Group selection page. Otherwise, continue on with this guide and review advanced or provisioning options.

Advanced Options

DOMAIN Specify a default domain for instances provisioned to this Cloud.

SCALE PRIORITY Only affects Docker Provisioning. Specifies the priority with which an instance will scale into the cloud. A lower priority number means this cloud integration will take scale precedence over other cloud integrations in the group.

APPLIANCE URL Alternate Appliance url for scenarios when the default Appliance URL (configured in admin > settings) is not reachable or resolvable for Instances provisioned in this cloud. The Appliance URL is used for Agent install and reporting.

TIME ZONE Configures the time zone on provisioned VM’s if necessary.

DATACENTER ID Used for differentiating pricing among multiple datacenters. Leave blank unless prices are properly configured.

NETWORK MODE Unmanaged or select a Network Integration (NSX, ACI etc)

LOCAL FIREWALL On or Off. Enable to managed Host and VM firewall/IP Table rules (linux only)

SECURITY SERVER Security Server setting is for Security Service Integrations such as ACI

TRUST PROVIDER Select Internal (Morpheus) or an existing Trust Provider Integration

STORAGE MODE Single Disk, LVM or Clustered

BACKUP PROVIDER Select Internal Backups (Morpheus) or a Backup Integration

REPLICATION PROVIDER Sets the default Replication Provider for the Cloud. Select an existing Replication Provider Integration

GUIDANCE Enable Guidance recommendations on cloud resources.

COSTING Enable for Morpheus to sync Costing data from the Cloud provider, when available. For on-prem Clouds, enabling costing activates a costing service designed to mirror the live costing experience of public clouds, including invoicing with line items and real-time cost data (Operations > Costing > Invoices).

If your organization utilizes reserved instances and you want to pull in related pricing data, select Costing
and Reservations. If this is not relevant, select Costing to save money on additional calls to the AWS Cost Explorer API or similar service for other clouds.

DNS INTEGRATION Records for instances provisioned in this cloud will be added to selected DNS integration.

SERVICE REGISTRY Services for instances provisioned in this cloud will be added to selected Service Registry integration.

CONFIG MANAGEMENT Select a Chef, Salt, Ansible or Puppet integration to be used with this Cloud.

CMDB Select CMDB Integration to automatically update selected CMDB.

CMDB DISCOVERY When checked, any automatically discovered (unmanaged) servers onboarded into Morpheus from this Cloud will also have CMDB records created for them.

CHANGE MANAGEMENT Select an existing Change Management Integration to set on the Cloud. ex: Cherwell

AGENT INSTALL MODE

- SSH / WINRM: Morpheus will use SSH or WINRM for Agent install.
- Cloud Init / Unattend (when available): (DEFAULT) Morpheus will utilize Cloud-Init or Cloudbase-Init for agent install when provisioning images with Cloud-Init/Cloudbase-Init installed. Morpheus will fall back on SSH or WINRM if cloud-init is not installed on the provisioned image. Morpheus will also add Agent installation to Windows unattend.xml data when performing Guest Customizations or utilizing sysprepped images.

API PROXY Set a proxy for outbound communication from the Morpheus Appliance to the Cloud endpoints. Proxies can be added in the Infrastructure > Networks > Proxies tab.

INSTALL AGENT Enable to have Agent Installation on by default for all provisioning into this Cloud. Disable for Agent Installation to be off by default for all provisioning into this Cloud.

Provisioning Options

PROXY Set a proxy for inbound communication from Instances to the Morpheus Appliance. Proxies can be added in the Infrastructure > Networks > Proxies tab.

Bypass Proxy for Appliance URL Enable to bypass proxy settings (if added) for Morpheus Agent communication to the Appliance URL.

NO PROXY Include a list of IP addresses or name servers to exclude from proxy traversal


4. After reviewing all options, click NEXT to advance to the Group selection page. Following Group selection, click COMPLETE to finish the integration process. If you’ve opted to inventory existing Instances, they will be viewable in Morpheus shortly. At this point, you are ready to provision new resources in Google Cloud Platform as needed!

Important: If you experience difficulties adding a GCP Cloud, review the above guide and ensure you’ve met all requirements for completing the integration. For example, if the Compute Engine API is not enabled, Morpheus will not accept credentials entered on the Create Cloud modal. If you repeatedly run into problems completing the integration process, review the above guide in its entirely and double check that each step is completed and your account meets all configuration requirements.
Create a GCP Project

On initial integration, Morpheus will sync Projects and allow you to scope the integration to a specific Project or to scope the integration to all Projects. As time goes on, additional Projects are continually synced and can be managed from within the Resources tab on the Cloud detail page (Infrastructure > Clouds > Selected GCP Cloud). Within the Resources tab, users can edit some Project settings as well as delete Projects if needed.

To create a new GCP Project:

1. Click + ADD RESOURCE POOL
2. Enter a name value for the new Project
3. Mark the “DEFAULT” box if you’d prefer newly provisioned Instances default to the new Project
4. Enter a Project ID and ensure it meets the listed validation requirements
5. Set a Parent value if the new Project should exist underneath a parent organization
6. Finally, select a billing account
7. Click SAVE CHANGES

After a few minutes, the new Project will be ready on the GCP side and Morpheus will be ready to provision new resources into it.

Enabling Live Costing for GCP

GCP costing is done at the Billing Account level. Each Billing Account can be linked to one or more GCP Projects. All projects which are linked to the Billing Account will have their costing data available to Morpheus but if the GCP Cloud has been scoped to only one Project, Morpheus will ingest costing data only for that Project. Users can view the Billing Account linked to a particular project by clicking on the hamburger menu (main menu button in the far upper-left of the console window) and selecting billing. A pop-up window will give users the option to navigate to the Billing Account which is linked to the currently-selected Project.

Within the Billing Account, Standard Usage Cost must be enabled for Morpheus to access costing data. From the page for the appropriate Billing Account, click on Billing Export and then click “Edit Settings” under the “Standard usage...
cost heading”. Specify a project and create a dataset or specify an existing one. In doing this, you’re specifying a location for the dataset which will be for the entire billing account and not just for the Project the dataset resides in.

With configuration in the GCP console completed, we can now enable cost onboarding from the Morpheus side. Add or edit an existing GCP Cloud (Infrastructure > Clouds). Within the Advanced Options section, note the COSTING PROJECT and COSTING DATASET fields. When selecting a Project, associated datasets (if any) will automatically be loaded into the dropdown in the next field for selection. Additionally, the COSTING field should be set to “Sync Costing” rather than “Off”. Recall from the previous paragraph that this is merely pointing to the Project that houses the appropriate dataset. If your GCP Cloud in Morpheus is configured for all Projects, all costing data will be consumed for the Projects linked to the associated Billing Account (assuming those Projects have billing enabled). If the GCP Cloud in Morpheus is scoped to just one Project, only billing data for that Project will be onboarded. For this reason, the selected Costing Project can be (but is not necessarily) the Project to which the Morpheus Cloud is scoped.
Windows Images

Morpheus can add custom metadata that will be injected into the unattend conf by GCP during provisioning. This is required for customizations including setting the Windows Administrator password during provisioning. GCP Windows Images must be sysprepped using the GCESysprep command prior to image creation, and must have platform/os set on the Virtual Image record in Morpheus after image sync for successful customization and Agent Installation.

GCP Windows Requirements

- GCP Windows Images must be sysprepped using the GCESysprep command prior to Image creation in GCP. Refer to Google’s “creating-windows-os-image” doc.
- Once the Image is synced into Morpheus, the Platform (Windows, Windows 2016 etc) must be set on the Morpheus Virtual Image record, otherwise linux is assumed and the metadata will not be generated correctly.
- The Global Windows “Administrator” password must be set in Morpheus under /admin/provisioning/settings > Windows Settings > Administrator Password, or Administrator and password defined on the Morpheus Virtual Image record.
- Be aware the unattend configuration during startup after sysprep delays causes a reboot and a prolonged finalization process during provisioning, and console/rdp may not be available during this time as windows is configuring.

Note: Some Google provided Windows Images have slow startups that cause the Morpheus Agent service to not start within the default 30 second service startup timeframe, including after initial reboot after sysprep/unattend configuration. This can be adjusted by running New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\" -Name "ServicesPipeTimeout" -PropertyType DWORD -Value 180000 in powershell on the Windows Image.

Important: Failure to use a GCP Windows Image that has not been sysprepped using GCESysprep will cause Agent Installation, Automation, and Console issues as Morpheus will not be able to set user credentials and authenticate.

12.12.8 Huawei Cloud

Features

- Virtual machine provisioning
- Backups
- Brownfield VM management and migration
- Hypervisor remote console
- Cloud sync
- Lifecycle management and resizing
- Network security group creation
- Network security group management
- Router and network creation
- Load balancer services
• Docker host management and configuration
• Floating IP assignment
• Huawei OBS buckets (create, manage, delete, and discovery)
• Huawei SFS (create, manage, and delete)

**Integrate Huawei Cloud with Morpheus**

To integrate Huawei Cloud with Morpheus, we’ll gather the following pieces of information:

• Account Name
• Identity (IAM) API URL
• Project
• Username
• Password

Begin by logging into your Huawei Cloud console. If you’re not currently logged in, you will be prompted to do so. Once on the console page, hover over your username in the upper-right corner of the application window and select “My Credentials”.

From the credentials page, we can gather the Account Name and the Project Name, record them for later when we provide the integration information to Morpheus.
To gather the API endpoint URL, take a look at the complete list of endpoints. If a specific endpoint exists for your region, use it. In any other case use the endpoint for all regions. It will be formatted like this: https://iam.myhuaweicloud.com/v3.

With this information gathered, and presuming you know the credentials for the service account you wish to use, we can move back into Morpheus-UI.

Navigate to Infrastructure > Clouds and click + ADD. Scroll to Huawei Cloud and click NEXT. The information we’ve gathered will be plugged into the CREATE CLOUD modal. The DOMAIN ID field will accept the Account Name field we gathered. Your completed CREATE CLOUD modal will look similar to the one pictured below:
After clicking NEXT, add this new Cloud to a Group or create a new Group. On finalizing the wizard, Huawei Cloud will be integrated into Morpheus and ready for provisioning. If you opted to inventory existing workloads, those will be onboarded shortly.

Add/Edit Huawei Cloud Modal Fields

Cloud Configuration

NAME  Name of the Cloud in Morpheus

CODE  Unique code used for api/cli, automation and policies.

LOCATION  Description field for adding notes on the cloud, such as location.

VISIBILITY  For setting cloud permissions in a multi-tenant environment. Not applicable in single tenant environments.

TENANT  If Visibility is set to Private, select the Tenant the Cloud resources will assigned to.

ENABLED  When disabled, automatic Cloud sync is paused and the Cloud will not be selectable for provisioning.
AUTOMATICALLY POWER ON VMS  When enabled, Morpheus will maintain the expected power state of managed VMs. Morpheus will power on any managed VMs in the Cloud that have been shut down for unknown reasons (not powered off by Morpheus) to ensure availability of services.

Note: When “AUTOMATICALLY POWER ON VMS” is enabled, the power state of managed VMs should be maintained in Morpheus. This setting is not applicable to discovered/unmanaged resources.

Details

IDENTITY API URL  The v3 identity endpoint. See the integration steps above for more detail

DOMAIN ID  The DOMAIN ID field takes the “Account Name” as shown on the Basic Information page of the account. See the integration steps above for more detail

PROJECT  The target project name. See the integration steps above for more detail

USERNAME  The service account username. See the integration steps above for more detail

PASSWORD  The integration service account password. See the integration steps above for more detail

IMAGE FORMAT  Select QCOW2, RAW or VMDK image type

Image Store  Set an OBS bucket as a permanent store location for Morpheus virtual images. Users are limited to uploading images of 2GB or less in size if an OBS bucket is not specified here

Inventory Existing Instances  Select for Morpheus to discover and sync existing VMs

Enable Hypervisor Console  Hypervisor console support for openstack currently only supports novnc. Be sure the novnc proxy is configured properly in your openstack environment.

Tip: When using the RAW image format, you can bypass the image conversion service within the cloud leading to quicker performance. Other image formats are converted to RAW format and back when performing various actions. Using the RAW format from the start will bypass these conversion steps.

Advanced Options

DOMAIN  Specify a default domain for instances provisioned to this Cloud.

SCALE PRIORITY  Only affects Docker Provisioning. Specifies the priority with which an instance will scale into the cloud. A lower priority number means this cloud integration will take scale precedence over other cloud integrations in the group.

APPLIANCE URL  Alternate Appliance url for scenarios when the default Appliance URL (configured in admin > settings) is not reachable or resolvable for Instances provisioned in this cloud. The Appliance URL is used for Agent install and reporting.

TIME ZONE  Configures the time zone on provisioned VM’s if necessary.

DATACENTER ID  Used for differentiating pricing among multiple datacenters. Leave blank unless prices are properly configured.

NETWORK MODE  Unmanaged or select a Network Integration (NSX, ACI etc)

LOCAL FIREWALL  On or Off. Enable to managed Host and VM firewall/IP Table rules (linux only)

SECURITY SERVER  Security Server setting is for Security Service Integrations such as ACI

TRUST PROVIDER  Select Internal (Morpheus) or an existing Trust Provider Integration
STORAGE MODE  Single Disk, LVM or Clustered

BACKUP PROVIDER  Select Internal Backups (Morpheus) or a Backup Integration

REPLICATION PROVIDER  Sets the default Replication Provider for the Cloud. Select an existing Replication Provider Integration

GUIDANCE  Enable Guidance recommendations on cloud resources.

COSTING  Enable for Morpheus to sync Costing data from the Cloud provider, when available. For on-prem Clouds, enabling costing activates a costing service designed to mirror the live costing experience of public clouds, including invoicing with line items and real-time cost data (Operations > Costing > Invoices). If your organization utilizes reserved instances and you want to pull in related pricing data, select Costing and Reservations. If this is not relevant, select Costing to save money on additional calls to the AWS Cost Explorer API or similar service for other clouds.

DNS INTEGRATION  Records for instances provisioned in this cloud will be added to selected DNS integration.

SERVICE REGISTRY  Services for instances provisioned in this cloud will be added to selected Service Registry integration.

CONFIG MANAGEMENT  Select a Chef, Salt, Ansible or Puppet integration to be used with this Cloud.

CMDB  Select CMDB Integration to automatically update selected CMDB.

CMDB DISCOVERY  When checked, any automatically discovered (unmanaged) servers onboarded into Morpheus from this Cloud will also have CMDB records created for them.

CHANGE MANAGEMENT  Select an existing Change Management Integration to set on the Cloud. ex: Cherwell

AGENT INSTALL MODE

- SSH / WINRM: Morpheus will use SSH or WINRM for Agent install.
- Cloud Init / Unattend (when available): (DEFAULT) Morpheus will utilize Cloud-Init or Cloudbase-Init for agent install when provisioning images with Cloud-Init/Cloudbase-Init installed. Morpheus will fall back on SSH or WINRM if cloud-init is not installed on the provisioned image. Morpheus will also add Agent installation to Windows unattend.xml data when performing Guest Customizations or utilizing sysprepped images.

API PROXY  Set a proxy for outbound communication from the Morpheus Appliance to the Cloud endpoints. Proxies can be added in the Infrastructure > Networks > Proxies tab.

INSTALL AGENT  Enable to have Agent Installation on by default for all provisioning into this Cloud. Disable for Agent Installation to be off by default for all provisioning into this Cloud.

Provisioning Options

PROXY  Set a proxy for inbound communication from Instances to the Morpheus Appliance. Proxies can be added in the Infrastructure > Networks > Proxies tab.

Bypass Proxy for Appliance URL  Enable to bypass proxy settings (if added) for Morpheus Agent communication to the Appliance URL.

NO PROXY  Include a list of IP addresses or name servers to exclude from proxy traversal

Huawei Scalable File Service (SFS)

The Morpheus integration with Huawei Cloud includes the capability to work with Huawei Scalable File Service (SFS). SFS is shared file storage hosted on Huawei Cloud. By integrating Morpheus with Huawei Cloud you can discover, create, manage, and delete SFS servers, as well as view and work with the file shares and files contained therein.

SFS Server Discovery and Management

On integrating Huawei Cloud with Morpheus, SFS servers and file shares are discovered automatically after a short time. The server(s) can be viewed in Infrastructure > Storage > Servers. By viewing the server detail page and clicking EDIT, the storage server can be scoped as needed. Administrators can choose to scope to other Huawei Cloud integrations (if more than one relevant integration currently exists), select from synced availability zones, and scope the storage server to specific Tenants if desired.
Additionally, Huawei SFS servers can be created from the storage server list page (Infrastructure > Storage > Servers) directly in Morpheus. Click + ADD to begin and set the storage server type value to “Huawei SFS”. Just like with existing synced SFS servers, those created from Morpheus can be scoped as needed.
SFS File Share Discovery and Management

Discovered file shares will appear among other file shares synced with Morpheus in Infrastructure > Storage > File Shares. Depending on the number of cloud integrations in your Morpheus appliance and the number of cloud integrations available to your user account, this list may be quite large. Using the search bar on this page, we can narrow down the list to file shares displayed to those whose names match the search terms.

We can drill into individual file shares by clicking on their hyperlinked name in the list of all integrated file shares. From the file share detail page, a list of files will appear on the files tab. Begin the process of adding a new file by clicking + ADD. The Access tab on the file shares detail page allows users to view and manage ACL rules.

**Note:** A “Failed to load files from storage provider” is present when the Morpheus appliance doesn’t have access to the file share.

New Huawei SFS file shares can be created directly in Morpheus. From the file shares list page, get started by clicking + ADD. Select the type “Huawei SFS Share”. Set the storage service field to a pre-existing Huawei SFS server. A friendly name for the file share in Morpheus and selecting from synced availability zones are required fields.
NEW FILE SHARE

NAME: Huawei File Share

STORAGE SERVICE: Labs Huawei SFS

AVAILABILITY ZONE: ap-southeast-1a

SHARE SIZE: 0 GB

ACTIVE

DEFAULT BACKUP TARGET

DEFAULT DEPLOYMENT ARCHIVE TARGET

DEFAULT VIRTUAL IMAGE STORE

Retention

RETENTION POLICY: None

SAVE CHANGES
Morpheus Documentation

**Huawei Object Storage Service (OBS)**

The Morpheus integration with Huawei Cloud also supports Object Storage Service (OBS). Morpheus will automatically onboard existing OBS servers and buckets shortly after completing the cloud integration. Before you can add a new OBS server from Morpheus, you must know or generate a key and secret value from the Huawei console and must provide a Huawei OBS API endpoint.

**Generate a Key and Secret**

From the Huawei web console, log into the account used to integrate Huawei Cloud with Morpheus. Hover over your account name in the upper-right corner of the application window and click “My Credentials”. Select “Access Keys” from the left-hand sidebar. To create a new key, click + Create Access Key. Complete the two-factor authentication steps in the box that appears.

Once the key is generated, download or record the key and store it in a safe location. The key will not be viewable or available for download again after this point.
**Create OBS Server in Morpheus**

With the key and secret value in hand from the previous section, navigate to Infrastructure > Storage > Servers. Click + ADD. On changing the server type to Huawei OBS, you will see the fields for the access key and the secret key. OBS API endpoints can be found in Huawei endpoint documentation. Include those three values in the Create Server modal along with a friendly name for use in Morpheus UI. Just like with SFS objects, we can choose to scope the server to all or specific Tenants at this time.
Create Huawei OBS Bucket

With an OBS server onboarded or created in Morpheus, you’re able to create and manage Huawei OBS buckets as needed. To create a new bucket, navigate to Infrastructure > Storage > Buckets. Click + ADD and select “Huawei OBS Bucket”. The following fields are required when creating a Huawei OBS bucket:

- **NAME**: A friendly name for use in Morpheus UI
- **STORAGE SERVICE**: Choose the OBS server to associate the new bucket with
- **BUCKET NAME**: The name of the bucket in Huawei Cloud, this must be unique
- **STORAGE CLASS**: If needed, view the discussion of storage classes in Huawei support documentation
- **BUCKET ACL**: Public Read, Public Read/Write, or Private
- **BUCKET POLICY**: Public Read, Public Read/Write, or Private
- **STORAGE QUOTA**: Set to 0 for no quota

Once finished, click **SAVE CHANGES**
NEW BUCKET

NAME | My OBS Bucket

STORAGE SERVICE | Labs Huawei OBS

BUCKET NAME | my-obs-bucket

STORAGE CLASS | Standard

BUCKET ACL | Private

BUCKET POLICY | Private

STORAGE QUOTA | 0 GB

CREATE BUCKET

ACTIVE

DEFAULT BACKUP TARGET

DEFAULT DEPLOYMENT ARCHIVE TARGET

DEFAULT VIRTUAL IMAGE STORE

Retention

RETENTION POLICY | None

SAVE CHANGES
Network and Router Creation

Once a Huawei Cloud is integrated into Morpheus, new network creation options become available. When adding a new network (Infrastructure > Networks > Networks Tab), a new type labeled “Huawei Private Network” is available when clicking +ADD. When the user creates this network construct in Morpheus, a layer two subnet is created but it’s not connected to a Virtual Private Cloud (VPC). This is by design as an Internet-routable network is not always desired. Continue on with this section after creating the network to also create a VPC (router).

Create a network

1. Navigate to Infrastructure > Networks
2. Click on the Networks tab
3. Click +ADD
4. Select Huawei Private Network
5. Complete the modal based on requirements for the new network
6. Click SAVE CHANGES

Create a router

1. Navigate to Infrastructure > Networks
2. Click on the Routers tab
3. Click +ADD
4. Select Huawei Router
5. Complete the modal based on requirements for the new router
6. Click SAVE CHANGES

When creating a router, it’s helpful to note that the External Network is the floating IP network that has been assigned to the Huawei project. This network will grant your Instances their routes out to the Internet. The Internal Subnet can be a layer two subnet that you may have created in the previous step. In addition, multiple subnets can be added to the router (VPC) and the IP address on the subnet would be the router’s internal IP address.

12.12.9 Hyper-V

Hyper-V is the virtualized server computing environment introduced by Microsoft. Hyper-V is consumed by Morpheus as a private cloud offering and is a common hypervisor technology in data centers. Morpheus provides an avenue to aggregate Hyper-V resources together to allow efficient and seamless deployment of applications as a virtual machine (VM) or Docker host in the world of Hyper-V.
Features

- Virtual Machine Provisioning
- Discovery of Existing Instances
- Containers
- Backups / Snapshots
- Resources Groups
- Migrations
- Auto Scaling
- Load Balancing
- Remote Console
- Periodic Synchronization
- Veeam Integration
- Lifecycle Management and Resize
- Unique Kerberos Authentication

Getting Started

To get started, a few prerequisites must first be met. The Hyper-V host must be installed with its firewall enabled and it can either be joined to a domain or standalone. The Hyper-V host must also have the external network of Hyper-V configured and it can share this network with the management operating system. A user account that is part of the local administrators group on the Hyper-V host is also required. This document covers Hyper-V 2008 and Hyper-V 2012.

Understanding WinRM

Morpheus uses WinRM to communicate to the Hyper-V host for deployment of the Morpheus Agent. The Morpheus Agent allows for the host dashboard to be populated with information in the form of graphs that cover CPU, Network, Storage, and memory consumption. Furthermore, this Agent provides logging and monitoring capabilities.

If Windows Remote Management (WinRM) is not installed and configured, WinRM scripts do not run and the WinRM command line tool cannot perform data operations or allow for the Morpheus Agent to be installed. WinRM uses HTTP port 5985 or HTTPS port 5986 for communications.

To better understand all of the default settings of WinRM please refer to the following page in Microsoft documentation.

Native Authentication

To configure WinRM with default settings (WINRM_NATIVE)

Type the following command at a command prompt:

$ winrm quickconfig
If you are not running under the local computer Administrator account, you must either select Run as Administrator from the Start menu or use the `runas` command at a command prompt.

When the tool displays Make these changes [y/n]?, type y.

If configuration is successful, the following output is displayed:

```
$ WinRM has been updated for remote management.
$ WinRM service type changed to delayed auto start.
$ WinRM service started.
$ Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.
```

Keep the default settings for client and server components of WinRM, or customize them. By default Kerberos is enabled and if domain authentication is not being used we want to disable that. Issue the below commands to setup basic authentication:

```
$ winrm set winrm/config/service/Auth '@{Basic="true"}''
$ winrm set winrm/config/service '@{AllowUnencrypted="true"}''
$ winrm set winrm/config/service/Auth '@{Kerberos="false"}''
```

**Domain Authentication**

To configure WinRM with Domain Authentication (WINRM_INTERNAL)

Type the following command at a command prompt

```
$ winrm quickconfig
```

If you are not running under the local computer Administrator account, you must either select Run as Administrator from the Start menu or use the `runas` command at a command prompt.

When the tool displays Make these changes [y/n]?, type y.

If configuration is successful, the following output is displayed:

```
$ WinRM has been updated for remote management.
$ WinRM service type changed to delayed auto start.
$ WinRM service started.
$ Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.
```

Keep the default settings for client and server components of WinRM, or customize them. Issue the below commands to setup domain authentication:

```
$ winrm set winrm/config/service/Auth @(Basic="true")'
$ winrm set winrm/config/service @(AllowUnencrypted="false")'
$ winrm set winrm/config/service/Auth @(Kerberos="true")'
```

Kerberos authentication will also need to be configured on the Morpheus appliance to support Windows domain accounts to access the remote host with WINRM_INTERNAL connection type.

On the Morpheus appliance the `krb5-user` package must be installed.

For Ubuntu the command is as follows:

```
$ sudo apt-get install krb5-user
```

For Centos the command is as follows:
Create a file in /etc called krb5.conf and replace the domain name with the name of the domain to be used. In this case we used Morpheus .com as the domain.

```plaintext
[libdefaults]
  default_realm = |morpheus| .COM
  dns_lookup_kdc = true
  verify_ap_req_nofail = false
  default_tgs_enctypes = rc4-hmac
  default_tkt_enctypes = rc4-hmac

[realms]
  |morpheus| .COM = {
    kdc = win-ad.|morpheus| .COM:88
    admin_server = win-ad.|morpheus| .COM:749
  }

[domain_realm]
  .|morpheus| .COM = |morpheus| .COM
  |morpheus| .COM = |morpheus| .COM

[login]
  krb4_convert = true
  krb4_get_tickets = false
```

After creation of the krb5.conf a keytab file is also required. See below for instructions on how to create a keytab file. http://www.itadmintools.com/2011/07/creating-kerberos-keytab-files.html

**Adding Hyper-V as a Private Cloud**

The Hyper-V host is prepared for Morpheus to communicate with it via WinRM so the Hyper-V private cloud is ready to be configured. Create a group and then create a Morpheus cloud for Hyper-V. Populated the information as show in Figure 1: specific for the environment being configured.
CREATE CLOUD

NAME: San Mateo Hyper-V
LOCATION: San Mateo, CA
DNS DOMAIN: localdomain
VISIBILITY: Public
SCALE PRIORITY: 1

Specifies the priority with which an instance will scale into the cloud. A lower priority number means this cloud integration will take scale precedence over other cloud integrations in the group.

Details

HYPER-V HOST: 192.168.163.141
WORKING PATH: D:\Morpheus
VM PATH: D:\VMs
DISK PATH: D:\VirtualDisks
USERNAME: Administrator
PASSWORD: ************
Note: The working path, vm path, and disk path should be created on the Hyper-V host by the Hyper-V administrator. If these paths are not created they will need to be setup and the Hyper-V settings will need to adjusted to reference them.
Service Plans

A default set of Service Plans are created in Morpheus for the VMware provisioning engine. These Service Plans can be considered akin to AWS Flavors or Openstack Flavors. They provide a means to set predefined tiers on memory, storage, cores, and CPU. Price tables can also be applied to these so estimated cost per virtual machine can be tracked as well as pricing for customers. By default, these options are fixed sizes but can be configured for dynamic sizing. A service plan can be configured to allow a custom user entry for memory, storage, or CPU. To configure this, simply edit an existing Service Plan tied to Hyper-V or create a new one. These are managed from the Admin > Plans & Pricing section.

<table>
<thead>
<tr>
<th>TYPE NAME</th>
<th>CLOUDS</th>
<th>MEMORY</th>
<th>STORAGE</th>
<th>PRICE SETS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory: 1GB, 1 vCPU</td>
<td>Google Labs</td>
<td>1.0GB</td>
<td>0MB</td>
<td></td>
</tr>
<tr>
<td>Memory: 2GB, 2 vCPU</td>
<td>Google Labs</td>
<td>2.0GB</td>
<td>0MB</td>
<td></td>
</tr>
<tr>
<td>Memory: 4GB, 4 vCPU</td>
<td>Google Labs</td>
<td>4.0GB</td>
<td>0MB</td>
<td></td>
</tr>
<tr>
<td>Memory: 8GB, 16 vCPU</td>
<td>Google Labs</td>
<td>8.0GB</td>
<td>0MB</td>
<td></td>
</tr>
<tr>
<td>Memory: 16GB, 32 vCPU</td>
<td>Google Labs</td>
<td>16.0GB</td>
<td>0MB</td>
<td></td>
</tr>
</tbody>
</table>

12.12. Clouds
So far this document has covered how to add the Hyper-V cloud integration and has enabled users the ability to provision virtual machine-based instances via the Add Instance catalog under the Provisioning menu. Another great feature provided by Morpheus out of the box is the ability to use Docker containers and even support multiple containers per Docker host. To do this a Docker Host must first be provisioned into Hyper-V (multiple are needed when dealing with horizontal scaling scenarios).

To provision a Docker Host simply navigate to the Clusters tab of the Cloud detail page or Infrastructure > Clusters section. From there click + ADD CLUSTER to add a Hyper-V Docker Host. A cluster is created when adding Docker hosts, even when only one host is needed.

Morpheus views a Docker host just like any other hypervisor with the caveat being that it is used for running containerized images instead of virtualized ones. Once a Docker Host is successfully provisioned a green checkmark will appear to the right of the host marking it as available for use. In the event of a failure click into the relevant host that failed and an error explaining the failure will be displayed in red at the top.

Some common error scenarios include network connectivity. For a Docker Host to function properly, it must be able to resolve the Morpheus appliance url which can be configured in Admin | Settings. If it is unable to resolve and negotiate with the appliance than the agent installation will fail and provisioning instructions will not be able to be issued to the host.

**12.12.10 IBM Cloud**

IBM Cloud offers a wide set of cloud computing services including compute, storage, database, networking, and more. It is deployed in data centers across the world and its services can scale to meet the needs of small development teams as well as large-scale enterprises. Morpheus integrates with IBM Cloud to offer virtual machine provisioning, brownfield discovery, and lifecycle management.

**Integrating IBM Cloud with Morpheus**

Connecting an IBM Cloud account with Morpheus is a simple process requiring only an API key. You can create an API key from the IBM Cloud web console if you don’t currently have access to one.

1. Navigate to Infrastructure > Clouds
2. Click + ADD
3. Complete the following required fields:
   - **NAME**: A friendly name for the cloud integration in Morpheus
   - **USERNAME**: The name given to the API key you’re using to authenticate the connection
   - **API Key**: The API key value
   - **DATACENTER**: Select the IBM Cloud data center

1. Click NEXT
2. Select a Group for this Cloud
3. Complete the wizard to save the new integration
Once the wizard has completed, the new IBM Cloud integration will appear alongside other Clouds currently available in Morpheus. If you’ve selected to automatically onboard existing resources, those will appear shortly.

IBM Cloud integrations also support a number of advanced options which were not discussed as part of the initial integration set up discussed above. For more information on the advanced options, consult the section below.

**Advanced Options**

**DOMAIN** Specify a default domain for instances provisioned to this Cloud.

**SCALE PRIORITY** Only affects Docker Provisioning. Specifies the priority with which an instance will scale into the cloud. A lower priority number means this cloud integration will take scale precedence over other cloud integrations in the group.

**APPLIANCE URL** Alternate Appliance url for scenarios when the default Appliance URL (configured in admin > settings) is not reachable or resolvable for Instances provisioned in this cloud. The Appliance URL is used for Agent install and reporting.

**TIME ZONE** Configures the time zone on provisioned VM’s if necessary.

**DATACENTER ID** Used for differentiating pricing among multiple datacenters. Leave blank unless prices are properly configured.

**NETWORK MODE** Unmanaged or select a Network Integration (NSX, ACI etc)

**LOCAL FIREWALL** On or Off. Enable to managed Host and VM firewall/IP Table rules (linux only)

**SECURITY SERVER** Security Server setting is for Security Service Integrations such as ACI

**TRUST PROVIDER** Select Internal (Morpheus) or an existing Trust Provider Integration

**STORAGE MODE** Single Disk, LVM or Clustered

**BACKUP PROVIDER** Select Internal Backups (Morpheus) or a Backup Integration
REPLICATION PROVIDER  Sets the default Replication Provider for the Cloud. Select an existing Replication Provider Integration

GUIDANCE  Enable Guidance recommendations on cloud resources.

COSTING  Enable for Morpheus to sync Costing data from the Cloud provider, when available. For on-prem Clouds, enabling costing activates a costing service designed to mirror the live costing experience of public clouds, including invoicing with line items and real-time cost data (Operations > Costing > Invoices). If your organization utilizes reserved instances and you want to pull in related pricing data, select Costing and Reservations. If this is not relevant, select Costing to save money on additional calls to the AWS Cost Explorer API or similar service for other clouds.

DNS INTEGRATION  Records for instances provisioned in this cloud will be added to selected DNS integration.

SERVICE REGISTRY  Services for instances provisioned in this cloud will be added to selected Service Registry integration.

CONFIG MANAGEMENT  Select a Chef, Salt, Ansible or Puppet integration to be used with this Cloud.

CMDB  Select CMDB Integration to automatically update selected CMDB.

CMDB DISCOVERY  When checked, any automatically discovered (unmanaged) servers onboarded into Morpheus from this Cloud will also have CMDB records created for them.

CHANGE MANAGEMENT  Select an existing Change Management Integration to set on the Cloud. ex: Cherwell

AGENT INSTALL MODE

- SSH / WINRM: Morpheus will use SSH or WINRM for Agent install.
- Cloud Init / Unattend (when available): (DEFAULT) Morpheus will utilize Cloud-Init or Cloudbase-Init for agent install when provisioning images with Cloud-Init/Cloudbase-Init installed. Morpheus will fall back on SSH or WINRM if cloud-init is not installed on the provisioned image. Morpheus will also add Agent installation to Windows unattend.xml data when performing Guest Customizations or utilizing sysprepped images.

API PROXY  Set a proxy for outbound communication from the Morpheus Appliance to the Cloud endpoints. Proxies can be added in the Infrastructure > Networks > Proxies tab.

INSTALL AGENT  Enable to have Agent Installation on by default for all provisioning into this Cloud. Disable for Agent Installation to be off by default for all provisioning into this Cloud.

Provisioning Options

PROXY  Set a proxy for inbound communication from Instances to the Morpheus Appliance. Proxies can be added in the Infrastructure > Networks > Proxies tab.

Bypass Proxy for Appliance URL  Enable to bypass proxy settings (if added) for Morpheus Agent communication to the Appliance URL.

NO PROXY  Include a list of IP addresses or name servers to exclude from proxy traversal

Overview

Morpheus KVM is a powerful, cheaper alternative to virtualization when it comes to other hypervisor offerings. It is also very capable of setting up complex shared storage and multiple networks across many hosts. Currently this process is a manual process but will become automated in the coming months. This guide will go over how to configure VLANs on a Morpheus KVM Host.

Getting Started

To get started, the first step is to go ahead and add the KVM host to morpheus and allow morpheus to configure it just like any other kvm host. When provisioning a manual kvm host be sure to enter the proper network interface name for the management network (not the trunk port). For example eno2 could be a management network while eno1 could be the trunk port network that the VLAN’s are going to be on as in this example.

Setting up a VLAN Interface

Before a VLAN can be used by KVM, an interface definition must first be configured for said vlan. In CentOS this is done by defining a network script in /etc/sysconfig/network-scripts.

Note:  It is highly recommended that NM_CONTROLLED is set to NO or NetworkManager is disabled entirely as it tends to get in the way.

If our trunk network is called eno1 we need to make a new script for each VLAN ID we would like to bridge onto. In our example we are going to look at VLAN 211. To do this we need to make a new script called ifcfg-eno1.211 (note the VLAN Id is a suffix to the script name after a period as this is conventional and required).

```
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=none
NAME=eno1.211
DEVICE=eno1.211
ONBOOT=yes
NM_CONTROLLED=no
VLAN=yes
DEVICETYPE=ovs
OVS_BRIDGE=br211
```

There are a few important things to note about this script. Firstly there is a flag called VLAN=yes that enables the kernel tagging of the VLAN. Secondly we have defined an OVS_BRIDGE name. Morpheus utilizes openswitch for its networking which is a very powerful tool used even by Openstack’s Neutron. It supports not just VLANs but VxLAN interacing.

The OVS_BRIDGE name means we also need to define a bridge port script called br211 by making a script called ifcfg-br211:

```
DEVICE=br211
ONBOOT=yes
DEVICETYPE=ovs
```

(continues on next page)
These configurations will enable persistence on these interfaces so that a reboot of the host will retain connectivity to the bridges. Next up, the interfaces need to be brought online. This can be done by restarting all network services but if a typo is made networking could be stuck disabled and access over SSH could be broken. To do this by interface simply run:

```
ifup eno1.211
ifup br211
ovs-vsctl
add-br br211
```

### Defining a LibVirt Network

Now that the bridge interface is defined properly for OVS, it must be defined in LibVirt so that Morpheus will detect the network and KVM can use it properly. By convention, these resource configurations are stored in `/var/morpheus/kvm/config`.

An XML definition must be created to properly define the network. In this case the network is named `public 185.3.48.0.xml`:

```
<network>
  <name>public 185.3.48.0</name>
  <forward mode="bridge"/>
  <bridge name="br211"/>
  <virtualport type="openvswitch"/>
</network>
```

This configuration defines the network name that will be synced into morpheus for selection as well as the type of interface being used (in this case a bridge to the `br211` interface over openvswitch).

Now that this xml specification is defined it must be registered with libvirt via the virsh commands:

```
virsh net-define "public 185.3.48.0.xml"
virsh net-autostart "public 185.3.48.0"
virsh net-start "public 185.3.48.0"
```

Once this is completed, simply refresh the cloud in morpheus and wait for the network to sync into the networks list. Once the network is synced make sure the appropriate settings are applied to it within Morpheus. This includes setting the CIDR, Gateway, Nameservers and if using IP Address Management, the IPAM Pool.
12.12.12 Canonical MAAS

MAAS from Canonical is an open-source server orchestration tool. It’s designed to allow administrators to build a datacenter from on-premises, bare-metal servers where large networks of individual units can be discovered, deployed, and reconfigured.

Integrating MAAS and Morpheus

Integrating MAAS with Morpheus is a simple process requiring the MAAS API URL and API Key. We’ll start by gathering what we need from the MAAS UI, then move back into Morpheus to store the required details.

We can gather the API key by clicking on the username in the upper-right corner of the MAAS UI window. From this preferences page, click on “API keys” as shown in the screenshot:

From the API keys page, select the displayed key and copy it. Alternatively, you can click the copy button in the UI to add the full key to your clipboard. Store this key in an accessible location for a later step.

In addition to the API key, we need the MAAS API URL. As entered in Morpheus, the value will be like the following

12.12. Clouds
example: http://<maas-hostname-or-ip>:5240. We’ll enter the API URL into Morpheus during the next step.

In Morpheus, navigate to the list of integrated Clouds and start a new MAAS Cloud integration:

1. Infrastructure > Clouds
2. Click + ADD
3. Select “MAAS”
4. Click NEXT

On the “CREATE CLOUD” modal, you must at least give a friendly name for the Cloud in Morpheus, MAAS API URL and API KEY. An example is shown below:

Tip: You’ll know the credentials are entered correctly when your list of MAAS resource pools is synced in as you can see in the example screenshot.

Click NEXT and add this new Cloud to an existing Group or create a new Group for it. Once you advanced past the end of the wizard, the Cloud is added and Morpheus begins to inventory (if you’ve opted to inventory when adding the Cloud).
12.12.13 Mac Stadium

Overview

MacStadium is a provider of enterprise-class hosting solutions for Apple Mac infrastructure. It can be used to deploy a hosted private cloud for large-scale CI/CD or even a single Mac mini to test an iOS app. It allows virtualized Mac build machines.

Features

- Virtual Machine Provisioning
- Backups / Snapshots
- Resource Groups
- Datastores and DRS Clusters
- Distributed Switches
- Datacenter / Cluster scoping
- Brownfield VM management and migration
- VMware to VMware migrations
- VMDK/OVF image conversion support
- Hypervisor Remote Console
• Periodic Synchronization
• Veeam Backup Integration
• Lifecycle Management and Resize

On top of all these features, Morpheus also adds additional features to VMware that do not exist out of the box to make it easier to manage in multitenant environments as well as hybrid cloud environments:

• Cloud-Init Support
• VHD to VMDK Image Conversion
• QCOW2 to VMDK Image Conversion
• Multitenancy resource allocation
• Virtual Image management (Blueprints)
• Auto-scaling and recovery

Getting Started

To get started with VMware, simply start by adding a Cloud in the Infrastructure > Clouds section.

To start adding a VMware cloud there will be some things you will need:

vCenter API Url  Typically this is the url to the vCenter web client with a /sdk in the path

Username/Password  A set of credentials with high level access to VMware (ensure the account has Datacenter level access)
Once these fields are entered, some selections will start pre-populating. A cloud integration is scoped to a specific data center, and can optionally be scoped down to a single cluster or even a single resource pool. If the drop downs do not populate, please verify the api url is resolvable, morpheus has access to vCenter on 443, and the provided credentials are correct and the user has sufficient permissions.

Another cool feature provided with the cloud integration is optional Resource Pool scoping. One can choose to allow the cloud to provision into All Resource Pools or a singular Resource Pool. When choosing All, these Resource Pools can be managed from a sub-account and visibility perspective via the Cloud Detail page (multi-tenancy).

The VMWare cloud integration provides a few additional options including allowing users to make host selections or keeping that aspect hidden such that the best host is automatically chosen for the requested provision.

The RPC Mode feature can be configured to allow Morpheus to install its agent on the Guest operating system via either SSH/WinRM or Vmware Tools Guest Process feature. The VMWare tools Guest Execution API can be tricky so it is recommended to use SSH/WinRM if possible. However, if it is not possible for the Appliance to have outbound access to all networks in which VMs are being provisioned to the SSH/WinRM ports (22, 5985 respectively) then Guest Execution is the only option.

The Use VNC console option on the VMware cloud requires special configuration on each ESXI host but allowed hypervisor level remote console support. (See the Advanced Section for details)

When following this add cloud wizard an option will be presented to create a group or add to an existing group. These groups can be given provisioning permission via role based access control. It is normally recommended that groups are organized such that one cloud exists in one group unless the networks are setup such that internal routing is possible between the clouds. This is very useful for bursting, or hybrid cloud configurations.

**Windows Provisioning Tips**

By default when provisioning windows templates, Morpheus performs guest customizations which initiates a sysprep. This resets the Administrator user and password. Morpheus will set the Administrator password from Administration > Settings > Provisioning > Windows Settings > Password.

Users can also set the username on an image as Administrator and enter a different password if unique passwords are required per image.

Guest customizations are required when assigning static IP’s manually or using IP pools. They can be disabled per virtual image advanced settings under Library > Virtual Images > Edit Image > Advanced > Uncheck “Force Guest Customization” if using DHCP. However the SID will not be changed from the source template. In addition, new VM’s will not be able to join a domain that had already been joined by the source template or any other VM’s with that SID.

**Existing Instances**

Morpheus provides several features regarding pulling in existing virtual machines and servers in an environment. Most cloud options contain a checkbox titled ‘Inventory Existing Instances’. When this option is selected, all VMs found within the specified scope of the cloud integration will be scanned periodically and Virtual Machines will be synced into Morpheus. By default these virtual machines are considered ‘unmanaged’ and do not appear in the Provisioning > Instances area but rather Infrastructure > Compute > Virtual Machines. However, a few features are provided with regards to unmanaged instances. They can be assigned to various accounts if using a multitenant master account, however it may be best suited to instead assign the ‘Resource Pool’ to an account and optionally move all servers with regards to that pool (more on this later). A server can also be made into a managed server. During this process remote access is requested and an agent install is performed on the guest operating system. This allows for guest operations regarding log acquisition and stats. If the agent install fails, a server will still be marked as managed and an Instance will be created in Provisioning, however certain features will not function. This includes stats collection and logs.
Note: All Cloud data is resynchronized on a 5 minute interval. This includes Datastores, Resource Pools, Networks, Blueprints, and Virtual Machines.

Service Plans

A default set of Service Plans are created in Morpheus for the VMware provisioning engine. These Service Plans can be considered akin to AWS Flavors or Openstack Flavors. They provide a means to set predefined tiers on memory, storage, cores, and cpu. Price tables can also be applied to these so estimated cost per virtual machine can be tracked as well as pricing for customers. By default, these options are fixed sizes but can be configured for dynamic sizing. A service plan can be configured to allow a custom user entry for memory, storage, or cpu. To configure this, simply edit an existing Service Plan tied to VMware or create a new one. These all can be easily managed from the Admin > Plans & Pricing section.

Virtual Images / Blueprints

Morpheus will automatically take an inventory of all blueprints configured in vCenter and present them as options during provisioning. However, in order for Morpheus to properly provision these virtual machines and provide accurate stats and health of these virtual machines, an agent must be installed during virtual machine startup. This means remote access needs to be granted at the guest operating system level to Morpheus. To properly configure these virtual images, find the relevant images in Library > Virtual Images and edit the entry. On this form, a few options are presented. The first is a check box asking whether or not cloud-init is enabled. If cloud-init is enabled, simply provide the default OS username configured (for Ubuntu the username is ubuntu and for CentOS the username is centos). For those looking
to add cloud-init to existing blueprints Morpheus requires no special configuration and can use the default `cloud.cfg` settings.

A global cloud-init username/password can also be configured per account as well as a keypair via the Admin->Provisioning settings section. The great benefit of utilizing cloud-init is default blueprints do not need common credential sets thereby increasing provisioning security.

Windows systems do not typically support cloud-init. So simply turn this checkbox off and provide the Administrator credentials. It should be noted that these credentials are encrypted in the database. If using WinRM for the RPC Mode instead of VMware tools, a Local or Domain Administrator account credential set can be provided instead.

**Snapshots**

Morpheus allows the ability to create a snapshot of a VM in VMware vCenter. From the instance detail page, simply select Actions > Create Snapshot to begin creation of a new Snapshot. Existing snapshots can be viewed in the BACKUPS tab on the instance detail page. Snapshots taken in vCenter will sync into Morpheus every five minutes. To revert to a previous snapshot, click on the revert icon located on the right side of the Snapshot. Snapshots can be deleted by clicking on the trash can icon.

**Note:** Access to Snapshots can be limited or removed entirely for specific user roles as needed. To edit a role’s Snapshots permissions, go to Administration > Roles > (Your selected role) > Snapshots. Users can be given Full, Read-only, or No access.

**Tagging and Metadata**

As of Morpheus version 4.1.0, tagging support is included for vCenter in addition to the other clouds that have already supported it in past versions. Tags will sync to vCenter from Morpheus and existing tags are also inventoried from vCenter into Morpheus.

**Note:** This feature requires a minimum API version of vCenter 6.5. The API version can be edited by navigating to ‘Infrastructure > Clouds’ and clicking the edit (pencil) button in the row for the relevant cloud. The field is labeled ‘VERSION’.

Tags can be created on-demand when provisioning from the ‘CONFIGURE’ tab of the ‘CREATE INSTANCE’ wizard (Provisioning > Instances). Within the ‘Metadata’ drawer, you will see sets of fields to enter key/value pairs. On creation of the instance, this metadata will be synced into vCenter.

‘Inputs’ from your library can also be exported as metadata for use with vCenter. When adding or editing a new Input (Library > Options > Inputs), simply mark the box labeled ‘EXPORT AS METADATA’. The ‘FIELD NAME’ becomes the tag category in VMware.
Docker

So far this document has covered how to add the VMware cloud integration and has enabled users the ability to provision virtual machine based instances via the Add Instance catalog in Provisioning. Another great feature provided by Morpheus out of the box is the ability to use Docker containers and even support multiple containers per Docker host. To do this a Docker Host must first be provisioned into VMware (multiple are needed when dealing with horizontal scaling scenarios).

To provision a Docker Host simply navigate to the Clusters tab of the Cloud detail page or Infrastructure > Clusters section. From there, click + ADD CLUSTER to add a VMware Docker Host. This host will show up in the Hosts tab next to other ESXi servers that were inventoried by the VMware cloud integration. Morpheus views a Docker host just like any other Hypervisor with the caveat being that it is used for running containerized images instead of virtualized ones. Once a Docker Host is successfully provisioned a green checkmark will appear to the right of the host marking it as available for use. In the event of a failure click into the relevant host that failed and an error explaining the failure will be displayed in red at the top.

Some common error scenarios include network connectivity. For a Docker Host to function properly, it must be able to resolve the Morpheus appliance url which can be configured in Administration > Settings. If it is unable to resolve and negotiate with the appliance than the agent installation will fail and provisioning instructions will not be able to be issued to the host.
Multitenancy

A very common scenario for Managed Service Providers is the need to provide access to VMware resources on a customer by customer basis. With VMware several administrative features have been added to ensure customer resources are properly scoped and isolated. For VMware it is possible to assign specific Networks, Datastores, and Resource Pools to customer accounts or even set the public visibility of certain resources, therefore allowing all sub accounts access to the resource.

Advanced

There are several advanced features provided within Morpheus that can leverage some cool aspects of VMware. One of these features is Remote Console support directly to the hypervisor. To enable this feature a few prerequisites must be met. First, the Morpheus appliance must have network access to the ESXi hosts within VCenter. Secondly, firewall settings need to be adjusted on each ESXi host. This can be done in VSphere under firewall configuration on the host. Simply check the gdbserver option, which will open up the necessary ports (starting at 5900 range).

**Important:** Hypervisor Console for vCenter 6.5 requires Morpheus v3.2.0+

Now that the ESXi hosts are ready to utilize remote console, simply edit the cloud in Morpheus via Infrastructure > Clouds. Check the option that says Enable Hypervisor Console. It is important to note that currently this functionality only works for newly provisioned vm’s provisioned directly via Morpheus. This should change soon however.

It is also possible to import vm snapshots for backup or conversion purposes from VCenter and also an ESXi host. However, this does require that the ESXi host license has an enterprise level license as it will not allow the appliance
to download a virtual image if it is not a paid VMware license.

12.12.14 Nutanix

Overview

Nutanix simplifies datacenter infrastructure by integrating server and storage resources allowing applications to run at scale. Morpheus provides and avenue to enhance the Nutanix resources to allow efficient and seamless deployment of applications as a virtual machine (VM) or as a container on a Docker host.

Features

- Virtual Machine Provisioning
- Containers
- Backups / Snapshots
- Resources Groups
- Migrations
- Auto Scaling
- Load Balancing
- Remote Console
- Periodic Synchronization
- Lifecycle Management and Resize

Morpheus can provide a single pane of glass and self-service portal for managing multiple Nutanix Clusters and allowing the seamless deployment of applications.

Note: Prism Central is not currently supported as a Cloud endpoint target

Getting Started

To get started this a few prerequisites must first be met. The Nutanix cluster should be provisioned and available on the network. Morpheus will look login to the Nutanix cluster with the Nutanix admin credentials and is typically located at the https://fqdn:9440 url.

Adding a Nutanix Cloud

The Nutanix cluster should be available and responding to the https://fqdn:9440 url for authentication by Morpheus.

NAME Name of the Cloud in Morpheus
CODE Unique code used for api/cli, automation and policies.
LOCATION Description field for adding notes on the cloud, such as location.
VISIBILITY For setting cloud permissions in a multi-tenant environment. Not applicable in single tenant environments.
TENANT If Visibility is set to Private, select the Tenant the Cloud resources will assigned to.
**ENABLED**  When disabled, automatic Cloud sync is paused and the Cloud will not be selectable for provisioning.

**AUTOMATICALLY POWER ON VMS**  When enabled, Morpheus will maintain the expected powered on state of managed VM’s and power on any managed VM’s in the cloud that have been shut down for unknown reasons (not powered off by Morpheus) to ensure availability of services.

**Note:**  When “AUTOMATICALLY POWER ON VMS” is enabled, the power state of managed VM’s should be maintained in Morpheus. This setting is not applicable to discovered/unmanaged resources.

**API URL**  URL of the Nutanix Prism API, example: https://10.30.21.220:9440. Prism Central is not currently supported as a Cloud endpoint target

**USERNAME**  Nutanix admin username

**PASSWORD**  Nutanix admin password

**Inventory Existing Instances**  If enabled, existing Virtual Machines will be inventoried and appear as unmanaged Virtual Machines in Morpheus.

**Advanced Options**

**DOMAIN**  Specify a default domain for instances provisioned to this Cloud.

**SCALE PRIORITY**  Only affects Docker Provisioning. Specifies the priority with which an instance will scale into the cloud. A lower priority number means this cloud integration will take scale precedence over other cloud integrations in the group.

**APPLIANCE URL**  Alternate Appliance url for scenarios when the default Appliance URL (configured in admin > settings) is not reachable or resolvable for Instances provisioned in this cloud. The Appliance URL is used for Agent install and reporting.

**TIME ZONE**  Configures the time zone on provisioned VM’s if necessary.

**DATACENTER ID**  Used for differentiating pricing among multiple datacenters. Leave blank unless prices are properly configured.

**NETWORK MODE**  Unmanaged or select a Network Integration (NSX, ACI etc)

**LOCAL FIREWALL**  On or Off. Enable to managed Host and VM firewall/IP Table rules (linux only)

**SECURITY SERVER**  Security Server setting is for Security Service Integrations such as ACI

**TRUST PROVIDER**  Select Internal (Morpheus) or an existing Trust Provider Integration

**STORAGE MODE**  Single Disk, LVM or Clustered

**BACKUP PROVIDER**  Select Internal Backups (Morpheus) or a Backup Integration

**REPLICATION PROVIDER**  Sets the default Replication Provider for the Cloud. Select an existing Replication Provider Integration

**GUIDANCE**  Enable Guidance recommendations on cloud resources.

**COSTING**  Enable for Morpheus to sync Costing data from the Cloud provider, when available. For on-prem Clouds, enabling costing activates a costing service designed to mirror the live costing experience of public clouds, including invoicing with line items and real-time cost data (Operations > Costing > Invoices). If your organization utilizes reserved instances and you want to pull in related pricing data, select Costing and Reservations. If this is not relevant, select Costing to save money on additional calls to the AWS Cost Explorer API or similar service for other clouds.

**DNS INTEGRATION**  Records for instances provisioned in this cloud will be added to selected DNS integration.
SERVICE REGISTRY  Services for instances provisioned in this cloud will be added to selected Service Registry integration.

CONFIG MANAGEMENT  Select a Chef, Salt, Ansible or Puppet integration to be used with this Cloud.

CMDB  Select CMDB Integration to automatically update selected CMDB.

CMDB DISCOVERY  When checked, any automatically discovered (unmanaged) servers onboarded into Morpheus from this Cloud will also have CMDB records created for them.

CHANGE MANAGEMENT  Select an existing Change Management Integration to set on the Cloud. ex: Cherwell

AGENT INSTALL MODE

- SSH / WINRM: Morpheus will use SSH or WINRM for Agent install.
- Cloud Init / Unattend (when available): (DEFAULT) Morpheus will utilize Cloud-Init or Cloudbase-Init for agent install when provisioning images with Cloud-Init/Cloudbase-Init installed. Morpheus will fall back on SSH or WINRM if cloud-init is not installed on the provisioned image. Morpheus will also add Agent installation to Windows unattend.xml data when performing Guest Customizations or utilizing syspreped images.

API PROXY  Set a proxy for outbound communication from the Morpheus Appliance to the Cloud endpoints. Proxies can be added in the Infrastructure > Networks > Proxies tab.

INSTALL AGENT  Enable to have Agent Installation on by default for all provisioning into this Cloud. Disable for Agent Installation to be off by default for all provisioning into this Cloud.

Provisioning Options

PROXY  Set a proxy for inbound communication from Instances to the Morpheus Appliance. Proxies can be added in the Infrastructure > Networks > Proxies tab.

Bypass Proxy for Appliance URL  Enable to bypass proxy settings (if added) for Morpheus Agent communication to the Appliance URL.

NO PROXY  Include a list of IP addresses or name servers to exclude from proxy traversal


Service Plans

A default set of Service Plans are created in Morpheus for the VMware provisioning engine. These Service Plans can be considered akin to AWS Flavors or Openstack Flavors. They provide a means to set predefined tiers on memory, storage, cores, and cpu. Price tables can also be applied to these so estimated cost per virtual machine can be tracked as well as pricing for customers. By default, these options are fixed sizes but can be configured for dynamic sizing. A service plan can be configured to allow a custom user entry for memory, storage, or cpu. To configure this, simply edit an existing Service Plan tied to Nutanix or create a new one. These all can be easily managed from the Admin | Service Plans & Pricing section.
Docker

So far this document has covered how to add the Nutanix cloud integration and has enabled users the ability to provision virtual machine based instances via the Add Instance catalog in Provisioning. Another great feature provided by Morpheus out of the box is the ability to use Docker containers and even support multiple containers per Docker host. To do this a Docker Host must first be provisioned into Nutanix (multiple are needed when dealing with horizontal scaling scenarios).

To provision a Docker Host, simply navigate to the Cloud detail page or Infrastructure > Clusters section. From there click + ADD CLUSTER to add a Nutanix Docker Host. Morpheus views a Docker host just like any other Hypervisor with the caveat being that it is used for running containerized images instead of virtualized ones. Once a Docker Host is successfully provisioned a green checkmark will appear to the right of the host marking it as available for use. In the event of a failure click into the relevant host that failed and an error explaining the failure will be displayed in red at the top.

Some common error scenarios include network connectivity. For a Docker Host to function properly, it must be able to resolve the Morpheus appliance url which can be configured in Admin Settings. If it is unable to resolve and negotiate with the appliance than the agent installation will fail and provisioning instructions will not be able to be issued to the host.

Snapshots

Morpheus allows the ability to create a snapshot of a Nutanix instance. From the instance detail page, simply select Actions > Create Snapshot to begin creation of a new Snapshot. Existing snapshots can be viewed in the BACKUPS tab on the instance detail page. Snapshots taken outside Morpheus will be synced every five minutes. To revert to a previous snapshot, click on the revert icon located on the right side of the Snapshot. Snapshots can be deleted by clicking on the trash can icon.

Note: Access to Snapshots can be limited or removed entirely for specific user roles as needed. To edit a role’s Snapshots permissions, go to Administration > Roles > (Your selected role) > Snapshots. Users can be given Full, Read-only, or No access.

12.12.15 Openstack

Overview

Openstack is becoming a widely used on-premise infrastructure orchestration platform. It has a wide array of contributors and enterprise sponsorships. There are several variations on Openstack as well. Morpheus supports integration with all the various platform offerings and ranges in support all the way back to Openstack Juno. The complete list of compatible versions is listed in our Integration Compatibility table. It leverages the APIs and provides full functionality as a self service portal in front of Openstack.
Features

- Virtual Machine Provisioning
- Backups and Snapshots
- Security Group Management
- Disk Mode support Local/Image (via Ceph)
- Floating IP Assignment support
- Brownfield VM management and Migration
- Lifecycle Management and Resize
- Docker Host management and configuration
- Manila File Services (SFS)
- Object Storage (OBS)
- Network Lifecycle
- LBaaS/Octavia Load Balancing Services

On top of all these features, Morpheus also adds additional features to Openstack that do not exist out of the box to make it easier to manage in multitenant environments as well as hybrid cloud environments:

- Image to QCOW2 Image Conversion
- QCOW2 to RAW Image Conversion
- Multitenancy resource allocation
- Virtual Image management (Blueprints)
- Auto-scaling and recovery
- Instance Cloning
- Morpheus Kubernetes Cluster Deployment

Tip: To allow Morpheus to list Hypervisor Hosts, ensure the Openstack user used for the Cloud Integration has sufficient privileges for os_compute_api:os-hypervisors in /etc/nova/policy.json in Openstack.

Getting Started

OpenStack Clouds are very easy to integrate with Morpheus. First, go to the Infrastructure > Clouds section and click + ADD. Select OpenStack to begin the integration process, most branded flavors of OpenStack will work with this Cloud selection as well.

Warning: Support for OpenStack v2 Identity API has been removed in v5.3.3

Cloud Configuration

NAME  Name of the Cloud in Morpheus
CODE   Unique code used for api/cli, automation and policies.
LOCATION  Description field for adding notes on the cloud, such as location.
VISIBILITY  For setting cloud permissions in a multi-tenant environment. Not applicable in single tenant environments.

TENANT  If Visibility is set to Private, select the Tenant the Cloud resources will assigned to.

ENABLED  When disabled, automatic Cloud sync is paused and the Cloud will not be selectable for provisioning.

AUTOMATICALLY POWER ON VMS  When enabled, Morpheus will maintain the expected power state of managed VMs. Morpheus will power on any managed VMs in the Cloud that have been shut down for unknown reasons (not powered off by Morpheus) to ensure availability of services.

Note:  When “AUTOMATICALLY POWER ON VMS” is enabled, the power state of managed VMs should be maintained in Morpheus. This setting is not applicable to discovered/unmanaged resources.

Details

IDENTITY API URL  v3 Identity endpoint.

DOMAIN ID  For Default domains, Default can be used. For other domain the Domain ID must be entered, not the Domain Name.

PROJECT  Target project

USERNAME  Service Username

PASSWORD  Service user password

OS VERSION  Select Openstack Version. Morpheus supports the latest versions of OpenStack, select the latest version available if your current version is not shown.

IMAGE FORMAT  Select QCOW2, RAW or VMDK Image Type

LB TYPE  Select LB Type for Openstack LB syncing and creation

Inventory Existing Instances  Select for Morpheus to discover and sync existing VM’s

Enable Hypervisor Console  Hypervisor console support for openstack currently only supports novnc. Be sure the novnc proxy is configured properly in your openstack environment. When disabled Morpheus will use ssh and rdp for console connection (vm/host credentials required)

Advanced Options

DOMAIN  Specify a default domain for instances provisioned to this Cloud.

SCALE PRIORITY  Only affects Docker Provisioning. Specifies the priority with which an instance will scale into the cloud. A lower priority number means this cloud integration will take scale precedence over other cloud integrations in the group.

APPLIANCE URL  Alternate Appliance url for scenarios when the default Appliance URL (configured in admin > settings) is not reachable or resolvable for Instances provisioned in this cloud. The Appliance URL is used for Agent install and reporting.

TIME ZONE  Configures the time zone on provisioned VM’s if necessary.

DATACENTER ID  Used for differentiating pricing among multiple datacenters. Leave blank unless prices are properly configured.

NETWORK MODE  Unmanaged or select a Network Integration (NSX, ACI etc)

LOCAL FIREWALL  On or Off. Enable to managed Host and VM firewall/IP Table rules (linux only)

SECURITY SERVER  Security Server setting is for Security Service Integrations such as ACI
Morpheus Documentation

TRUST PROVIDER  Select Internal (Morpheus) or an existing Trust Provider Integration

STORAGE MODE  Single Disk, LVM or Clustered

BACKUP PROVIDER  Select Internal Backups (Morpheus) or a Backup Integration

REPLICATION PROVIDER  Sets the default Replication Provider for the Cloud. Select an existing Replication Provider Integration

GUIDANCE  Enable Guidance recommendations on cloud resources.

COSTING  Enable for Morpheus to sync Costing data from the Cloud provider, when available. For on-prem Clouds, enabling costing activates a costing service designed to mirror the live costing experience of public clouds, including invoicing with line items and real-time cost data (Operations > Costing > Invoices). If your organization utilizes reserved instances and you want to pull in related pricing data, select Costing and Reservations. If this is not relevant, select Costing to save money on additional calls to the AWS Cost Explorer API or similar service for other clouds.

DNS INTEGRATION  Records for instances provisioned in this cloud will be added to selected DNS integration.

SERVICE REGISTRY  Services for instances provisioned in this cloud will be added to selected Service Registry integration.

CONFIG MANAGEMENT  Select a Chef, Salt, Ansible or Puppet integration to be used with this Cloud.

CMDB  Select CMDB Integration to automatically update selected CMDB.

CMDB DISCOVERY  When checked, any automatically discovered (unmanaged) servers onboarded into Morpheus from this Cloud will also have CMDB records created for them.

CHANGE MANAGEMENT  Select an existing Change Management Integration to set on the Cloud. ex: Cherwell

AGENT INSTALL MODE

- SSH / WINRM: Morpheus will use SSH or WINRM for Agent install.
- Cloud Init / Unattend (when available): (DEFAULT) Morpheus will utilize Cloud-Init or Cloudbase-Init for agent install when provisioning images with Cloud-Init/Cloudbase-Init installed. Morpheus will fall back on SSH or WINRM if cloud-init is not installed on the provisioned image. Morpheus will also add Agent installation to Windows unattend.xml data when performing Guest Customizations or utilizing syspreped images.

API PROXY  Set a proxy for outbound communication from the Morpheus Appliance to the Cloud endpoints. Proxies can be added in the Infrastructure > Networks > Proxies tab.

INSTALL AGENT  Enable to have Agent Installation on by default for all provisioning into this Cloud. Disable for Agent Installation to be off by default for all provisioning into this Cloud.

Provisioning Options

PROXY  Set a proxy for inbound communication from Instances to the Morpheus Appliance. Proxies can be added in the Infrastructure > Networks > Proxies tab.

Bypass Proxy for Appliance URL  Enable to bypass proxy settings (if added) for Morpheus Agent communication to the Appliance URL.

NO PROXY  Include a list of IP addresses or name servers to exclude from proxy traversal


Note:  v5.3.3 adds openstack project management which requires additional permissions in openstack:
Most of the information in the dialog can be acquired from the Openstack dashboard, under Project > Access & Security > API Access. The API URL that is needed is the one tied to Identity. The Domain and Project inputs typically correlate to the multitenant domain setup within Openstack (sometimes just left at default) as well as the project name given to instances. Morpheus allows multiple integrations to the same Openstack cluster to be scoped to various domains and projects as needed.

The remaining options help Morpheus determine which API capabilities exist in the selected Openstack environment. Hence the need for the Openstack version and image format. If a newer Openstack cluster is being used then exists in the dropdown, simply select the most recent version in the dropdown and this should function sufficiently until the new version is added.

Tip: Some Openstack environments do not support QCOW2 and force RAW image formats (like Metapod). This is due to some network overhead in Ceph created by using QCOW2. Morpheus keeps two copies of Openstack image templates for this exact purpose.

Saving this cloud integration should perform a verification step and close upon successful completion.

Existing Instances

Morpheus provides several features regarding pulling in existing virtual machines and servers in an environment. Most cloud options contain a checkbox titled ‘Inventory Existing Instances’. When this option is selected, all VMs found within the specified scope of the cloud integration will be scanned periodically and Virtual Machines will be synced into Morpheus.

By default these virtual machines are considered ‘unmanaged’ and do not appear in the Provisioning > Instances area but rather Infrastructure > Compute > Virtual Machines. However, a few features are provided with regards to unmanaged instances. They can be assigned to various accounts if using a multitenant master account, however it may be best suited to instead assign the ‘Resource Pool’ to an account and optionally move all servers with regards to that pool (more on this later).

A server can also be made into a managed server. During this process remote access is requested and an agent install is performed on the guest operating system. This allows for guest operations regarding log acquisition and stats. If the agent install fails, a server will still be marked as managed and an Instance will be created in Provisioning, however certain features will not function. This includes stats collection and logs.
Service Ports

Morpheus consumes the following OpenStack service ports by default as part of its cloud integration. If your OpenStack implementation has been configured to use alternate service ports, these can be overwritten in the Cloud configuration under the Service Endpoints section when adding or editing the Cloud integration.

### Default Service Ports

- **Identity**: 5000
- **Compute**: 8774
- **Image**: 9292
- **Key Manager**: 9311
- **Network**: 9696
- **Volume API v3**: 8776 v3
- **Manila**: 8786

### OpenStack Scalable File Service (SFS)

The Morpheus integration with Openstack Cloud includes the capability to work with Openstack Scalable File Service (SFS). SFS is shared file storage hosted on Openstack Cloud. By integrating Morpheus with Openstack you can discover, create, manage, and delete SFS servers, as well as view and work with the file shares and files contained therein.
SFS Server Discovery and Management

On integrating Openstack Cloud with Morpheus, SFS servers and file shares are discovered automatically after a short time. The server(s) can be viewed in Infrastructure > Storage > Servers. By viewing the server detail page and clicking EDIT, the storage server can be scoped as needed. Administrators can choose to scope to other Openstack Cloud integrations (if more than one relevant integration currently exists), select from synced availability zones, and scope the storage server to specific Tenants if desired.

Additionally, Openstack SFS servers can be created from the storage server list page (Infrastructure > Storage > Servers) directly in Morpheus. Click +ADD to begin and set the storage server type value to “Openstack SFS”. Just like with existing synced SFS servers, those created from Morpheus can be scoped as needed.

SFS File Share Discovery and Management

Discovered file shares will appear among other file shares synced with Morpheus in Infrastructure > Storage > File Shares. Depending on the number of cloud integrations in your Morpheus appliance and the number of cloud integrations available to your user account, this list may be quite large. Using the search bar on this page, we can narrow down the list to only file shares whose names match the search terms.

We can drill into individual file shares by clicking on the hyperlinked name in the list of all integrated file shares. From the file share detail page, a list of files will appear on the files tab. Begin the process of adding a new file by clicking +ADD. The Access tab on the file shares detail page allows users to view and manage ACL rules.

Note: “Failed to load files from storage provider” is present when the Morpheus appliance doesn’t have access to the file share.

New Openstack SFS file shares can also be created directly in Morpheus. From the file shares list page, get started by clicking +ADD. Select the type “Openstack SFS Share”. Set the storage service field to a pre-existing Openstack SFS server. Setting a friendly name for the file share in Morpheus and selecting from synced availability zones is required.
Network and Router Creation

Once an OpenStack Cloud is integrated into Morpheus, new network creation options become available. When adding a new network (Infrastructure > Networks > Networks Tab), a new type labeled “OpenStack Private Network” is available when clicking +ADD. When the user creates this network construct in Morpheus, a layer two subnet is created but it’s not connected to a Virtual Private Cloud (VPC). This is by design as an Internet-routable network is not always desired. Continue on with this section after creating the network to also create a VPC (router).

Create a network

1. Navigate to Infrastructure > Networks
2. Click on the Networks tab
3. Click +ADD
4. Select OpenStack Private Network
5. Complete the modal based on requirements for the new network
6. Click SAVE CHANGES

Create a router

1. Navigate to Infrastructure > Networks
2. Click on the Routers tab
3. Click +ADD
4. Select OpenStack Router
5. Complete the modal based on requirements for the new router
6. Click SAVE CHANGES

When creating a router, it’s helpful to note that the External Network is the floating IP network that has been assigned to the OpenStack project. This network will grant your Instances their routes out to the Internet. The Internal Subnet can be a layer two subnet that you may have created in the previous step. In addition, multiple subnets can be added to the router (VPC) and the IP address on the subnet would be the router’s internal IP address.

Advanced

There are a few advanced features when it comes to provisioning on top of Openstack. Most of these present themselves in the provisioning wizard. This includes OS Volume Type (Local or Volume) which dictates whether the main OS disk is copied and run off the hypervisor or remotely mounted as a volume via Glacier. Some Openstack setups only configure hypervisors with minimal local disks so volume type is needed.

Another option during provisioning is “Assign Floating IP”. This option does exactly what it says and is similar to the feature on the Openstack instance dashboard itself. It should be noted that this will attempt to acquire a floating IP from the project and, if out of capacity, will attempt to increase capacity to the project if the cloud credentials provided have sufficient administrative privileges to do so.
Docker

So far this document has covered how to add the Openstack cloud integration and has described how to provision virtual machine-based Instances via the Add Instance catalog in Provisioning. Another great feature provided by Morpheus out of the box is the ability to work with Docker containers and even support multiple containers per Docker host. To do this, a Docker host must first be provisioned into Openstack (multiple hosts are needed when dealing with horizontal scaling scenarios).

To provision a Docker Host, navigate to Infrastructure > Clusters and click + ADD CLUSTER. Complete the provisioning wizard including selecting the appropriate Group and Cloud. Alternatively, you can navigate to the Clusters tab for a specific Cloud (Infrastructure > Clouds > Specific Cloud detail page > Clusters tab) and begin the process of provisioning a Docker host to that Cloud from there. Once completed, this host will show up in the Hosts sections (Infrastructure > Hosts OR Infrastructure > Clouds > Specific Cloud detail page > Hosts tab). Morpheus views a Docker host just like any other Hypervisor with the caveat being that it is used for running containerized images instead of virtualized ones.

Once a Docker Host is successfully provisioned, a green checkmark will appear to the right of the host marking it as available for use. In the event of a failure, click into the relevant host that failed and an error explaining the failure will be displayed in red at the top.

Some common error scenarios include network connectivity. For a Docker Host to function properly, it must be able to resolve the Morpheus appliance URL which can be configured in Administration > Settings. If it is unable to resolve and negotiate with the appliance, the Morpheus Agent installation will fail and provisioning instructions will not be able to be issued to the host.

12.12.16 Oracle VM

Add an Oracle VM Cloud

Cloud Configuration

NAME  Name of the Cloud in Morpheus

CODE  Unique code used for api/cli, automation and policies.

LOCATION  Description field for adding notes on the cloud, such as location.

VISIBILITY  For setting cloud permissions in a multi-tenant environment. Not applicable in single tenant environments.

TENANT  If Visibility is set to Private, select the Tenant the Cloud resources will assigned to.

ENABLED  When disabled, automatic Cloud sync is paused and the Cloud will not be selectable for provisioning.

AUTOMATICALLY POWER ON VMS  When enabled, Morpheus will maintain the expected power state of managed VMs. Morpheus will power on any managed VMs in the Cloud that have been shut down for unknown reasons (not powered off by Morpheus) to ensure availability of services.

Note:  When “AUTOMATICALLY POWER ON VMS” is enabled, the power state of managed VMs should be maintained in Morpheus. This setting is not applicable to discovered/unmanaged resources.
Details

**API URL**  Oracle VM API URL. ex: https://10.20.30.40:7002/ovm/core/wsapi/rest

**USERNAME**  Oracle VM User

**PASSWORD**  Oracle VM User Password

**REPOSITORY**  Available repositories will auto-populate upon successful authentication with the above credentials. Select appropriate repository for this Cloud.

**SERVER POOL**  Available server pools will auto-populate upon successful authentication with the above credentials. Select appropriate server pool for this Cloud.

**Inventory Existing Instances**  If enabled, existing Virtual Machines will be inventoried and appear as unmanaged Virtual Machines in Morpheus.

The Cloud can now be added to a Group or configured with additional Advanced options.

**Advanced Options**

**DOMAIN**  Specify a default domain for instances provisioned to this Cloud.

**SCALE PRIORITY**  Only affects Docker Provisioning. Specifies the priority with which an instance will scale into the cloud. A lower priority number means this cloud integration will take scale precedence over other cloud integrations in the group.

**APPLIANCE URL**  Alternate Appliance url for scenarios when the default Appliance URL (configured in admin > settings) is not reachable or resolvable for Instances provisioned in this cloud. The Appliance URL is used for Agent install and reporting.

**TIME ZONE**  Configures the time zone on provisioned VM’s if necessary.

**DATACENTER ID**  Used for differentiating pricing among multiple datacenters. Leave blank unless prices are properly configured.

**NETWORK MODE**  Unmanaged or select a Network Integration (NSX, ACI etc)

**LOCAL FIREWALL**  On or Off. Enable to managed Host and VM firewall/IP Table rules (linux only)

**SECURITY SERVER**  Security Server setting is for Security Service Integrations such as ACI

**TRUST PROVIDER**  Select Internal (Morpheus) or an existing Trust Provider Integration

**STORAGE MODE**  Single Disk, LVM or Clustered

**BACKUP PROVIDER**  Select Internal Backups (Morpheus) or a Backup Integration

**REPLICATION PROVIDER**  Sets the default Replication Provider for the Cloud. Select an existing Replication Provider Integration

**GUIDANCE**  Enable Guidance recommendations on cloud resources.

**COSTING**  Enable for Morpheus to sync Costing data from the Cloud provider, when available. For on-prem Clouds, enabling costing activates a costing service designed to mirror the live costing experience of public clouds, including invoicing with line items and real-time cost data (Operations > Costing > Invoices). If your organization utilizes reserved instances and you want to pull in related pricing data, select Costing and Reservations. If this is not relevant, select Costing to save money on additional calls to the AWS Cost Explorer API or similar service for other clouds.

**DNS INTEGRATION**  Records for instances provisioned in this cloud will be added to selected DNS integration.

**SERVICE REGISTRY**  Services for instances provisioned in this cloud will be added to selected Service Registry integration.

**CONFIG MANAGEMENT**  Select a Chef, Salt, Ansible or Puppet integration to be used with this Cloud.
CMDB  Select CMDB Integration to automatically update selected CMDB.

CMDB DISCOVERY  When checked, any automatically discovered (unmanaged) servers onboarded into Morpheus from this Cloud will also have CMDB records created for them.

CHANGE MANAGEMENT  Select an existing Change Management Integration to set on the Cloud. ex: Cherwell

AGENT INSTALL MODE
- SSH / WINRM: Morpheus will use SSH or WINRM for Agent install.
- Cloud Init / Unattend (when available): (DEFAULT) Morpheus will utilize Cloud-Init or Cloudbase-Init for agent install when provisioning images with Cloud-Init/Cloudbase-Init installed. Morpheus will fall back on SSH or WINRM if cloud-init is not installed on the provisioned image. Morpheus will also add Agent installation to Windows unattend.xml data when performing Guest Customizations or utilizing sysprepped images.

API PROXY  Set a proxy for outbound communication from the Morpheus Appliance to the Cloud endpoints. Proxies can be added in the Infrastructure > Networks > Proxies tab.

INSTALL AGENT  Enable to have Agent Installation on by default for all provisioning into this Cloud. Disable for Agent Installation to be off by default for all provisioning into this Cloud.

Provisioning Options

PROXY  Set a proxy for inbound communication from Instances to the Morpheus Appliance. Proxies can be added in the Infrastructure > Networks > Proxies tab.

Bypass Proxy for Appliance URL  Enable to bypass proxy settings (if added) for Morpheus Agent communication to the Appliance URL.

NO PROXY  Include a list of IP addresses or name servers to exclude from proxy traversal


**12.12.17 Oracle Cloud**

Add Oracle Public Cloud

**Important:** A Keypair (both public and private key) must be added to Morpheus with the Public Key in ssh-rsa format. The Public Key in PEM format needs to be added to Oracle Cloud users keys in Oracle Cloud console for authentication.

**Note:** Information on uploading the Public Key and generating Tenancy’s OCID and User’s OCID can be found at https://docs.cloud.oracle.com/iaas/Content/API/Concepts/apisigningkey.htm

**Cloud Configuration**

NAME  Name of the Cloud in Morpheus

CODE  Unique code used for api/cli, automation and policies.

LOCATION  Description field for adding notes on the cloud, such as location.

VISIBILITY  For setting cloud permissions in a multi-tenant environment. Not applicable in single tenant environments.
**TENANT**  If Visibility is set to Private, select the Tenant the Cloud resources will assigned to.

**ENABLED**  When disabled, automatic Cloud sync is paused and the Cloud will not be selectable for provisioning.

**AUTOMATICALLY POWER ON VMS**  When enabled, Morpheus will maintain the expected power state of managed VMs. Morpheus will power on any managed VMs in the Cloud that have been shut down for unknown reasons (not powered off by Morpheus) to ensure availability of services.

**Note:**  When “AUTOMATICALLY POWER ON VMS” is enabled, the power state of managed VMs should be maintained in Morpheus. This setting is not applicable to discovered/unmanaged resources.

### Details

**TENANCY OCID**  The OCID string from *Tenancy Information* section in Oracle Cloud

**USER OCID**  OCID String for the OPC API user

**SELECT KEY PAIR**  Select a keypair added to Morpheus matching the public key added to specified OPC API user

**REGION**  Select the OPC region (populates after successful account authentication)

**COMPARTMENT**  Select Compartment (populates after successful account authentication)

**INVENTORY**  Turn on for Morpheus to discover and sync existing VMs

### Advanced Options

**DOMAIN**  Specify a default domain for instances provisioned to this Cloud.

**SCALE PRIORITY**  Only affects Docker Provisioning. Specifies the priority with which an instance will scale into the cloud. A lower priority number means this cloud integration will take scale precedence over other cloud integrations in the group.

**APPLIANCE URL**  Alternate Appliance url for scenarios when the default Appliance URL (configured in *admin > settings*) is not reachable or resolvable for Instances provisioned in this cloud. The Appliance URL is used for Agent install and reporting.

**TIME ZONE**  Configures the time zone on provisioned VM’s if necessary.

**DATACENTER ID**  Used for differentiating pricing among multiple datacenters. Leave blank unless prices are properly configured.

**NETWORK MODE**  Unmanaged or select a Network Integration (NSX, ACI etc)

**LOCAL FIREWALL**  On or Off. Enable to managed Host and VM firewall/IP Table rules (linux only)

**SECURITY SERVER**  Security Server setting is for Security Service Integrations such as ACI

**TRUST PROVIDER**  Select Internal (Morpheus) or an existing Trust Provider Integration

**STORAGE MODE**  Single Disk, LVM or Clustered

**BACKUP PROVIDER**  Select Internal Backups (Morpheus) or a Backup Integration

**REPLICATION PROVIDER**  Sets the default Replication Provider for the Cloud. Select an existing Replication Provider Integration

**GUIDANCE**  Enable Guidance recommendations on cloud resources.

**COSTING**  Enable for Morpheus to sync Costing data from the Cloud provider, when available. For on-prem Clouds, enabling costing activates a costing service designed to mirror the live costing experience of public clouds, including invoicing with line items and real-time cost data (Operations > Costing > Invoices). If your organization
utilizes reserved instances and you want to pull in related pricing data, select *Costing and Reservations*. If this is not relevant, select *Costing* to save money on additional calls to the AWS Cost Explorer API or similar service for other clouds.

**DNS INTEGRATION**  Records for instances provisioned in this cloud will be added to selected DNS integration.

**SERVICE REGISTRY**  Services for instances provisioned in this cloud will be added to selected Service Registry integration.

**CONFIG MANAGEMENT**  Select a Chef, Salt, Ansible or Puppet integration to be used with this Cloud.

**CMDB**  Select CMDB Integration to automatically update selected CMDB.

**CMDB DISCOVERY**  When checked, any automatically discovered (unmanaged) servers onboarded into Morpheus from this Cloud will also have CMDB records created for them.

**CHANGE MANAGEMENT**  Select an existing Change Management Integration to set on the Cloud. ex: Cherwell

**AGENT INSTALL MODE**

- SSH / WINRM: Morpheus will use SSH or WINRM for Agent install.
- Cloud Init / Unattend (when available): (DEFAULT) Morpheus will utilize Cloud-Init or Cloudbase-Init for agent install when provisioning images with Cloud-Init/Cloudbase-Init installed. Morpheus will fall back on SSH or WINRM if cloud-init is not installed on the provisioned image. Morpheus will also add Agent installation to Windows unattend.xml data when performing Guest Customizations or utilizing syspreped images.

**API PROXY**  Set a proxy for outbound communication from the Morpheus Appliance to the Cloud endpoints. Proxies can be added in the *Infrastructure > Networks > Proxies* tab.

**INSTALL AGENT**  Enable to have Agent Installation on by default for all provisioning into this Cloud. Disable for Agent Installation to be off by default for all provisioning into this Cloud.

**Provisioning Options**

**PROXY**  Set a proxy for inbound communication from Instances to the Morpheus Appliance. Proxies can be added in the *Infrastructure > Networks > Proxies* tab.

**Bypass Proxy for Appliance URL**  Enable to bypass proxy settings (if added) for Morpheus Agent communication to the Appliance URL.

**NO PROXY**  Include a list of IP addresses or name servers to exclude from proxy traversal

**USER DATA (LINUX)**  Add cloud-init user data. Morpheus 4.1.0 and earlier assumes bash syntax. Morpheus 4.1.1 and later supports all User Data formats. Refer to [https://cloudinit.readthedocs.io/en/latest/topics/format.html](https://cloudinit.readthedocs.io/en/latest/topics/format.html) for more information.

**Enable Live Costing for Oracle Public Cloud**

Morpheus version 4.2.1 and higher support live costing data from the Oracle Cloud metering API. In order to authenticate with this API, edit your existing Oracle Cloud account integration or begin the process of newly integrating an account that wasn’t previously consumable in Morpheus (Infrastructure > Clouds > +ADD).

In the advanced options section of the add/edit cloud modal for Oracle Public Cloud, the COSTING KEY and COSTING SECRET fields must be completed to work with metering API data in Morpheus. Unlike the OCI API authentication used to initially integrate Oracle Cloud, the metering API uses token-based authentication. We must access a Client ID and Client Secret value from the Oracle Public Cloud console to complete these fields.
Morpheus Documentation

Navigate to Oracle cloud sign in page, the URL for which is similar to the following example:
https://idcs-00a0xxxxxxxxxxxxx.identity.oraclecloud.com/ui/v1/signin

If you're not redirected to the admin console similar to the one pictured below, log out and replace ‘signin’ at the end of the URL with ‘adminconsole’ as in the following example:
https://idcs-00a0xxxxxxxxxxxxx.identity.oraclecloud.com/ui/v1/adminconsole

You'll immediately be redirected back to the same signin page but in doing that you should be taken to the admin console after authenticating your session once again.

Create a new application and select the type “Confidential Application”.

---

848 Chapter 12. Guides
On the Details tab, enter a “Name” value and click “Next”.

On the Client tab, choose to “Configure this application as a client now” to reveal additional fields. Then, in the Authorization section, mark the boxes for “Client Credentials” and “JWT Assertion”.
In the Token Issuance Policy section, click the “+Add Scope” button. Click the right-facing arrow button in the row for “CloudPortalResourceApp”. Mark the box to give read access for metering and click “Add”.

Click “Next” until the “Finish” button is shown, then click “Finish”.

The Client ID and Client Secret value will be shown at this point. If these values need to be referenced in the future, simply edit the application and go to the Configuration tab. The Client ID and Client Secret are shown in the General Information section.
Back in Morpheus, enter these values in the COSTING KEY and COSTING SECRET fields of the add/edit cloud modal for your Oracle Public Cloud integration. You also need to fill in the IDENTITY SERVICE value. This value can be found in the URL for your Oracle admin console as shown in the image below. It will be in a format `idcs-xxxxxx`.

Save changes to the Cloud.
12.12.18 Open Telekom Cloud

Open Telekom Cloud is an Openstack-based public cloud offering. Morpheus offers a robust integration into OTC and supports many of its features, including those listed in the next section.

Features

- Virtual machine provisioning
- Backups
- Brownfield VM management and migration
- Hypervisor remote console
- Cloud sync
- Lifecycle management and resizing
- Network security group creation
- Network security group management
- Router and network creation
- Load balancer services
- Docker host management and configuration
- Floating IP assignment
- OBS buckets (create, manage, delete, and discovery)

Add an Open Telekom Cloud

Navigate to Infrastructure > Clouds and click + ADD. Scroll to Open Telekom Cloud and click NEXT. Complete the ADD CLOUD modal, the remainder of this guide includes descriptions of the fields presented on this modal with advice on formatting needed values and where certain data can be located.

Cloud Configuration

NAME Name of the Cloud in Morpheus
CODE Unique code used for api/cli, automation and policies.
LOCATION Description field for adding notes on the cloud, such as location.
VISIBILITY For setting cloud permissions in a multi-tenant environment. Not applicable in single tenant environments.
TENANT If Visibility is set to Private, select the Tenant the Cloud resources will assigned to.
ENABLED When disabled, automatic Cloud sync is paused and the Cloud will not be selectable for provisioning.
AUTOMATICALLY POWER ON VMS When enabled, Morpheus will maintain the expected power state of managed VMs. Morpheus will power on any managed VMs in the Cloud that have been shut down for unknown reasons (not powered off by Morpheus) to ensure availability of services.

Note: When “AUTOMATICALLY POWER ON VMS” is enabled, the power state of managed VMs should be maintained in Morpheus. This setting is not applicable to discovered/unmanaged resources.
Details

IDENTITY API URL  The v3 identity API URL, such as https://iam.eu-de.otc.t-systems.com/v3

DOMAIN ID  Note that this is the Domain ID and not the Domain Name. The Domain ID can be found via the CLI by typing openstack domain list. For default domains, “Default” can be used

PROJECT  OTC projects are groupings of resources and can include compute resources, storage or networking. Multiple projects may be nested under your account. Select the project to which Morpheus should onboard from (if desired) and provision

REGION  OTC Region

USERNAME  The username for the OTC service account that Morpheus will use. Ensure this account has sufficient cloud privileges to avoid interruption of work in Morpheus

PASSWORD  The password for the above service account

IMAGE FORMAT  Select QCOW, RAW or VMDK

IMAGE STORE  Set an OBS bucket as a permanent store location for Morpheus virtual images. Users are limited to uploading images of 2GB or less in size if an OBS bucket is not specified here

INVENTORY EXISTING IMAGES  When selected, Morpheus will automatically onboard existing cloud resources which can be converted to managed Instance if desired. View onboarded cloud resources in the Compute Section (Infrastructure > Compute)

ENABLE HYPERVERSOR CONSOLE  Hypervisor console support for Openstack currently only supports novnc. Be sure the novnc proxy is configured properly in your Openstack environment

Service Endpoints

If needed, update the following service endpoints. A complete listing of OTC API endpoints is here.

- COMPUTE SERVICE
- IMAGE SERVICE
- STORAGE SERVICE
- NETWORK SERVICE
- LOAD BALANCER SERVICE
- OBJECT STORAGE SERVICE
- SHARED FILE SYSTEM SERVICE

Advanced Options

DOMAIN  Specify a default domain for instances provisioned to this Cloud.

SCALE PRIORITY  Only affects Docker Provisioning. Specifies the priority with which an instance will scale into the cloud. A lower priority number means this cloud integration will take scale precedence over other cloud integrations in the group.

APPLIANCE URL  Alternate Appliance url for scenarios when the default Appliance URL (configured in admin > settings) is not reachable or resolvable for Instances provisioned in this cloud. The Appliance URL is used for Agent install and reporting.

TIME ZONE  Configures the time zone on provisioned VM’s if necessary.

DATACENTER ID  Used for differentiating pricing among multiple datacenters. Leave blank unless prices are properly configured.
NETWORK MODE  Unmanaged or select a Network Integration (NSX, ACI etc)
LOCAL FIREWALL  On or Off. Enable to managed Host and VM firewall/IP Table rules (linux only)
SECURITY SERVER  Security Server setting is for Security Service Integrations such as ACI
TRUST PROVIDER  Select Internal (Morpheus) or an existing Trust Provider Integration
STORAGE MODE  Single Disk, LVM or Clustered
BACKUP PROVIDER  Select Internal Backups (Morpheus) or a Backup Integration
REPLICATION PROVIDER  Sets the default Replication Provider for the Cloud. Select an existing Replication Provider Integration
GUIDANCE  Enable Guidance recommendations on cloud resources.
COSTING  Enable for Morpheus to sync Costing data from the Cloud provider, when available. For on-prem Clouds, enabling costing activates a costing service designed to mirror the live costing experience of public clouds, including invoicing with line items and real-time cost data (Operations > Costing > Invoices). If your organization utilizes reserved instances and you want to pull in related pricing data, select Costing and Reservations. If this is not relevant, select Costing to save money on additional calls to the AWS Cost Explorer API or similar service for other clouds.
DNS INTEGRATION  Records for instances provisioned in this cloud will be added to selected DNS integration.
SERVICE REGISTRY  Services for instances provisioned in this cloud will be added to selected Service Registry integration.
CONFIG MANAGEMENT  Select a Chef, Salt, Ansible or Puppet integration to be used with this Cloud.
CMDB  Select CMDB Integration to automatically update selected CMDB.
CMDB DISCOVERY  When checked, any automatically discovered (unmanaged) servers onboarded into Morpheus from this Cloud will also have CMDB records created for them.
CHANGE MANAGEMENT  Select an existing Change Management Integration to set on the Cloud. ex: Cherwell
AGENT INSTALL MODE
• SSH / WINRM: Morpheus will use SSH or WINRM for Agent install.
• Cloud Init / Unattend (when available): (DEFAULT) Morpheus will utilize Cloud-Init or Cloudbase-Init for agent install when provisioning images with Cloud-Init/Cloudbase-Init installed. Morpheus will fall back on SSH or WINRM if cloud-init is not installed on the provisioned image. Morpheus will also add Agent installation to Windows unattend.xml data when performing Guest Customizations or utilizing syspreped images.
API PROXY  Set a proxy for outbound communication from the Morpheus Appliance to the Cloud endpoints. Proxies can be added in the Infrastructure > Networks > Proxies tab.
INSTALL AGENT  Enable to have Agent Installation on by default for all provisioning into this Cloud. Disable for Agent Installation to be off by default for all provisioning into this Cloud.
Provisioning Options
PROXY  Set a proxy for inbound communication from Instances to the Morpheus Appliance. Proxies can be added in the Infrastructure > Networks > Proxies tab.
Bypass Proxy for Appliance URL  Enable to bypass proxy settings (if added) for Morpheus Agent communication to the Appliance URL.
NO PROXY  Include a list of IP addresses or name servers to exclude from proxy traversal.

Network and Router Creation

Once an Open Telekom Cloud is integrated into Morpheus, new network creation options become available. When adding a new network (Infrastructure > Networks > Networks Tab), a new type labeled “Open Telekom Private Network” is available when clicking +ADD. When the user creates this network construct in Morpheus, a layer two subnet is created but it’s not connected to a Virtual Private Cloud (VPC). This is by design as an Internet-routable network is not always desired. Continue on with this section after creating the network to also create a VPC (router).

Create a network

1. Navigate to Infrastructure > Networks
2. Click on the Networks tab
3. Click +ADD
4. Select Open Telekom Private Network
5. Complete the modal based on requirements for the new network
6. Click SAVE CHANGES

Create a router

1. Navigate to Infrastructure > Networks
2. Click on the Routers tab
3. Click +ADD
4. Select Open Telekom Router
5. Complete the modal based on requirements for the new router
6. Click SAVE CHANGES

When creating a router, it’s helpful to note that the External Network is the floating IP network that has been assigned to the OTC project. This network will grant your Instances their routes out to the Internet. The Internal Subnet can be a layer two subnet that you may have created in the previous step. In addition, multiple subnets can be added to the router (VPC) and the IP address on the subnet would be the router’s internal IP address.

12.12.19 SCVMM

Requirements

- Access to SCVMM host on port 5985 for Agent installation
- Access to Hyper-V host on port 2179 for hypervisor console access
- Morpheus Agent installation (installed on the target SCVMM host via port 5985 and WinRM)
- User with administrator privileges
Agent Requirement

SCVMM and Hyper-V integrations utilize the Morpheus Agent for communication with the Morpheus appliance, making the Morpheus Agent required. This also means SCVMM and Hyper-V Clouds can only point to one Morpheus Appliance at any given time. If another Morpheus Appliance adds an SCVMM or Hyper-V Cloud that is already managed by another Morpheus Appliance, the Morpheus Agent appliance_url will be updated to point to the new Morpheus appliance_url, and the previous Morpheus Appliance will no longer be able to communicate with the SCVMM Cloud or Hyper-V Cloud until the Agent configuration is updated to point to the previous appliance again. In Morpheus version 4.2.1 and higher, multiple Morpheus clouds can be created by integrating with the same SCVMM host. This allows users to create separate Clouds with different SCVMM Cloud, Host and/or Cluster combinations.

Note: Morpheus only supports integration with standalone SCVMM installations and not high-availability cluster installation at this time.

Add a SCVMM Cloud

1. Navigate to Infrastructure > Clouds
2. Select + CREATE CLOUD, select SCVMM, and then click Next.
3. Enter the following into the Create Cloud modal:

   Note: You will need to open port 5985 in order for Morpheus to communicate to SCVMM. You will also want to make sure the SCVMM Controller has WinRM enabled.

Cloud Configuration

NAME Name of the Cloud in Morpheus
CODE Unique code used for api/cli, automation and policies.
LOCATION Description field for adding notes on the cloud, such as location.
VISIBILITY For setting cloud permissions in a multi-tenant environment. Not applicable in single tenant environments.
TENANT If Visibility is set to Private, select the Tenant the Cloud resources will assigned to.
ENABLED When disabled, automatic Cloud sync is paused and the Cloud will not be selectable for provisioning.
AUTOMATICALLY POWER ON VMS When enabled, Morpheus will maintain the expected power state of managed VMs. Morpheus will power on any managed VMs in the Cloud that have been shut down for unknown reasons (not powered off by Morpheus) to ensure availability of services.

Note: When “AUTOMATICALLY POWER ON VMS” is enabled, the power state of managed VMs should be maintained in Morpheus. This setting is not applicable to discovered/unmanaged resources.

Details

SCVMM HOST IP address or URL of SCVMM host server
USERNAME SCVMM Username, for example: svc.scvmm
PASSWORD SCVMM user Password
**CLOUD**  To scope the SCVMM Integration to a single Cloud, select it from the Cloud dropdown, which populates after establishing communication and authorization over port 5985 using the supplied username and password. To scope to all Clouds, leave the dropdown selection as Select Cloud.

**HOST GROUP**  To scope the SCVMM Integration to a single host group, select a host group from the dropdown list. To scope to all host groups, select All Hosts.

**CLUSTER**  To scope the SCVMM Integration to a single cluster, select a cluster from the dropdown list. To scope to all host groups, select All.

**LIBRARY SHARE**  Select a Library Share to be used with the cloud integration.

**SHARED CONTROLLER**

When creating additional Morpheus clouds that point to an SCVMM host already integrated with this appliance, select the appropriate shared controller value from the dropdown.

**Important:** Only set SHARED CONTROLLER on additional Morpheus clouds and not on the Primary Morpheus SCVMM cloud. Failure to set the SHARED CONTROLLER on secondary Morpheus clouds pointed to the same SCVMM cluster will cause agent comm issues resulting in provisioning failures.

**WORKING PATH**  Path for Morpheus to write to, for example c:\cloud

**DISK PATH**  Path for Virtual Disks, for example c:\virtualdisks

**HIDE HOST SELECTION FROM USERS**  Prevents host selection from appearing in provisioning wizards.

**INVENTORY EXISTING INSTANCES**  Enable for Morpheus to automatically discover existing VMs in the scoped resources.

**ENABLE HYPERVERISOR CONSOLE**  Enable to use VNC Hypervisor Console for Morpheus console connection as opposed to the default SSH and RDP console connection methods. Requires resolution of all Hyper-V host names and access over port 443 from the Morpheus appliance to Hyper-V hosts.

**Advanced Options**

**DOMAIN**  Specify a default domain for instances provisioned to this Cloud.

**SCALE PRIORITY**  Only affects Docker Provisioning. Specifies the priority with which an instance will scale into the cloud. A lower priority number means this cloud integration will take scale precedence over other cloud integrations in the group.

**APPLIANCE URL**  Alternate Appliance url for scenarios when the default Appliance URL (configured in admin > settings) is not reachable or resolvable for Instances provisioned in this cloud. The Appliance URL is used for Agent install and reporting.

**TIME ZONE**  Configures the time zone on provisioned VM’s if necessary.

**DATACENTER ID**  Used for differentiating pricing among multiple datacenters. Leave blank unless prices are properly configured.

**NETWORK MODE**  Unmanaged or select a Network Integration (NSX, ACI etc)

**LOCAL FIREWALL**  On or Off. Enable to managed Host and VM firewall/IP Table rules (linux only)

**SECURITY SERVER**  Security Server setting is for Security Service Integrations such as ACI

**TRUST PROVIDER**  Select Internal (Morpheus) or an existing Trust Provider Integration

**STORAGE MODE**  Single Disk, LVM or Clustered
BACKUP PROVIDER  Select Internal Backups (Morpheus) or a Backup Integration

REPLICATION PROVIDER  Sets the default Replication Provider for the Cloud. Select an existing Replication Provider Integration

GUIDANCE  Enable Guidance recommendations on cloud resources.

COSTING  Enable for Morpheus to sync Costing data from the Cloud provider, when available. For on-prem Clouds, enabling costing activates a costing service designed to mirror the live costing experience of public clouds, including invoicing with line items and real-time cost data (Operations > Costing > Invoices). If your organization utilizes reserved instances and you want to pull in related pricing data, select Costing and Reservations. If this is not relevant, select Costing to save money on additional calls to the AWS Cost Explorer API or similar service for other clouds.

DNS INTEGRATION  Records for instances provisioned in this cloud will be added to selected DNS integration.

SERVICE REGISTRY  Services for instances provisioned in this cloud will be added to selected Service Registry integration.

CONFIG MANAGEMENT  Select a Chef, Salt, Ansible or Puppet integration to be used with this Cloud.

CMDB  Select CMDB Integration to automatically update selected CMDB.

CMDB DISCOVERY  When checked, any automatically discovered (unmanaged) servers onboarded into Morpheus from this Cloud will also have CMDB records created for them.

CHANGE MANAGEMENT  Select an existing Change Management Integration to set on the Cloud. ex: Cherwell

AGENT INSTALL MODE

• SSH / WINRM: Morpheus will use SSH or WINRM for Agent install.

• Cloud Init / Unattend (when available): (DEFAULT) Morpheus will utilize Cloud-Init or Cloudbase-Init for agent install when provisioning images with Cloud-Init/Clocloudbase-Init installed. Morpheus will fall back on SSH or WINRM if cloud-init is not installed on the provisioned image. Morpheus will also add Agent installation to Windows unattend.xml data when performing Guest Customizations or utilizing sysprepped images.

API PROXY  Set a proxy for outbound communication from the Morpheus Appliance to the Cloud endpoints. Proxies can be added in the Infrastructure > Networks > Proxies tab.

INSTALL AGENT  Enable to have Agent Installation on by default for all provisioning into this Cloud. Disable for Agent Installation to be off by default for all provisioning into this Cloud.

Provisioning Options

PROXY  Set a proxy for inbound communication from Instances to the Morpheus Appliance. Proxies can be added in the Infrastructure > Networks > Proxies tab.

Bypass Proxy for Appliance URL  Enable to bypass proxy settings (if added) for Morpheus Agent communication to the Appliance URL.

NO PROXY  Include a list of IP addresses or name servers to exclude from proxy traversal


4. After clicking NEXT, the new Cloud can be added to a Group or configured with additional advanced options.
12.12.20 Softlayer

Add a Softlayer Cloud

Cloud Configuration

NAME  Name of the Cloud in Morpheus
CODE  Unique code used for api/cli, automation and policies.
LOCATION  Description field for adding notes on the cloud, such as location.
VISIBILITY  For setting cloud permissions in a multi-tenant environment. Not applicable in single tenant environments.
TENANT  If Visibility is set to Private, select the Tenant the Cloud resources will assigned to.
ENABLED  When disabled, automatic Cloud sync is paused and the Cloud will not be selectable for provisioning.
AUTOMATICALLY POWER ON VMS  When enabled, Morpheus will maintain the expected power state of managed VMs. Morpheus will power on any managed VMs in the Cloud that have been shut down for unknown reasons (not powered off by Morpheus) to ensure availability of services.

Note:  When “AUTOMATICALLY POWER ON VMS” is enabled, the power state of managed VMs should be maintained in Morpheus. This setting is not applicable to discovered/unmanaged resources.

Details

Username  Softlayer Username
API Key  Softlayer User API Key, accessible in the Softlayer Portal under `Account > Users > View API Key`
Datacenter  Datacenters will auto-populate upon successful authentication with the above credentials. Select appropriate Datacenter for this Cloud.
Object Store  Select the destination Object Store
Inventory Existing Instances  If enabled, existing Softlayer Instances will be inventoried and appear as unmanaged Virtual Machines in Morpheus.

The Cloud can now be added to a Group or configured with additional Advanced options.

Advanced Options

DOMAIN  Specify a default domain for instances provisioned to this Cloud.
SCALE PRIORITY  Only affects Docker Provisioning. Specifies the priority with which an instance will scale into the cloud. A lower priority number means this cloud integration will take scale precedence over other cloud integrations in the group.
APPLIANCE URL  Alternate Appliance url for scenarios when the default Appliance URL (configured in admin > settings) is not reachable or resolvable for Instances provisioned in this cloud. The Appliance URL is used for Agent install and reporting.
TIME ZONE  Configures the time zone on provisioned VM’s if necessary.
DATACENTER ID  Used for differentiating pricing among multiple datacenters. Leave blank unless prices are properly configured.
NETWORK MODE  Unmanaged or select a Network Integration (NSX, ACI etc)
LOCAL FIREWALL  On or Off. Enable to managed Host and VM firewall/IP Table rules (linux only)
SECURITY SERVER  Security Server setting is for Security Service Integrations such as ACI
TRUST PROVIDER  Select Internal (Morpheus) or an existing Trust Provider Integration
STORAGE MODE  Single Disk, LVM or Clustered
BACKUP PROVIDER  Select Internal Backups (Morpheus) or a Backup Integration
REPLICATION PROVIDER  Sets the default Replication Provider for the Cloud. Select an existing Replication Provider Integration
GUIDANCE  Enable Guidance recommendations on cloud resources.
COSTING  Enable for Morpheus to sync Costing data from the Cloud provider, when available. For on-prem Clouds, enabling costing activates a costing service designed to mirror the live costing experience of public clouds, including invoicing with line items and real-time cost data (Operations > Costing > Invoices). If your organization utilizes reserved instances and you want to pull in related pricing data, select Costing and Reservations. If this is not relevant, select Costing to save money on additional calls to the AWS Cost Explorer API or similar service for other clouds.
DNS INTEGRATION  Records for instances provisioned in this cloud will be added to selected DNS integration.
SERVICE REGISTRY  Services for instances provisioned in this cloud will be added to selected Service Registry integration.
CONFIG MANAGEMENT  Select a Chef, Salt, Ansible or Puppet integration to be used with this Cloud.
CMDB  Select CMDB Integration to automatically update selected CMDB.
CMDB DISCOVERY  When checked, any automatically discovered (unmanaged) servers onboarded into Morpheus from this Cloud will also have CMDB records created for them.
CHANGE MANAGEMENT  Select an existing Change Management Integration to set on the Cloud. ex: Cherwell
AGENT INSTALL MODE
  • SSH / WINRM: Morpheus will use SSH or WINRM for Agent install.
  • Cloud Init / Unattend (when available): (DEFAULT) Morpheus will utilize Cloud-Init or Cloudbase-Init for agent install when provisioning images with Cloud-Init/Cloudbase-Init installed. Morpheus will fall back on SSH or WINRM if cloud-init is not installed on the provisioned image. Morpheus will also add Agent installation to Windows unattend.xml data when performing Guest Customizations or utilizing sysprepped images.
API PROXY  Set a proxy for outbound communication from the Morpheus Appliance to the Cloud endpoints. Proxies can be added in the Infrastructure > Networks > Proxies tab.
INSTALL AGENT  Enable to have Agent Installation on by default for all provisioning into this Cloud. Disable for Agent Installation to be off by default for all provisioning into this Cloud.
Provisioning Options
PROXY  Set a proxy for inbound communication from Instances to the Morpheus Appliance. Proxies can be added in the Infrastructure > Networks > Proxies tab.
Bypass Proxy for Appliance URL  Enable to bypass proxy settings (if added) for Morpheus Agent communication to the Appliance URL.
NO PROXY  Include a list of IP addresses or name servers to exclude from proxy traversal
12.12.21 UCS Manager

Overview

The Morpheus UCS Manager Integration enables UCS M B and C Chassis Inventory, VM and Container Host Bare Metal Provisioning, PXE boot with IPMI, Storage Profile, SAN Connection Profile, Server Pool, BIOS Profile, Boot Profile, Maintenance Profile, UUID Pool and Disk Group Profile sync.

Adding UCS Manager Cloud

1. Navigate to Infrastructure > Clouds
2. Select + ADD
3. Select UCS MANAGER from the Clouds list
4. Populate the following:
   
   **Cloud Configuration**
   
   **NAME**  Name of the Cloud in Morpheus
   
   **CODE**  Unique code used for api/cli, automation and policies.
   
   **LOCATION**  Description field for adding notes on the cloud, such as location.
   
   **VISIBILITY**  For setting cloud permissions in a multi-tenant environment. Not applicable in single tenant environments.
   
   **TENANT**  If Visibility is set to Private, select the Tenant the Cloud resources will assigned to.
   
   **ENABLED**  When disabled, automatic Cloud sync is paused and the Cloud will not be selectable for provisioning.
   
   **AUTOMATIcALLY POWER ON VMS**  When enabled, Morpheus will maintain the expected power state of managed VMs. Morpheus will power on any managed VMs in the Cloud that have been shut down for unknown reasons (not powered off by Morpheus) to ensure availability of services.

   **Note:** When “AUTOMATICALLY POWER ON VMS” is enabled, the power state of managed VMs should be maintained in Morpheus. This setting is not applicable to discovered/unmanaged resources.

   **Details**

   **UCS MANAGER**  IP or hostname of UCS Manager

   **USERNAME**  UCS Manager User

   **PASSWORD**  UCS Manager Password

   **ORGANIZATION**
   
   - **EXISTING**  (select)
   
   - **NEW**  (create)
     
     - **ORG NAME**  Enter name for the new Organization

   **SERVER PREFIX**  String provisioned servers will be prefixed with

   **DATA DISK MODE**
   
   - LVM data disk
Morpheus Documentation

- Single Disk

**DATA VOLUME** Defaults to `/dev/sdb` *Check to enable SOFTWARE RAID

**NET INTERFACE** Defaults to eth0

5. Select NEXT

6. Select an existing or create a new Group to add the Cloud to. The Cloud can be added to additional Groups in a Groups Clouds tab.

7. Select NEXT

8. Review and then Select COMPLETE

### 12.12.22 UpCloud

**Overview**

UpCloud is a cloud hosting provider that offers both Linux and Windows virtual machines on their MAXIOPS infrastructure which is billed as I.A.A.S (infrastructure-as-a-service). They have datacenters based in the UK, USA, Germany, Netherlands, Singapore and Finland. Servers can be created a lightning fast 45 seconds with their faster than SSD technology.

**Features**

- Virtual Machine Provisioning
- Containers
- Backups / Snapshots
- Migrations
- Auto Scaling
- Load Balancing
- Remote Console
- Periodic Synchronization
- Lifecycle Management and Resize
- Inventory
- Cloudinit

**Requirements**

An UpCloud User with API, Server and Storage permissions is required.

*To enable API access for a Main Account UpCloud User:*

1. Login to UpCloud
2. Select **My Account > User Accounts**
3. Select **Change** on the target user
4. Check the box for **API connections: Allow API connections from**
5. Under Access Permissions > Allow access to individual servers, check the box for **User has control access to all servers**.

6. Under Access Permissions > Allow control access to individual storages, check the box for **User has control access to all storages**.

7. Save

To Enable API, API, Server and Storage permissions for a SubAccount User:

When creating or editing a Sub Account UpCloud user:

1. Check the box for **API connections: Allow API connections from**

2. Under Access Permissions > Allow access to individual servers, check the box for **User has control access to all servers**.

3. Under Access Permissions > Allow control access to individual storages, check the box for **User has control access to all storages**.

4. Save

**Adding an UpCloud Cloud**

**Configure**

1. Navigate to Infrastructure > Clouds

2. Select **+ Create Cloud** Button

3. Select UpCloud from the Add Cloud modal

4. Select **NEXT**

5. Enter the following:

   **Cloud Configuration**

   **NAME** Name of the Cloud in Morpheus

   **CODE** Unique code used for api/cli, automation and policies.

   **LOCATION** Description field for adding notes on the cloud, such as location.

   **VISIBILITY** For setting cloud permissions in a multi-tenant environment. Not applicable in single tenant environments.

   **TENANT** If Visibility is set to Private, select the Tenant the Cloud resources will assigned to.

   **ENABLED** When disabled, automatic Cloud sync is paused and the Cloud will not be selectable for provisioning.

   **AUTOMATICALLY POWER ON VMS** When enabled, Morpheus will maintain the expected power state of managed VMs. Morpheus will power on any managed VMs in the Cloud that have been shut down for unknown reasons (not powered off by Morpheus) to ensure availability of services.

   **Note:** When “AUTOMATICALLY POWER ON VMS” is enabled, the power state of managed VMs should be maintained in Morpheus. This setting is not applicable to discovered/unmanaged resources.

**Details**

**USERNAME** UpCloud User Account Username
**PASSWORD**  UpCloud User Account Password

**ZONE**  Select UpCloud Datacenter to scope cloud to

**INVENTORY**
- **Off**: Existing UpCloud Servers will not be inventoried in Morpheus
- **Basic**: Existing Servers are inventoried with Power state, Memory and Cores statistics synced.
- **Full**: Existing Servers are inventoried with Power state, Memory and Cores statistics, plus IP Addresses, Storage Info, and Console VNC Information.

**Note**: Full Inventory level recommended. Basic Inventory level can reduce Cloud Sync times when inventorying Datacenters with large amounts of servers. Credentials need to be added by editing the Virtual Machine in order to connect.

The Cloud can now be added to a Group or configured with additional Advanced options.

**Advanced Options**

**DOMAIN**  Specify a default domain for instances provisioned to this Cloud.

**SCALE PRIORITY**  Only affects Docker Provisioning. Specifies the priority with which an instance will scale into the cloud. A lower priority number means this cloud integration will take scale precedence over other cloud integrations in the group.

**APPLIANCE URL**  Alternate Appliance url for scenarios when the default Appliance URL (configured in `admin > settings`) is not reachable or resolvable for Instances provisioned in this cloud. The Appliance URL is used for Agent install and reporting.

**TIME ZONE**  Configures the time zone on provisioned VM’s if necessary.

**DATACENTER ID**  Used for differentiating pricing among multiple datacenters. Leave blank unless prices are properly configured.

**NETWORK MODE**  Unmanaged or select a Network Integration (NSX, ACI etc)

**LOCAL FIREWALL**  On or Off. Enable to managed Host and VM firewall/IP Table rules (linux only)

**SECURITY SERVER**  Security Server setting is for Security Service Integrations such as ACI

**TRUST PROVIDER**  Select Internal (Morpheus) or an existing Trust Provider Integration

**STORAGE MODE**  Single Disk, LVM or Clustered

**BACKUP PROVIDER**  Select Internal Backups (Morpheus) or a Backup Integration

**REPLICATION PROVIDER**  Sets the default Replication Provider for the Cloud. Select an existing Replication Provider Integration

**GUIDANCE**  Enable Guidance recommendations on cloud resources.

**COSTING**  Enable for Morpheus to sync Costing data from the Cloud provider, when available. For on-prem Clouds, enabling costing activates a costing service designed to mirror the live costing experience of public clouds, including invoicing with line items and real-time cost data (Operations > Costing > Invoices). If your organization utilizes reserved instances and you want to pull in related pricing data, select *Costing and Reservations*. If this is not relevant, select *Costing* to save money on additional calls to the AWS Cost Explorer API or similar service for other clouds.

**DNS INTEGRATION**  Records for instances provisioned in this cloud will be added to selected DNS integration.
SERVICE REGISTRY  Services for instances provisioned in this cloud will be added to selected Service Registry integration.

CONFIG MANAGEMENT  Select a Chef, Salt, Ansible or Puppet integration to be used with this Cloud.

CMDB  Select CMDB Integration to automatically update selected CMDB.

CMDB DISCOVERY  When checked, any automatically discovered (unmanaged) servers onboarded into Morpheus from this Cloud will also have CMDB records created for them.

CHANGE MANAGEMENT  Select an existing Change Management Integration to set on the Cloud. ex: Cherwell

AGENT INSTALL MODE

- SSH / WINRM: Morpheus will use SSH or WINRM for Agent install.
- Cloud Init / Unattend (when available): (DEFAULT) Morpheus will utilize Cloud-Init or Cloudbase-Init for agent install when provisioning images with Cloud-Init/Cloudbase-Init installed. Morpheus will fall back on SSH or WINRM if cloud-init is not installed on the provisioned image. Morpheus will also add Agent installation to Windows unattend.xml data when performing Guest Customizations or utilizing syspreped images.

API PROXY  Set a proxy for outbound communication from the Morpheus Appliance to the Cloud endpoints. Proxies can be added in the Infrastructure > Networks > Proxies tab.

INSTALL AGENT  Enable to have Agent Installation on by default for all provisioning into this Cloud. Disable for Agent Installation to be off by default for all provisioning into this Cloud.

Provisioning Options

PROXY  Set a proxy for inbound communication from Instances to the Morpheus Appliance. Proxies can be added in the Infrastructure > Networks > Proxies tab.

Bypass Proxy for Appliance URL  Enable to bypass proxy settings (if added) for Morpheus Agent communication to the Appliance URL.

NO PROXY  Include a list of IP addresses or name servers to exclude from proxy traversal


Group

A Group must be specified or created for the new Cloud to be added to. Clouds can be added to additional Groups or removed from Groups after being created.

- USE EXISTING: Add the new Cloud to an exiting Group in Morpheus.
- CREATE NEW: Creates a new Group in Morpheus and adds the Cloud to the Group.
Review

Confirm all settings are correct and select **COMPLETE**.

The UpCloud Cloud will be added, and Morpheus will perform the initial cloud sync of:

- UpCloud Servers will added as Virtual Machines (if Inventory is enabled)
- UpCloud Templates (My Templates) will sync and be added to Library > Virtual Images.

**Note:** The Console tab will only appear for Inventoried Servers if Inventory Level is set to **Full**

Provisioning to UpCloud

Instances and Apps can be created using the private Images synced from UpCloud or from the Morpheus provided Image Catalog.

Provision a synced Image

Images synced from UpCloud can be provisioned by using:

- The **UPCLOUD** Instance Type and selecting the Image from the Image dropdown in the configure section when provisioning and Instance, App, or creating an App Blueprint.
- Creating custom Library Instance Types and selecting a synced Image when creating a Node Type for the custom Instance Type.

**Important:** Synced images should be configured prior to provisioning by editing the Image in the Library > Virtual Images section.

Provision a Morpheus provided UpCloud Image

Morpheus provides a number of pre-configured Images that are available in the default Morpheus Catalog when provisioning and Instance, App, or creating an App Blueprint. UpCloud Images are included in the following Instance Types in the default Morpheus catalog.

- **ACTIVEMQ**
- **APACHE**
- **CASSANDRA**
- **DEBIAN**
- **ELASTICSEARCH**
- **GRAILS**
- **JAVA**
- **MONGO**
- **MYSQL**
- **NGINX**
• PHP
• RABBITMQ
• REDIS
• OMCAT
• UBUNTU
• WINDOWS
• GRAILS

12.12.23 vCloud Director

Configuration

Add vCD Cloud From Infrastructure > Clouds

1. Navigate to Infrastructure > Clouds
2. Select + ADD
3. Select VCLOUD DIRECTOR from the Clouds list
4. Select NEXT
5. Populate the following:
   Cloud Configuration
   NAME Name of the Cloud in Morpheus
   CODE Unique code used for api/cli, automation and policies.
   LOCATION Description field for adding notes on the cloud, such as location.
   VISIBILITY For setting cloud permissions in a multi-tenant environment. Not applicable in single tenant environments.
   TENANT If Visibility is set to Private, select the Tenant the Cloud resources will assigned to.
   ENABLED When disabled, automatic Cloud sync is paused and the Cloud will not be selectable for provisioning.
   AUTOMATICALLY POWER ON VMS When enabled, Morpheus will maintain the expected power state of managed VMs. Morpheus will power on any managed VMs in the Cloud that have been shut down for unknown reasons (not powered off by Morpheus) to ensure availability of services.

   Note: When “AUTOMATICALLY POWER ON VMS” is enabled, the power state of managed VMs should be maintained in Morpheus. This setting is not applicable to discovered/unmanaged resources.

Details

API URL

vCloud Director API Url Example: https://org.vcd.company.com
USERNAME vCD Organization Administrator or System Administrator User
   • User must have an Organizational Administrator or System Administrator Role
- Username must be in the format of <name>@<org>
- When using a user with the System Administrator role, ensure this user has permission set correctly, such as to view objects created by the organization administrator if needed. Otherwise, things like catalogs and vApps created by the Organization Administrator might not be visible to Morpheus.

**PASSWORD** Password for the user indicated above

**ORGANIZATION** Select Organization. Dropdown populates upon successful authorization.

**VDC** Select VDC. Dropdown populates upon successful authorization.

**API VERSION** Example. 31.0. Note: Full version required. 31 would not be valid, must be xx.x (vCD API versions are strings)

**CATALOG** Optionally select a vCD catalog to store Morpheus artifacts or use the default “morpheus_auto” catalog

**Inventory Existing Instances** If enabled, existing Virtual Machines will be inventoried and appear as unmanaged Virtual Machines in Morpheus.

**Advanced Options**

**DOMAIN** Specify a default domain for instances provisioned to this Cloud.

**SCALE PRIORITY** Only affects Docker Provisioning. Specifies the priority with which an instance will scale into the cloud. A lower priority number means this cloud integration will take scale precedence over other cloud integrations in the group.

**APPLIANCE URL** Alternate Appliance url for scenarios when the default Appliance URL (configured in admin > settings) is not reachable or resolvable for Instances provisioned in this cloud. The Appliance URL is used for Agent install and reporting.

**TIME ZONE** Configures the time zone on provisioned VM’s if necessary.

**DATACENTER ID** Used for differentiating pricing among multiple datacenters. Leave blank unless prices are properly configured.

**NETWORK MODE** Unmanaged or select a Network Integration (NSX, ACI etc)

**LOCAL FIREWALL** On or Off. Enable to managed Host and VM firewall/IP Table rules (linux only)

**SECURITY SERVER** Security Server setting is for Security Service Integrations such as ACI

**TRUST PROVIDER** Select Internal (Morpheus) or an existing Trust Provider Integration

**STORAGE MODE** Single Disk, LVM or Clustered

**BACKUP PROVIDER** Select Internal Backups (Morpheus) or a Backup Integration

**REPLICATION PROVIDER** Sets the default Replication Provider for the Cloud. Select an existing Replication Provider Integration

**GUIDANCE** Enable Guidance recommendations on cloud resources.

**COSTING** Enable for Morpheus to sync Costing data from the Cloud provider, when available. For on-prem Clouds, enabling costing activates a costing service designed to mirror the live costing experience of public clouds, including invoicing with line items and real-time cost data (Operations > Costing > Invoices). If your organization utilizes reserved instances and you want to pull in related pricing data, select Costing and Reservations. If this is not relevant, select Costing to save money on additional calls to the AWS Cost Explorer API or similar service for other clouds.

**DNS INTEGRATION** Records for instances provisioned in this cloud will be added to selected DNS integration.
SERVICE REGISTRY  Services for instances provisioned in this cloud will be added to selected Service Registry integration.

CONFIG MANAGEMENT  Select a Chef, Salt, Ansible or Puppet integration to be used with this Cloud.

CMDB  Select CMDB Integration to automatically update selected CMDB.

CMDB DISCOVERY  When checked, any automatically discovered (unmanaged) servers onboarded into Morpheus from this Cloud will also have CMDB records created for them.

CHANGE MANAGEMENT  Select an existing Change Management Integration to set on the Cloud. ex: Cherwell

AGENT INSTALL MODE

- SSH / WINRM: Morpheus will use SSH or WINRM for Agent install.
- Cloud Init / Unattend (when available): (DEFAULT) Morpheus will utilize Cloud-Init or Cloudbase-Init for agent install when provisioning images with Cloud-Init/Cloudbase-Init installed. Morpheus will fall back on SSH or WINRM if cloud-init is not installed on the provisioned image. Morpheus will also add Agent installation to Windows unattend.xml data when performing Guest Customizations or utilizing syspreped images.

API PROXY  Set a proxy for outbound communication from the Morpheus Appliance to the Cloud endpoints. Proxies can be added in the Infrastructure > Networks > Proxies tab.

INSTALL AGENT  Enable to have Agent Installation on by default for all provisioning into this Cloud. Disable for Agent Installation to be off by default for all provisioning into this Cloud.

Provisioning Options

PROXY  Set a proxy for inbound communication from Instances to the Morpheus Appliance. Proxies can be added in the Infrastructure > Networks > Proxies tab.

Bypass Proxy for Appliance URL  Enable to bypass proxy settings (if added) for Morpheus Agent communication to the Appliance URL.

NO PROXY  Include a list of IP addresses or name servers to exclude from proxy traversal


6. Select NEXT

7. Select an existing or create a new Group to add the Cloud to. The Cloud can be added to additional Groups in a Groups Clouds tab.

8. Select NEXT

9. Review and then Select COMPLETE

How to create vCloud Director templates for Morpheus

To create a Windows Template

Create a new machine in VMware vCenter and install a base version of your preferred Windows build.

1. Apply any service packs / updates to the operating system.

2. Set the Network location to Private the below PowerShell will set the location.
3. Configure WinRM to allow remote management and open the firewall.
   - To do this, under local computer Administrator, open a command prompt and run `winrm quickconfig`

4. Install VMware tools

5. Install .Net at least 4.5

6. Enable remote PowerShell this can be done in PowerShell.
   ```
   Enable-PSremoting
   ```

7. Shutdown the virtual machine and convert to a template.

**Note:** Do not run sysprep

---

**To create a Linux Centos template**

Create a new machine in VMware vCenter and install a base version of your preferred Linux distro build. If you are using cloud init as part of your image you will need to ensure your virtual machine has a cdrom.

1. Before installing the operating system setup a single `ext` or `xfs` partition without a swap disk (This is so that `growpart` can extend the disk. `growpart` currently does not support `lvm`)

2. Install the distro and apply any updates to the operating system and security updates

3. Install cloud-init using command `yum install cloud-init`

4. Install `cloud-utils-growpart` using command `yum install cloud-utils-growpart`

5. Install vmware tools

6. Install git by running `yum install git`

7. `epel-release`

8. `selinux` set to permissive (enforced can cause problems with cloud-init)

**To create a Linux Ubuntu template**

Create a new machine in VMware vCenter and install a base version of your preferred Linux distro build. If you are using cloud init as part of your image you will need to ensure your virtual machine has a cdrom.

1. Before installing the operating system setup a single `ext` partition without a swap disk (This is so that `growpart` can extend the disk. `growpart` currently does not support `lvm`)

2. Install the distro and apply any updates to the operating system and security updates

3. Ensure you have set a root password

4. Install cloud-init by running `sudo apt install cloud-init`

5. Install `cloud-utils-growpart` `sudo apt install cloud-utils`

6. Install desired hypervisor drivers (Virto, Open-VM Tools)

7. Install git by running `sudo apt install git`
8. As Debian 9 includes network manager ensure this is disabled. Change the below file

```
/etc/NetworkManager/NetworkManager.conf
```

to the following:

```
managed=false
```

We also recommend disabling network manager and setting the network adapter to eth0 rather than the automatically assigned name. https://support.morpheusdata.com/hc/en-us/articles/115002881228-Creating-a-CentOS-7-Morpheus-VMware-Image

To import your template into vCloud director you will need to login as either an administrator or organisation administrator.

Once logged into vCloud director you will then need select Manage Organizations and then select your organization.

From within the organisation click on Catalogues > select an existing catalogue or create a new catalogue.

**Note:** Please note once you connect Morpheus to your vCD environment, it will create a catalogue called Auto Morpheus. This is a working catalogue and is ignored by Morpheus when searching for images, so any images in the catalogue will not be synced into Morpheus.

Open the catalogue and select the import template from vCenter and then browse the data stores for your templates. Select your template and the type in a new name and description then check the copy template into vCloud director.

Once you click ok the import process will begin. When the import has completed the template will appear in Morpheus within Library > Virtual Images

If the image does not appear within the virtual images you may need to use the filters to filter the virtual images by the vmware (vmdk / ovf / ova) type.

You may also need to refresh the cloud. To do this go to Infrastructure > Clouds > select the vCloud Director cloud > select Refresh.

### 12.12.24 VMware vCenter

**Overview**

VMware is a very common cloud integration choice supported by Morpheus. They have provided a top notch virtualization solution and one might argue pioneered the virtualization space altogether. As such, many companies utilize this technology and all the features that come with it, so Morpheus covers a broad feature set in vCenter.
Features

- Virtual Machine Provisioning
- Backups / Snapshots
- Resource Groups
- Datastores and DRS Clusters
- Distributed Switches
- Datacenter / Cluster scoping
- Brownfield VM management and migration
- VMware to VMware migrations
- VMDK/OVF image conversion support
- Hypervisor Remote Console
- Periodic Synchronization
- Veeam Backup Integration
- Lifecycle Management and Resize
- Metadata tag sync

On top of all these features, Morpheus also adds additional features to VMware that do not exist out of the box to make it easier to manage in multitenant environments as well as hybrid cloud environments:

- Cloud-Init Support
- VHD to VMDK Image Conversion
- QCOW2 to VMDK Image Conversion
- Multitenancy resource allocation
- Virtual Image management (Blueprints)
- Auto-scaling and recovery

Getting Started

To get started with VMware, simply start by adding a Cloud in the Infrastructure > Clouds section.
To start adding a VMware cloud there will be some things you will need:

**vCenter API Url**  Typically this is the url to the vCenter web client with a /sdk in the path

**Username/Password** A set of credentials with high level access to VMware (ensure the account has Datacenter level access)

Once these fields are entered, some selections will start pre-populating. A cloud integration is scoped to a specific data center, and can optionally be scoped down to a single cluster or even a single resource pool. If the drop downs do not populate, please verify the api url is resolvable, morpheus has access to vCenter on 443, and the provided credentials are correct and the user has sufficient permissions.

Another cool feature provided with the cloud integration is optional **Resource Pool** scoping. One can choose to allow the cloud to provision into All Resource Pools or a singular Resource Pool. When choosing *All*, these Resource Pools can be managed from a sub-account and visibility perspective via the Cloud Detail page (multi-tenancy).

The VMware cloud integration provides a few additional options including allowing users to make host selections or keeping that aspect hidden such that the best host is automatically chosen for the requested provision.

The **RPC Mode** feature can be configured to allow Morpheus to install its agent on the Guest operating system via either SSH/WinRM or Vmware Tools Guest Process feature. The VMware tools Guest Execution API can be tricky so it is recommended to use SSH/WinRM if possible. However, if it is not possible for the Appliance to have outbound access to all networks in which VMs are being provisioned to the SSH/WinRM ports (22, 5985 respectively) then Guest Execution is the only option.

The **Use VNC** console option on the VMware cloud requires special configuration on each ESXI host but allowed hypervisor level remote console support. (See the Advanced Section for details)

When following this add cloud wizard an option will be presented to create a group or add to an existing group. These groups can be given provisioning permission via role based access control. It is normally recommended that groups are
organized such that one cloud exists in one group unless the networks are setup such that internal routing is possible between the clouds. This is very useful for bursting, or hybrid cloud configurations.

**Windows Provisioning Tips**

By default when provisioning windows templates, Morpheus performs guest customizations which initiates a sysprep. This resets the Administrator user and password. Morpheus will set the Administrator password from Administration > Settings > Provisioning > Windows Settings > Password.

Users can also set the username on an image as Administrator and enter a different password if unique passwords are required per image.

Guest customizations are required when assigning static IP’s manually or using IP pools. They can be disabled per virtual image advanced settings under Library > Virtual Images > Edit Image > Advanced > Uncheck “Force Guest Customization” if using DHCP. However the SID will not be changed from the source template. In addition, new VM’s will not be able to join a domain that had already been joined by the source template or any other VM’s with that SID.

**Existing Instances**

Morpheus provides several features regarding pulling in existing virtual machines and servers in an environment. Most cloud options contain a checkbox titled ‘Inventory Existing Instances’. When this option is selected, all VMs found within the specified scope of the cloud integration will be scanned periodically and Virtual Machines will be synced into Morpheus. By default these virtual machines are considered ‘unmanaged’ and do not appear in the Provisioning > Instances area but rather Infrastructure > Compute > Virtual Machines. However, a few features are provided with regards to unmanaged instances. They can be assigned to various accounts if using a multitenant master account, however it may be best suited to instead assign the ‘Resource Pool’ to an account and optionally move all servers with regards to that pool (more on this later). A server can also be made into a managed server. During this process remote access is requested and an agent install is performed on the guest operating system. This allows for guest operations regarding log acquisition and stats. If the agent install fails, a server will still be marked as managed and an Instance will be created in Provisioning, however certain features will not function. This includes stats collection and logs.

**Note:** All Cloud data is resynchronized on a 5 minute interval. This includes Datastores, Resource Pools, Networks, Blueprints, and Virtual Machines.

**Service Plans**

A default set of Service Plans are created in Morpheus for the VMware provisioning engine. These Service Plans can be considered akin to AWS Flavors or Openstack Flavors. They provide a means to set predefined tiers on memory, storage, cores, and cpu. Price tables can also be applied to these so estimated cost per virtual machine can be tracked as well as pricing for customers. By default, these options are fixed sizes but can be configured for dynamic sizing. A service plan can be configured to allow a custom user entry for memory, storage, or cpu. To configure this, simply edit an existing Service Plan tied to VMware or create a new one. These all can be easily managed from the Admin > Plans & Pricing section.
Virtual Images / Blueprints

Morpheus will automatically take an inventory of all blueprints configured in vCenter and present them as options during provisioning. However, in order for Morpheus to properly provision these virtual machines and provide accurate stats and health of these virtual machines, an agent must be installed during virtual machine startup. This means remote access needs to be granted at the guest operating system level to Morpheus. To properly configure these virtual images, find the relevant images in Library > Virtual Images and edit the entry. On this form, a few options are presented. The first is a check box asking whether or not cloud-init is enabled. If cloud-init is enabled, simply provide the default OS username configured (for Ubuntu the username is `ubuntu` and for CentOS the username is `centos`). For those looking to add cloud-init to existing blueprints Morpheus requires no special configuration and can use the default `cloud.cfg` settings.

A global cloud-init username/password can also be configured per account as well as a keypair via the Admin->Provisioning settings section. The great benefit of utilizing cloud-init is default blueprints do not need common credential sets thereby increasing provisioning security.

Windows systems do not typically support cloud-init. So simply turn this checkbox off and provide the `Administrator` credentials. It should be noted that these credentials are encrypted in the database. If using WinRM for the RPC Mode instead of VMware tools, a Local or Domain Administrator account credential set can be provided instead.
Snapshots

Morpheus allows the ability to create a snapshot of a VM in VMware vCenter. From the instance detail page, simply select **Actions > Create Snapshot** to begin creation of a new Snapshot. Existing snapshots can be viewed in the **BACKUPS** tab on the instance detail page. Snapshots taken in vCenter will sync into Morpheus every five minutes. To revert to a previous snapshot, click on the revert icon located on the right side of the Snapshot. Snapshots can be deleted by clicking on the trash can icon.

**Note:** Access to Snapshots can be limited or removed entirely for specific user roles as needed. To edit a role’s Snapshots permissions, go to Administration > Roles > (Your selected role) > Snapshots. Users can be given Full, Read-only, or No access.

Tagging and Metadata

As of Morpheus version 4.1.0, tagging support is included for vCenter in addition to the other clouds that have already supported it in past versions. Tags will sync to vCenter from Morpheus and existing tags are also inventoried from vCenter into Morpheus.

**Note:** This feature requires a minimum API version of vCenter 6.5. The API version can be edited by navigating to ‘Infrastructure > Clouds’ and clicking the edit (pencil) button in the row for the relevant cloud. The field is labeled ‘VERSION’.

Tags can be created on-demand when provisioning from the ‘CONFIGURE’ tab of the ‘CREATE INSTANCE’ wizard (Provisioning > Instances). Within the ‘Metadata’ drawer, you will see sets of fields to enter key/value pairs. On creation of the instance, this metadata will be synced into vCenter.

‘Inputs’ from your library can also be exported as metadata for use with vCenter. When adding or editing a new Input (Library > Options > Inputs), simply mark the box labeled ‘EXPORT AS METADATA’. The ‘FIELD NAME’ becomes the tag category in VMWare.
So far this document has covered how to add the VMware cloud integration and has enabled users the ability to provision virtual machine based instances via the Add Instance catalog in Provisioning. Another great feature provided by Morpheus out of the box is the ability to use Docker containers and even support multiple containers per Docker host. To do this a Docker Host must first be provisioned into VMware (multiple are needed when dealing with horizontal scaling scenarios).

To provision a Docker Host simply navigate to the Clusters tab of the Cloud detail page or Infrastructure > Clusters section. From there, click + ADD CLUSTER to add a VMware Docker Host. This host will show up in the Hosts tab next to other ESXi servers that were inventoried by the VMware cloud integration. Morpheus views a Docker host just like any other Hypervisor with the caveat being that it is used for running containerized images instead of virtualized ones. Once a Docker Host is successfully provisioned a green checkmark will appear to the right of the host marking it as available for use. In the event of a failure click into the relevant host that failed and an error explaining the failure will be displayed in red at the top.

Some common error scenarios include network connectivity. For a Docker Host to function properly, it must be able to resolve the Morpheus appliance url which can be configured in Administration > Settings. If it is unable to resolve and negotiate with the appliance than the agent installation will fail and provisioning instructions will not be able to be issued to the host.
Multitenancy

A very common scenario for Managed Service Providers is the need to provide access to VMware resources on a customer by customer basis. With VMware several administrative features have been added to ensure customer resources are properly scoped and isolated. For VMware it is possible to assign specific Networks, Datastores, and Resource Pools to customer accounts or even set the public visibility of certain resources, therefore allowing all sub accounts access to the resource.

Advanced

There are several advanced features provided within Morpheus that can leverage some cool aspects of VMware. One of these features is Remote Console support directly to the hypervisor. To enable this feature a few prerequisites must be met. First, the Morpheus appliance must have network access to the ESXi hosts within VCenter. Secondly, firewall settings need to be adjusted on each ESXi host. This can be done in VSphere under firewall configuration on the host. Simply check the gdbserver option, which will open up the necessary ports (starting at 5900 range).

Important: Hypervisor Console for vCenter 6.5 requires Morpheus v3.2.0+

Now that the ESXi hosts are ready to utilize remote console, simply edit the cloud in Morpheus via Infrastructure > Clouds. Check the option that says Enable Hypervisor Console. It is important to note that currently this functionality only works for newly provisioned vm’s provisioned directly via Morpheus. This should change soon however.

It is also possible to import vm snapshots for backup or conversion purposes from VCenter and also an ESXi host. However, this does require that the ESXi host license has an enterprise level license as it will not allow the appliance
to download a virtual image if it is not a paid VMware license.

**VMware Permissions**

When integrating VMware vCenter with Morpheus, users must supply credentials for a vCenter account and Morpheus will only have access privileges equal to the integrated account. Many users will choose to use a vCenter administrator account so that Morpheus can freely do any function in vCenter without worrying about hitting access limits. Others, for security reasons, may want to restrict Morpheus only to the minimum permissions it needs to perform its functions. Follow the guide in this section to configure a user with minimal permissions and associate it with the appropriate usage levels before using it to create a Morpheus Cloud integration.

**Create vCenter Users and Roles**

For this example, I’ve added a new local user to be my Morpheus integration user (Menu > Administration > Users and Groups) but any existing user, whether locally-created or sourced from an identity integration (like Active Directory), works fine.

![Users and Groups](image)

The next step is to create a Role (Menu > Administration > Roles). You can edit an existing Role to be sure it has the correct privileges. I’ve opted to create a new role and assign the correct privileges. Below the screenshot, take note of the complete set of required privileges. Once all privileges are set, name the Role (if it’s a new one) and click Finish.
Privileges

Datastore/Datastore Cluster

- Allocate Space
- Browse Datastore
- Low Level file Operations
- Remove File
- Update virtual machine files
- Update virtual machine metadata

Distributed Switch

- Port configuration operation
- Port setting operation

Global

- Log Event
- Manage custom attributes
- Set custom attribute

Network

- Assign Network
- Configure
- Remove

Resource

- Apply recommendation
- Assign vApp to resource pool
• Assign virtual machine to resource pool
• Migrate powered off virtual machine
• Migrate powered on virtual machine

Scheduled task
• Create tasks
• Modify task
• Remove task
• Run task

Tasks
• Create task
• Update task

Virtual Machine
• Configuration (all)
• Guest Operations (all)
• Interaction (all)
• Inventory (all)
• Provisioning (all)
• Service configuration (all)
• Snapshot management (all)
• vSphere Replication (all)

vApp
• Clone
• Export
• Import

vSphere Tagging
• Assign or Unassign vSphere Tag
• Create vSphere Tag
• Create vSphere Tag Category
• Delete vSphere Tag
• Delete vSphere Tag Category
• Edit vSphere Tag
• Edit vSphere Tag Category
• Modify UsedBy Field For Category
• Modify UsedBy Field For Tag
• privilege.InventoryService.Tagging.CreateScope.label
• privilege.InventoryService.Tagging.DeleteScope.label
With the User and Role created, add permissions to associate the User and Role to the appropriate usage constructs. Navigate to the usage construct you wish to work with, navigate to the permissions tab, click the plus (+) button. In the screenshot below, I’m adding the permission for the vCenter usage construct. The complete list of usages and whether or not to mark the propagation box is below the image.

Note: For organization and security purposes, permissions can also be added to folders. This allows Morpheus to see the folders and onboard any resources within them (if desired). Once the vCenter Cloud integration has been created in Morpheus, you can view folders from the Cloud Detail Page (Infrastructure > Clouds > Selected Cloud > Resources Tab). By editing the folder here (Actions > Edit), folders can be set as the “Default” and/or the “Image Target”. When a folder is set as Default, this folder is pre-selected when provisioning new Instances into the Cloud. When a folder is set as the Image Target, Morpheus will look into this folder to onboard VMware images into Morpheus.

**Usage**

**vCenter**

- Non-Propagating

**Datacenter**

- Non-Propagating

**Cluster**

- Non-Propagating

**Host**

- Non-Propagating

**Datastore/Datastore Cluster**

- Propagating

After completing the above steps, all VMware Cloud functionality should be available in Morpheus without running into permissions errors.
Creating a Morpheus VMware Image

Morpheus comes out of the box with a default set of blueprints for use in many modern deployment scenarios. These consist mostly of base operating system images with a few additional adjustments. These adjustments typically include the addition of cloud-init (which is highly recommended to be used in most environments, but not mandatory). However, in many on-premise deployments there are custom image requirements as well as networking requirements. This guide will go over how to create a VMware Images for use within Morpheus.

Creating a Windows Image

Supported Versions


Image Preparation

Create a new machine in VMware vCenter and install a base version of your preferred Windows build. The smaller the VMDK drive, typically the faster you can clone and deploy. Utilizing Morpheus, provisioning and post deploy scripts can expand drives to desired sizing.

1. Ensure VMtools is installed on the operating system.
2. Apply any service packs / updates to the operating system.
3. Configure WinRM to allow remote management and open the firewall. This is optional if using VMtools RPC mode for agent install and Morpheus Agent for guest exec. To enable this, under local computer Administrator, open a command prompt and run

   ```
   winrm quickconfig
   ```

4. Install .Net at least 4.5
5. Ensure Windows Firewall will allow WinRM connections.
6. Shutdown the virtual machine and convert to a template.

**Note:** WinRM is not required and is used as a fallback when using vmtools guest exec and customizations

**Note:** Morpheus will sysprep images based on the “Force Guest Customizations” flag under the Virtual Image’s settings when using DHCP. Ensure a sysprep has not been performed on the template if this flag is enabled or if using Static IPs/IP Pools when provisioning, which will always use Guest Customizations and trigger a sysprep.
Creating a CentOS/RHEL 7 Image

Create a new virtual machine in VMware vCenter and install a base version of your preferred Linux distro build. If you are using cloud init as part of your image you will need to ensure your virtual machine has a cdrom.

1. Before installing the operating system setup a single ext or xfs partition without a swap disk (This is so that growpart can extend the disk. growpart currently does not support lvm)
2. Install the distro and apply any updates to the operating system and security updates
3. Install cloud-init using command yum install cloud-init
4. Install cloud-utils-growpart using command yum install cloud-utils-growpart
5. Install open-vm-tools using command yum install open-vm-tools
6. Install git by running yum install git
7. Install epel-release repo using command yum install epel-release
8. selinux set to permissive (enforced can cause problems with cloud-init) sudo vi /etc/selinux/config

Cloud-Init

To get started with a base CentOS image we first install cloud-init. This is a relatively simple process using yum:

```bash
yum -y install epel-release
yum -y install git wget ntp curl cloud-init dracut-modules-growroot
rpm -qa kernel | sed 's/^kernel-//' | xargs -I {} dracut -f /boot/initramfs-{}.img {}
```

There are two parts to this yum installation. We are first ensuring some core dependencies are installed for automation as well as cloud-init. git for example is installed for use by ansible playbook automation down the line and is therefore optional if not using ansible. The dracut-modules-growroot is responsible for resizing the root partition upon first boot to match the virtual disk size that was potentially adjusted during provisioning.

A great benefit to using cloud-init is credentials don’t have to be locked into the blueprint. It is advisable, within Morpheus, to configure the default cloud-init user that gets created when the vm boots automatically by cloud-init. This is located in Administration > Settings > Provisioning, within the Cloud-Init Settings section.

Network Interfaces

A slightly annoying change with centOS 7 is that the network interfaces have changed naming convention. You may notice when running ifconfig that the primary network interface is set to something like ens2344 or some other random number. This naming is dynamic typically by hardware id and we don’t want this to fluctuate when provisioning the blueprint in various VMware environments. Fortunately, there is a way to turn this functionality off and restore the interface back to eth0.

Firstly we need to adjust our bootloader to disable interface naming like this.

```bash
sed -i -e 's/quiet/quiet net.ifnames=0 biosdevname=0/' /etc/default/grub
grub2-mkconfig -o /boot/grub2/grub.cfg
```

The above command adds a few arguments to the kernel args list (namely net.ifnames=0 and biosdevname=0. It may be useful to view the /etc/default/grub file and ensure these settings were indeed applied.

The next step is to adjust the network-scripts in centOS. we need to ensure we have a file called /etc/sysconfig/network-scripts/ifcfg-eth0

Below is a script that we run on our packer builds to prepare the machines network configuration files.
This script tries to ensure there is a new ifcfg-eth0 config created to replace the old ens config file. Please do verify this config exists after running. If it does not you will have to be sure to build one on your own.

```
TYPE=Ethernet
DEVICE=eth0
NAME=eth0
ONBOOT=yes
NM_CONTROLLED="no"
BOOTPROTO="dhcp"
DEFROUTE=yes
```

Creating a CentOS/RHEL 8 Image

Create a new virtual machine in VMware vCenter and install a base version of your preferred Linux build. You must be running ESXi 6.7 Update 2 or later.

Prepare The New CentOS 8/RHEL 8 Image

1. Install epel-release: `yum -y install epel-release` (This step is not necessary for RHEL)
2. Install git, wget, curl, cloud-init, cloud-utils-growpart, and open-vm-tools: `yum -y install git wget curl cloud-init cloud-utils-growpart open-vm-tools`
3. Update: `yum -y update`
4. Finally run: `rpm -qa kernel | sed 's/^kernel-//' | xargs -I {} dracut -f /boot/initramfs-{}.img {}`

SELinux Settings

If allowed by your internal IT policies, set SELinux to permissive to avoid potential issues with cloud-init down the road.

1. Edit the following: `vi /etc/selinux/config`
2. Make the following change: `setenforce 0`
Network Interfaces

Run the following to rename the network NIC. Values inside angle brackets should be filled in with the appropriate value for your environment (ex. <varname>):

1. `sed -i -e 's/quiet/quiet net.ifnames=0 biosdevname=0/ /etc/default/grub`
2. `grub2-mkconfig -o /boot/grub2/grub.cfg` (location may be different, could be located at `/boot/efi/EFI/centos/grub.cfg`)
3. `ifdown <orginal-nic>`
4. `mv /etc/sysconfig/network-scripts/<orginal-nic> /etc/sysconfig/network-scripts/ifcfg-eth0` (this changes name/device to eth0)
5. Edit `ifcfg-eth0` and change the NAME to eth0
6. `bash -c 'echo NM_CONTROLLED="no" >> /etc/sysconfig/network-scripts/ifcfg-eth0'`
7. `ip link set <orginal-nic> down`
8. `ip link set <orginal-nic> name eth0`
9. `ip link set eth0 up`
10. `ifup eth0`

Final VMWare Tasks

1. Detach any install media
2. Shutdown the VM
3. Convert the VM to template on the Morpheus side
4. Refresh the Morpheus Cloud to allow the new template to sync

Creating an Ubuntu 20.04 Image

Download the Ubuntu 20.04 ISO from Canonical, and upload the base image to vCetner. Then, create a new virtual machine in vCenter.

Note: Since we’ll include cloud-init with our image, we will need to ensure the virtual machine has a cdrom. Select the Ubuntu 20.04 ISO we just downloaded from the CD/DVD drive dropdown menu when creating the new virtual machine.

Before installing the operating system, set up a single ext partition without a swap disk. Then, continue on installing Ubuntu making the following selections during the setup process:

- Update to the latest installer if a later version is available
- Use the entire disk and deselect the option to set up the disk as an LVM group
- Configure an account and set a password
- Opt to install OpenSSH Server
- Other optional packages aren’t needed for this basic Ubuntu image
Complete the installation process and reboot the machine. Update the package list and apply any upgrades:

```
apt-get update
apt-get upgrade
```

Change the network interface to `eth0` by editing `/etc/default/grub`. The line `GRUB_CMDLINE_LINUX=""` should be edited to `GRUB_CMDLINE_LINUX="net.ifnames=0 biosdevname=0"`.

Update GRUB:

```
update-grub
```

Update the 70-persistent-net.rules file:

```
cat << EOF > /etc/udev/rules.d/70-persistent-net.rules
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", ATTR{dev_id}=="0x0", ATTR{type}=="1", NAME="eth0"
EOF
```

Remove `subiquity-disable-cloudinit-networking.cfg` as cloud-init will skip network configuration if it’s present:

```
rm -f /etc/cloud/cloud.cfg.d/subiquity-disable-cloudinit-networking.cfg
```

Update 99-pve.cfg:

```
cat << EOF > /etc/cloud/cloud.cfg.d/99-pve.cfg
datasource_list: [ConfigDrive, NoCloud]
EOF
```

Remove Netplan files, they will not be regenerated if they exist:

```
rm -f /etc/netplan/00-installer-config.yaml
rm -f /etc/netplan/50-cloud-init.yaml
```

Run cloud-init clean:

```
cloud-init clean
```

Next, reboot the system and confirm the network interface is labeled `eth0` once the machine comes back up. Then, clear BASH history for root. The history entry has a copy in the memory and it will flush back to the file when you log out. You can avoid this with the following command:

```
cat /dev/null > ~/.bash_history && history -c && exit
```

Shutdown the system:

```
shutdown -h now
```

Convert the VM to a template in vCenter before moving back to Morpheus to onboard the image and use it to begin building your provisioning library.
Gotyas

SELinux can cause issues with cloud-init when in enforced mode. It may be advisable to set this to permissive unless it is mandatory within your organization to use an enforced SELinux configuration. If that is the case please see the documentation for the cloud_init_t security policies.

Network Manager will also prevent the required restart of the Network Service when assigning static IP’s. Disable Network Manager when possible or Static IP assignment may not work until the Network Service is restarted manually.

A Note on Proxies

Proxy configurations are known to vary in some organizations and makes building a base blueprint a little more difficult. In order to fully configure proxies a few environment variables must be set in the /etc/environment file (This can be done automatically in a default user-data script for cloud-init as well in edit cloud).

```
http_proxy="http://myproxyaddress:8080"
https_proxy="http://myproxyaddress:8080"
ftp_proxy="http://myproxyaddress:8080"
no_proxy=127.0.0.1,localhost,applianceUrl
https_no_proxy=127.0.0.1,localhost,applianceUrl
```

**Important:** It is very important to properly set the no_proxy list (applianceUrl) should be replaced with the actual appliance url. In future releases, morpheus plans to automatically take care of this.

**Note:** If using cloud-init agent install mode these settings need to be set in the custom Cloud-Init User data section of “Edit Cloud” or “Edit Virtual Image”

**Important:** If using this virtual machine as a docker host, proxy settings must also be configured in the docker config. See Docker guides for instructions on how to properly set this. If necessary this can be wrapped in a task automation workflow for your own use.

12.12.25 VMware Fusion

**Add a VMware Fusion Cloud**

1. Navigate to Infrastructure > Clouds
2. Select + CREATE CLOUD, select VMware Fusion, and then click Next.
3. Enter the following into the Create Cloud modal:

   **Cloud Configuration**
   - **NAME** Name of the Cloud in Morpheus
   - **CODE** Unique code used for api/cli, automation and policies.
   - **LOCATION** Description field for adding notes on the cloud, such as location.
   - **VISIBILITY** For setting cloud permissions in a multi-tenant environment. Not applicable in single tenant environments.
TENANT If Visibility is set to Private, select the Tenant the Cloud resources will assigned to.

ENABLED When disabled, automatic Cloud sync is paused and the Cloud will not be selectable for provisioning.

AUTOMATICALLY POWER ON VMS When enabled, Morpheus will maintain the expected power state of managed VMs. Morpheus will power on any managed VMs in the Cloud that have been shut down for unknown reasons (not powered off by Morpheus) to ensure availability of services.

Note: When “AUTOMATICALLY POWER ON VMS” is enabled, the power state of managed VMs should be maintained in Morpheus. This setting is not applicable to discovered/unmanaged resources.

Details

VMWARE FUSION HOST IP or URL of VMware Fusion Host
WORKING PATH Existing folder Morpheus will write to on Host
USERNAME Host Username
PASSWORD Host Password
BRIDGE NAME Will auto-populate upon successful authentication with the Fusion Host (E.X. ‘EN0: ETHERNET’)

4. The Cloud can now be added to a Group or configured with additional Advanced options.

Advanced Options

DOMAIN Specify a default domain for instances provisioned to this Cloud.
SCALE PRIORITY Only affects Docker Provisioning. Specifies the priority with which an instance will scale into the cloud. A lower priority number means this cloud integration will take scale precedence over other cloud integrations in the group.
APPLIANCE URL Alternate Appliance url for scenarios when the default Appliance URL (configured in admin > settings) is not reachable or resolvable for Instances provisioned in this cloud. The Appliance URL is used for Agent install and reporting.
TIME ZONE Configures the time zone on provisioned VM’s if necessary.
DATACENTER ID Used for differentiating pricing among multiple datacenters. Leave blank unless prices are properly configured.
NETWORK MODE Unmanaged or select a Network Integration (NSX, ACI etc)
LOCAL FIREWALL On or Off. Enable to managed Host and VM firewall/IP Table rules (linux only)
SECURITY SERVER Security Server setting is for Security Service Integrations such as ACI
TRUST PROVIDER Select Internal (Morpheus) or an existing Trust Provider Integration
STORAGE MODE Single Disk, LVM or Clustered
BACKUP PROVIDER Select Internal Backups (Morpheus) or a Backup Integration
REPLICATION PROVIDER Sets the default Replication Provider for the Cloud. Select an existing Replication Provider Integration
GUIDANCE Enable Guidance recommendations on cloud resources.
COSTING Enable for Morpheus to sync Costing data from the Cloud provider, when available. For on-prem Clouds, enabling costing activates a costing service designed to mirror the live costing experience of public clouds, including invoicing with line items and real-time cost data (Operations > Costing > Invoices). If your organization
utilizes reserved instances and you want to pull in related pricing data, select Costing and Reservations. If this is not relevant, select Costing to save money on additional calls to the AWS Cost Explorer API or similar service for other clouds.

DNS INTEGRATION  Records for instances provisioned in this cloud will be added to selected DNS integration.

SERVICE REGISTRY  Services for instances provisioned in this cloud will be added to selected Service Registry integration.

CONFIG MANAGEMENT  Select a Chef, Salt, Ansible or Puppet integration to be used with this Cloud.

CMDB  Select CMDB Integration to automatically update selected CMDB.

CMDB DISCOVERY  When checked, any automatically discovered (unmanaged) servers onboarded into Morpheus from this Cloud will also have CMDB records created for them.

CHANGE MANAGEMENT  Select an existing Change Management Integration to set on the Cloud. ex: Cherwell

AGENT INSTALL MODE

• SSH / WINRM: Morpheus will use SSH or WINRM for Agent install.
• Cloud Init / Unattend (when available): (DEFAULT) Morpheus will utilize Cloud-Init or Cloudbase-Init for agent install when provisioning images with Cloud-Init/Cloudbase-Init installed. Morpheus will fall back on SSH or WINRM if cloud-init is not installed on the provisioned image. Morpheus will also add Agent installation to Windows unattend.xml data when performing Guest Customizations or utilizing sysprepped images.

API PROXY  Set a proxy for outbound communication from the Morpheus Appliance to the Cloud endpoints. Proxies can be added in the Infrastructure > Networks > Proxies tab.

INSTALL AGENT  Enable to have Agent Installation on by default for all provisioning into this Cloud. Disable for Agent Installation to be off by default for all provisioning into this Cloud.

Provisioning Options

PROXY  Set a proxy for inbound communication from Instances to the Morpheus Appliance. Proxies can be added in the Infrastructure > Networks > Proxies tab.

Bypass Proxy for Appliance URL  Enable to bypass proxy settings (if added) for Morpheus Agent communication to the Appliance URL.

NO PROXY  Include a list of IP addresses or name servers to exclude from proxy traversal


12.12.26 Xen Server

Add a Xen Server Cloud

1. Navigate to Infrastructure > Clouds
2. Select + CREATE CLOUD, select Xen, and then click Next.
3. Enter the following into the Create Cloud modal:

   Cloud Configuration

   NAME  Name of the Cloud in Morpheus
   CODE  Unique code used for api/cli, automation and policies.
LOCATION Description field for adding notes on the cloud, such as location.

VISIBILITY For setting cloud permissions in a multi-tenant environment. Not applicable in single tenant environments.

TENANT If Visibility is set to Private, select the Tenant the Cloud resources will assigned to.

ENABLED When disabled, automatic Cloud sync is paused and the Cloud will not be selectable for provisioning.

AUTOMATICALLY POWER ON VMS When enabled, Morpheus will maintain the expected power state of managed VMs. Morpheus will power on any managed VMs in the Cloud that have been shut down for unknown reasons (not powered off by Morpheus) to ensure availability of services.

Note: When “AUTOMATICALLY POWER ON VMS” is enabled, the power state of managed VMs should be maintained in Morpheus. This setting is not applicable to discovered/unmanaged resources.

Details

API URL IP or URL of Xen Host. ex: xenserver.domain.com

CUSTOM PORT Port for non standard xen server clouds

USERNAME Xen Host Username

PASSWORD Xen Host Password

Inventory Existing Instances If enabled, existing Virtual Machines will be inventoried and appear as unmanaged Virtual Machines in Morpheus.

4. The Cloud can now be added to a Group or configured with additional Advanced options.

Advanced Options

DOMAIN Specify a default domain for instances provisioned to this Cloud.

SCALE PRIORITY Only affects Docker Provisioning. Specifies the priority with which an instance will scale into the cloud. A lower priority number means this cloud integration will take scale precedence over other cloud integrations in the group.

APPLIANCE URL Alternate Appliance url for scenarios when the default Appliance URL (configured in admin > settings) is not reachable or resolvable for Instances provisioned in this cloud. The Appliance URL is used for Agent install and reporting.

TIME ZONE Configures the time zone on provisioned VM’s if necessary.

DATACENTER ID Used for differentiating pricing among multiple datacenters. Leave blank unless prices are properly configured.

NETWORK MODE Unmanaged or select a Network Integration (NSX, ACI etc)

LOCAL FIREWALL On or Off. Enable to managed Host and VM firewall/IP Table rules (linux only)

SECURITY SERVER Security Server setting is for Security Service Integrations such as ACI

TRUST PROVIDER Select Internal (Morpheus) or an existing Trust Provider Integration

STORAGE MODE Single Disk, LVM or Clustered

BACKUP PROVIDER Select Internal Backups (Morpheus) or a Backup Integration

REPLICATION PROVIDER Sets the default Replication Provider for the Cloud. Select an existing Replication Provider Integration

GUIDANCE Enable Guidance recommendations on cloud resources.
COSTING  Enable for Morpheus to sync Costing data from the Cloud provider, when available. For on-prem Clouds, enabling costing activates a costing service designed to mirror the live costing experience of public clouds, including invoicing with line items and real-time cost data (Operations > Costing > Invoices). If your organization utilizes reserved instances and you want to pull in related pricing data, select Costing and Reservations. If this is not relevant, select Costing to save money on additional calls to the AWS Cost Explorer API or similar service for other clouds.

DNS INTEGRATION  Records for instances provisioned in this cloud will be added to selected DNS integration.

SERVICE REGISTRY  Services for instances provisioned in this cloud will be added to selected Service Registry integration.

CONFIG MANAGEMENT  Select a Chef, Salt, Ansible or Puppet integration to be used with this Cloud.

CMDB  Select CMDB Integration to automatically update selected CMDB.

CMDB DISCOVERY  When checked, any automatically discovered (unmanaged) servers onboarded into Morpheus from this Cloud will also have CMDB records created for them.

CHANGE MANAGEMENT  Select an existing Change Management Integration to set on the Cloud. ex: Cherwell

AGENT INSTALL MODE

- SSH / WINRM: Morpheus will use SSH or WINRM for Agent install.
- Cloud Init / Unattend (when available): (DEFAULT) Morpheus will utilize Cloud-Init or Cloudbase-Init for agent install when provisioning images with Cloud-Init/Cloudbase-Init installed. Morpheus will fallback on SSH or WINRM if cloud-init is not installed on the provisioned image. Morpheus will also add Agent installation to Windows unattend.xml data when performing Guest Customizations or utilizing sysprepped images.

API PROXY  Set a proxy for outbound communication from the Morpheus Appliance to the Cloud endpoints. Proxies can be added in the Infrastructure > Networks > Proxies tab.

INSTALL AGENT  Enable to have Agent Installation on by default for all provisioning into this Cloud. Disable for Agent Installation to be off by default for all provisioning into this Cloud.

Provisioning Options

PROXY  Set a proxy for inbound communication from Instances to the Morpheus Appliance. Proxies can be added in the Infrastructure > Networks > Proxies tab.

Bypass Proxy for Appliance URL  Enable to bypass proxy settings (if added) for Morpheus Agent communication to the Appliance URL.

NO PROXY  Include a list of IP addresses or name servers to exclude from proxy traversal


12.12.27 Creating a CentOS 7 Morpheus Image

Overview

Morpheus comes out of the box with a default set of blueprints for use in many modern deployment scenarios. These consist mostly of base operating system images with a few additional adjustments. These adjustments typically include the addition of cloud-init (which is highly recommended to be used in most environments, but not mandatory). However, in many on-premise deployments there are custom image requirements as well as networking requirements. This guide will go over how to create a base CentOS 7 Image for use within Morpheus.
Creating a CentOS 7 Morpheus VMware Image

VMWare

When running in VMWare it is highly recommended that VMware Tools be installed. Without it, Morpheus will have difficulty assessing the host ip address and performing some additional automation tasks for the operating system.

Cloud-Init

To get started with a base CentOS image we first install cloud-init. This is a relatively simple process using yum:

```bash
yum -y install epel-release
yum -y install git wget ntp curl cloud-init dracut-modules-growroot
rpm -qa kernel | sed 's/^kernel-//' | xargs -I {} dracut -f /boot/initramfs-{}.img {}
```

There are two parts to this yum installation. We are first ensuring some core dependencies are installed for automation as well as cloud-init. git for example is installed for use by ansible playbook automation down the line and is therefore optional if not using ansible. The dracut-modules-growroot is responsible for resizing the root partition upon first boot to match the virtual disk size that was potentially adjusted during provisioning.

A great benefit to using cloud-init is credentials don’t have to be locked into the blueprint. It is advisable, within Morpheus, to configure the default cloud-init user that gets created when the vm boots automatically by cloud-init. This is located in the Cloud-Init Settings section at Administration > Settings > Provisioning.

Network Interfaces

A slightly annoying change with centOS 7 is that the network interfaces have changed naming convention. You may notice when running ifconfig that the primary network interface is set to something like ens2344 or some other random number. This naming is dynamic typically by hardware id and we don’t want this to fluctuate when provisioning the blueprint in various VMware environments. Fortunately, there is a way to turn this functionality off and restore the interface back to eth0.

Firstly we need to adjust our bootloader to disable interface naming like this.

```bash
sed -i -e 's/quiet/quiet net.ifnames=0 biosdevname=0/" /etc/default/grub
grub2-mkconfig -o /boot/grub2/grub.cfg
```

The above command adds a few arguments to the kernel args list (namely net.ifnames=0 and biosdevname=0. It may be useful to view the /etc/default/grub file and ensure these settings were indeed applied.

The next step is to adjust the network-scripts in centOS. we need to ensure we have a file called /etc/sysconfig/network-scripts/ifcfg-eth0

Below is a script that we run on our packer builds to prepare the machines network configuration files.

```bash
export iface_file=$(basename "$(find /etc/sysconfig/network-scripts/ -name 'ifcfg*' -not -name 'ifcfg-lo' | head -n 1)")
export iface_name=${iface_file:6}
echo $iface_file
echo $iface_name
sudo mv /etc/sysconfig/network-scripts/$iface_file /etc/sysconfig/network-scripts/ --ifcfg-eth0
sudo sed -i -e "s/$iface_name/eth0/" /etc/sysconfig/network-scripts/ifcfg-eth0
sudo bash -c 'echo NM_CONTROLLED="no" >> /etc/sysconfig/network-scripts/ifcfg-eth0'
```
Morpheus Documentation

This script tries to ensure there is a new ifcfg-eth0 config created to replace the old ens config file. Please do verify this config exists after running. If it does not you will have to be sure to build one on your own.

```plaintext
TYPE=Ethernet
DEVICE=eth0
NAME=eth0
ONBOOT=yes
NM_CONTROLLED="no"
BOOTPROTO="dhcp"
DEFROUTE=yes
```

Gotyas

SELinux can cause issues with cloud-init when in enforced mode. It may be advisable to set this to permissive unless it is mandatory within your organization to use an enforced SELinux configuration. If that is the case please see the documentation for the cloud_init_t security policies.

Network Manager will also prevent the required restart of the Network Service when assigning static IP’s. Disable Network Manager when possible or Static IP assignment may not work until the Network Service is restarted manually.

A Note on Proxies

Proxy configurations are known to vary in some organizations and makes building a base blueprint a little more difficult. In order to fully configure proxies a few environment variables must be set in the `/etc/environment` file (This can be done automatically in a default user-data script for cloud-init as well in edit cloud).

```plaintext
http_proxy="http://myproxyaddress:8080"
https_proxy="http://myproxyaddress:8080"
ftp_proxy="http://myproxyaddress:8080"
no_proxy=127.0.0.1,localhost,applianceUrl
https_no_proxy=127.0.0.1,localhost,applianceUrl
```

**Important:** It is very important to properly set the no_proxy list (applianceUrl) should be replaced with the actual appliance url. In future releases, morpheus plans to automatically take care of this.

**Note:** If using cloud-init agent install mode these settings need to be set in the custom Cloud-Init User data section of “Edit Cloud” or “Edit Virtual Image”

**Important:** If using this virtual machine as a docker host, proxy settings must also be configured in the docker config. See Docker guides for instructions on how to properly set this. If necessary this can be wrapped in a task automation workflow for your own use.
12.12.28 Morpheus Cloud Capability Coverage

<table>
<thead>
<tr>
<th>Cloud Integration</th>
<th>Ubuntu</th>
<th>CentOS</th>
<th>Debian</th>
<th>Linux Guest Cust</th>
<th>Cloud Init</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>Alibaba</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>Azure</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Cloud Limited</td>
</tr>
<tr>
<td>Digital Ocean</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>Google Cloud</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>Huawei</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>Hyperv</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>IBM Cloud / Softlayer</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>KVM</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>No/Yes</td>
</tr>
<tr>
<td>Nutanix</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>Openstack</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>Oracle Cloud</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>OVM</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>OTC</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>SCVMM</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>NO</td>
<td>Yes</td>
</tr>
<tr>
<td>Upcloud</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>VCD</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Vmware</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Xen</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

12.13 Containers

12.13.1 Docker Registry

Overview

Without any additional configuration Morpheus can provision images from Docker’s public hub at https://hub.docker.com/ using their public api at https://index.docker.io/v1/

However, many organizations maintain private Docker registries for security measures. Additional public and private Docker registries can be added to Morpheus.

Adding a Docker Registry Integration

1. Navigate to Administration > Integrations
2. Click “New Integration”
3. Select the Docker Repository Type
4. Add the following:
   - **Name** Name for the Registry in Morpheus
   - **Repository url** Docker Registry url or IP address
   - **Username** Username if private registry
Password  Password if private registry

5. Save Changes

Note: You must either have signed certificates for your registry or configure your docker host(s) to accept insecure registries

Provisioning an Instance from Docker Registry

Docker images from the Integrated Registry can be provisioned using the generic *Docker* Instance Type, or by adding images to Node Types for custom Library Instance Types.

12.14 Deployment

12.14.1 Git

Authentication

Add a private Github or Git repository. Authentication can be handled by supplying any one of the following:

- Username and password
- Access token
- Key pair

Note: Git and Github integrations can be authenticated over HTTPS with a username and password or with an access token. They are authenticated over SSH by providing a key pair. In previous versions of Morpheus, Git (not Github)
integrations could only be authenticated over SSH.

Key pairs are stored in Morpheus and selected from a dropdown menu when needed. To add a key pair to Morpheus:

1. Generate an SSH key pair, or use an existing SSH key pair.
2. Navigate to Infrastructure > Keys & Certs
3. Select + ADD
4. Enter both the Public and Private keys
5. Click SAVE CHANGES

### 12.15 DNS

#### 12.15.1 AWS Route53

**Overview**

Morpheus integrates directly with Amazon Route 53 to automatically create DNS entries for Instances provisioned to a configured Cloud or Group. Morpheus also syncs in Route 53 Domains for easy selection while provisioning, or setting as the default Domain on a Cloud or Network.

**Add Route 53 Integration**

Route 53 can be added in the Administration or Infrastructure sections:

1. In Administration > Integrations, select + New Integration
2. In Infrastructure > Networks > Services, select Add Service
3. Provide the following:
   - **TYPE** Route 53
   - **NAME** Name for the Integration in Morpheus
   - **REGION** AWS Region for the Integration
   - **ACCESS KEY** AWS User IAM Access Key
   - **SECRET KEY** AWS User IAM Secret Key
4. Once saved the Integration will be added and visible in both Administration > Integrations and Infrastructure > Networks > Services

**Note:** All fields can be edited after saving.
Domains

Once the integration is added, Route 53 Domains will sync and listed under Infrastructure > Networks > Domains.

Note: Default Domains can be set on Networks and Clouds, and can be selected when provisioning. Additional configuration options are available by editing a domain in Networks > Domains.

Configuring Route 53 with Clouds and Groups

DNS Integrations are available in the DNS Integration dropdown in Cloud and Group settings. Morpheus will register Instances with the DNS provider when provisioned into a Cloud or Group with a DNS Integration added.

Add DNS Integration to a Cloud

1. In Infrastructure > Clouds edit the target Cloud.
2. Expand the Advanced Options section.
3. In the DNS Integration dropdown, select an available DNS Integration.
4. Save Changes

Add DNS Integration to a Group

1. In Infrastructure > Groups select the target Group.
2. Select the Edit button for the Group
3. Expand the Advanced Options section.
4. In the DNS Integration dropdown, select an available DNS Integration.
5. Save Changes

Note: Instances provisioned into a Cloud or Group with a DNS Integration added will be registered as instance-name.domain with the DNS Provider during provisioning, and de-registered at teardown.

12.15.2 Microsoft DNS

Overview

Morpheus integrates directly with Microsoft DNS to automatically create DNS entries for Instances provisioned to a configured Cloud or Group. Morpheus also syncs in Microsoft DNS Domains for easy selection while provisioning, or setting as the default Domain on a Cloud or Network.
Add Microsoft DNS Integration

**Important:** The Morpheus Microsoft DNS integration works over http/5985. If you have turned off the http listener on 5985 and only enabled https/5986 it will fail.

Microsoft DNS can be added in the *Administration* or *Infrastructure* sections:

1. In *Administration > Integrations*, select *+ New Integration*
2. In *Infrastructure > Networks > Services*, select *Add Service*
3. Provide the following:
   - **TYPE** Microsoft DNS
   - **NAME** Name for the Integration in Morpheus
   - **DNS SERVER** IP or resolvable hostname of DNS server *morpheus* will connect to. If using a jump box, specify the IP or resolvable hostname of the jump box here, and the main DNS Server in the **COMPUTER NAME** field below.
   - **USERNAME** DNS provider username
   - **PASSWORD** DNS provider user password
   - **COMPUTER NAME** If the DNS SERVER specified is not the main DNS server but rather a jump box, enter the Computer Name of the main DNS Server here. If the DNS SERVER specified above is the main DNS server and not a jump box, leave **COMPUTER NAME** blank.
   - **CREATE POINTERS** Enabled to create A records during provisioning
4. Once saved, the Integration will be added and visible in both *Administration > Integrations* and *Infrastructure > Networks > Services*

**Note:** All fields can be edited after saving.

Domains

Once the integration is added, Microsoft DNS Domains will sync and listed under *Infrastructure > Networks > Domains*.

**Note:** Default Domains can be set on Networks and Clouds, and can be selected when provisioning. Additional configuration options are available by editing a domain in *Networks > Domains*
Configuring Microsoft DNS with Clouds and Groups

DNS Integrations are available in the DNS Integration dropdown in Cloud and Group settings. Morpheus will register Instances with the DNS provider when provisioned into a Cloud or Group with a DNS Integration added. To take full advantage of the Morpheus Microsoft DNS integration, a service account in the Admins group is not required. However, an account must have the following minimum access to use all features:

- Read, Create, and Delete rights on objects
- Belongs to the local group WinRMRemoteWMIUsers
- WinRM Quickconfig must be run on the DNS server
- CIMv2 needs access according to instructions in our KnowledgeBase

Add DNS Integration to a Cloud

1. In Infrastructure > Clouds edit the target Cloud.
2. Expand the Advanced Options section.
3. In the DNS Integration dropdown, select an available DNS Integration.
4. Save Changes

Add DNS Integration to a Group

1. In Infrastructure > Groups select the target Group.
2. Select the Edit button for the Group
3. Expand the Advanced Options section.
4. In the DNS Integration dropdown, select an available DNS Integration.
5. Save Changes

Note: Instances provisioned into a Cloud or Group with a DNS Integration added will be registered as instance-name.domain with the DNS Provider during provisioning, and de-registered at teardown.

12.15.3 PowerDNS

Overview

Morpheus integrates directly with PowerDNS to automatically create DNS entries for Instances provisioned to a configured Cloud or Group. Morpheus also syncs in PowerDNS Domains for easy selection while provisioning, or setting as the default Domain on a Cloud or Network.
Add PowerDNS Integration

PowerDNS can be added in the Administration or Infrastructure sections:

1. In Administration > Integrations, select + New Integration
2. In Infrastructure > Networks > Services, select Add Service
3. Provide the following:
   - **TYPE**: PowerDNS
   - **NAME**: Name for the Integration in Morpheus
   - **API HOST**: URL of PowerDNS API. Example: http://10.30.20.10:8081
   - **Token**: PowerDNS API Token
   - **Version**: PowerDNS API Version
4. Once saved, the Integration will be added and visible in both Administration > Integrations and Infrastructure > Networks > Services

**Note**: All fields can be edited after saving.

Domains

Once the integration is added, PowerDNS Domains will sync and listed under Infrastructure > Networks > Domains.

**Note**: Default Domains can be set on Networks and Clouds, and can be selected when provisioning. Additional configuration options are available by editing a domain in Networks > Domains.

Configuring PowerDNS with Clouds and Groups

DNS Integrations are available in the DNS Integration dropdown in Cloud and Group settings.

Morpheus will register Instances with the DNS provider when provisioned into a Cloud or Group with a DNS Integration added.

Add DNS Integration to a Cloud

1. In Infrastructure > Clouds edit the target Cloud.
2. Expand the Advanced Options section.
3. In the DNS Integration dropdown, select an available DNS Integration.
4. Save Changes
Add DNS Integration to a Group

1. In Infrastructure > Groups select the target Group.
2. Select the Edit button for the Group
3. Expand the Advanced Options section.
4. In the DNS Integration dropdown, select an available DNS Integration.
5. Save Changes

Note: Instances provisioned into a Cloud or Group with a DNS Integration added will be registered as instance-name.domain with the DNS Provider during provisioning, and de-registered at teardown.

12.16 Identity Management

12.16.1 Active Directory

Overview

Active Directory is Microsoft’s primary authentication service widely used in Enterprise organizations and even via Microsoft’s cloud services. While Active Directory also supports LDAP protocol support (which Morpheus can integrate with as well), the main Active Directory integration can also be utilized. It is even possible to map Active Directory groups to equivalent Roles within Morpheus. Morpheus will connect over port 389 for non-secure LDAP and port 636 for secure LDAP.

Note: To use Active Directory, a valid / trusted SSL certificate must be in place on the Active Directory services (self signed will not work).

Adding an Active Directory Integration

1. Navigate to Administration > Tenants
2. Select a Tenant
3. Select IDENTITY SOURCES
4. Select + IDENTITY SOURCE
5. Choose “Active Directory”
6. Populate the following:
   - Name  Unique name for authentication type.
   - AD Server  Hostname or IP address of AD Server.
   - Domain  Domain name of AD Domain.
   - Binding Username  Service account username for bind user.
   - Binding Password  Password for bind service account.
   - Required Group  The AD group users must be in to have access (optional)
Default Role The default role a user is assigned if no group is listed under AD user that maps under Role Mappings section.

Service Account Holder This is the admin account type in Morpheus and an AD group can be created and populated to a user that this role should be assigned. Roles are assigned dynamically based on group membership.

ENABLE ROLE MAPPING PERMISSION When selected, Tenant users with appropriate rights to view and edit Roles will have the ability to set role mapping for the Identity Source integration. This allows the Tenant user to edit only the role mappings without viewing or potentially editing the Identity Source configuration.

MANUAL ROLE ASSIGNMENT When selected, administrators can manually edit Roles for users created through this identity source integration from the user detail page (Administration > Users > Selected user).

Note: For more on Identity Source role mapping permissions, see the associated guide in our KnowledgeBase.

1. Select SAVE CHANGES.

Now allowed AD users can login to Morpheus via their Active Directory credentials and a User will be automatically generated to Morpheus with matching metadata and mapped Role permissions.

Note: Only the username is required with password, not the username@domain.

Note: Sub-tenant Morpheus API authentication for Active Directory generated users is not currently supported.

12.16.2 SAML Integration

Overview

The Morpheus SAML identity source integration allows customers to add user SSO to Morpheus, authenticated by external login SAML providers.
Adding a SAML Integration

To add a SAML integration:

1. Navigate to Administration > Tenants
2. Select a tenant.
3. Select IDENTITY SOURCES in the Tenant detail page
4. Select + ADD IDENTITY SOURCE.
5. Select SAML (external login) from the TYPE field
6. Add a Name and optional Description for the SAML integration
There are 3 sections with fields that need to be populated depending on the desired configuration:

- SAML Configuration
- Role Mappings
- User Attribute Names

**SAML Configuration**

**LOGIN REDIRECT URL** This is the SAML endpoint Morpheus will redirect to when a user signs into Morpheus via SAML.

**LOGOUT POST URL** The url morpheus will post to when a SAML user log out of Morpheus to log out of the SAML provider as well.

**SIGNING PUBLIC KEY** Add the X.509 Certificate public key from the SAML provider.
Role Mappings

DEFAULT ROLE  Role a saml user will be assigned by default when no role is mapped

ROLE ATTRIBUTE NAME  The name of the attribute filed that will map to morpheus roles, such a MemberOf

REQUIRED ROLE ATTRIBUTE VALUE  Role attribute value that a user must be assigned/a member of to be authorized, such as group or role in the SAML SP.

ENABLE ROLE MAPPING PERMISSION  When selected, Tenant users with appropriate rights to view and edit Roles will have the ability to set role mapping for the Identity Source integration. This allows the Tenant user to edit only the role mappings without viewing or potentially editing the Identity Source configuration.

MANUAL ROLE ASSIGNMENT  When selected, administrators can manually edit Roles for users created through this identity source integration from the user detail page (Administration > Users > Selected user).

Note:  For more on Identity Source role mapping permissions, see the associated guide in our KnowledgeBase.

The rest of the Role Mapping Fields will be the existing Roles in morpheus with a Role Attribute Value field.

User Attribute Names

GIVEN NAME ATTRIBUTE NAME  SAML SP field value to map to Morpheus user First Name

SURNAME ATTRIBUTE NAME  SAML SP field value to map to Morpheus user Last Name

EMAIL ATTRIBUTE NAME  SAML SP field value to map to Morpheus user email address
### Identity Source

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TYPE</strong></td>
<td>SAML (Beta)</td>
</tr>
<tr>
<td><strong>ACTIVE</strong></td>
<td>Yes</td>
</tr>
<tr>
<td><strong>NAME</strong></td>
<td>SAML</td>
</tr>
<tr>
<td><strong>DESCRIPTION</strong></td>
<td>onelogin SAML</td>
</tr>
</tbody>
</table>

### SAML Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LOGIN REDIRECT URL</strong></td>
<td><a href="https://morpheusdata-dev.onelogin.com/trust/saml2/http-">https://morpheusdata-dev.onelogin.com/trust/saml2/http-</a></td>
</tr>
<tr>
<td></td>
<td><a href="https://morpheusdata-dev.onelogin.com/trust/saml2/http-">https://morpheusdata-dev.onelogin.com/trust/saml2/http-</a></td>
</tr>
<tr>
<td></td>
<td>Do not include SAMLRequest parameter</td>
</tr>
<tr>
<td><strong>LOGOUT POST URL</strong></td>
<td><a href="https://morpheusdata-dev.onelogin.com/trust/saml2/http-">https://morpheusdata-dev.onelogin.com/trust/saml2/http-</a></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SIGNING PUBLIC KEY</strong></td>
<td>MIIEFzCCAv-gAvlBAglUayYdMuoxBTGcaJARainhrJwWQwDQYJKcZIhvcNAQEF</td>
</tr>
</tbody>
</table>

### Role Mappings

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DEFAULT ROLE</strong></td>
<td>System Admin</td>
</tr>
<tr>
<td><strong>ROLE ATTRIBUTE NAME</strong></td>
<td>MemberOf</td>
</tr>
<tr>
<td><strong>REQUIRED ROLE ATTRIBUTE VALUE</strong></td>
<td>dev</td>
</tr>
<tr>
<td><strong>LEGACY ACCOUNT ADMIN</strong></td>
<td>Role Attribute Value</td>
</tr>
</tbody>
</table>

### User Attribute Names

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GIVEN NAME ATTRIBUTE NAME</strong></td>
<td>firstName</td>
</tr>
<tr>
<td><strong>SURNAME ATTRIBUTE NAME</strong></td>
<td>lastName</td>
</tr>
<tr>
<td><strong>EMAIL ATTRIBUTE NAME</strong></td>
<td>Email</td>
</tr>
</tbody>
</table>
Once populated, select SAVE CHANGES and the SAML identity source integration will be added.

In the Identity Sources section, important information for configuration of the SAML integration is provided. Use the SP ENTITY ID and SP ACS URL for configuration on the external login SAML provider side.

- SP ENTITY ID
- SP ACS URL
- IDP LOGIN REDIRECT URL
- IDP LOGOUT POST URL
- SP METADATA

Sample Metadata code output:

```xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<EntityDescriptor entityID="https://someip.com/saml/CDWPjmZt" xmlns="urn:oasis:names:tc:SAML:2.0:metadata">
  <SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</NameIDFormat>
    <AssertionConsumerService index="0" isDefault="true" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://someip.com/externalLogin/callback/CDWPjmZt"/>
  </SPSSODescriptor>
</EntityDescriptor>
```

Note: Different SAML providers will have different field names and requirements. A onelogin SAML Test Connector (IdP w/attr) was used for the example integration this article.

**Onelogin SAML SSO**

For Onelogin SAML integration, the following fields are mapped:

- LOGIN REDIRECT URL : SAML 2.0 Endpoint (HTTP)
- LOGOUT POST URL : SLO Endpoint (HTTP)
- SIGNING PUBLIC KEY : X.509 Certificate
- SP ENTITY ID: ACS (Consumer) URL Validator
- SP ACS URL: ACS (Consumer) URL
12.16.3 Azure Active Directory SSO (SAML)

Azure Active Directory Single Sign-on can be added as a Identity Source in Morpheus using the SAML Identity Source Type. The Azure AD SSO configuration is slightly different than other SAML providers, and this guide will assist in adding a Azure AD SSO Identity Source.

Create a Azure AD SAML Integration

Azure requires inputting the *Identifier (Entity ID)* and *Reply URL (Assertion Consumer Service URL)* in the Azure SSO configuration before it provides the Endpoints and Certificate necessary to add the Integration into Morpheus. In order to get the *Identifier (Entity ID)* and *Reply URL (Assertion Consumer Service URL)* to input into Azure SSO config, we need to create a base SAML Integration in Morpheus first.

To add a base SAML integration:

1. Navigate to Administration > Tenants
2. Select a tenant.
3. Select IDENTITY SOURCES in the Tenant detail page
4. Select + ADD IDENTITY SOURCE.
5. Select SAML SSO from the TYPE field
6. Add a Name, optional Description and any value in the LOGIN REDIRECT URL field. Since we do not have the LOGIN REDIRECT URL from Azure yet, type any text such as *test* into the LOGIN REDIRECT URL field so the Identity Source Integration can be saved and the *Identifier (Entity ID)* and *Reply URL (Assertion Consumer Service URL)* generated. We will edit the Integration with the proper LOGIN REDIRECT URL after configuring SSO in Azure.
7. Select SAVE CHANGES.

Upon save, the *Entity ID* (Identifier (Entity ID)) and *SP ACS URL* (Reply URL (Assertion Consumer Service URL)) will be provide in the Identity Source list view. Copy these for use in Azure SSO config.

Configure Azure SSO

This guide assumes an Azure AD Application has already been created in Azure with a subscription level high enough to configure SSO in the application. Please refer to Azure documentation if this has not already been configured.

1. Next, in the Azure Active Directory Application details page, select *Single sign-on*, then enter the following:
   
   • **Single Sign-on Mode dropdown** Select SAML-based Sign-on
   
   • **Identifier (Entity ID)** Enter the Entity ID URL from the Morpheus Identity Source Integration above.
   
   • **Reply URL (Assertion Consumer Service URL)** Enter the SP ACS URL from the Morpheus Identity Source Integration above.

2. Save and click the *Test SAML Settings* button. Azure will confirm connection with Morpheus

3. In Azure’s *User Attributes & Claims* settings (step 2), select *Add a group claim with value user. groups* [SecurityGroup]

User Attributes & Claims config
4. Copy or keep available for reference the Claim Names/Namespace URLs for entering Role Attribute Values in the Morpheus Identity Source Integration.

5. In Azure SSO config, if one has not been generated, select Create new certificate to generate a new SAML Signing Certificate.

6. Enter a valid email address to receive certificate expiration notifications (these are not Morpheus-generated email).

7. In Azure SSO config, select `Configure {AD App Name}`

8. In the Configure sign-on pane, copy the following:
   
   • **SAML Single Sign-On Service URL** This will be used for the LOGIN REDIRECT URL in the Morpheus Identity Source Integration settings
   
   • **Sign-Out URL** This will be used for the LOGOUT REDIRECT URL in the Morpheus Identity Source Integration settings
   
   • **Click on the SAML XML Metadata link, open the xml file, and copy the key between the <X509Certificate> and </X509Certificate> tags. This will be used for the Public Key value in the SAML RESPONSE section of the Morpheus Identity Source Integration settings**

   Example Key (this is an example and is not valid):
   
   ```
   MIIC8ECCAdigAwIBAgIQEOZIX195d8Gw0BAQsFADA0MTIwMAYDVQQDEytNaWNyb3NvZnQgQXp1cmUgRmVkZXJhdGVkIFNTTyBDZX ... TlaMDQxMjAwBgNVBAMTTU1pY3Jvc29mdCBBenVyZSBGZWRlcmF0ZWQgU1NPIENlcnRpZmljYXRlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2k/ V6GcBpRoxJd0DLbhubwd0kp65LD9IUh5PUy2ohBHvFAy3S204mXoH7LWvY3oNrqxaNAksbYF6pokONf/ XeTdzu14xGnTuD9zRqPsoHHisyfBFUG/CxYxxo6w9fAPzJGLzc0Y51M20jINaqI4R/ pqp3qw+nYf7DXsy6f1Sspk64jfZD1jSvjd7upMitKPeOCRmeBUCnebjzwXgFBO714/5g1oOJWfT7Wpr4VVo/ p86xzQRv0GQpo19V1J3jJbhjLm4LjWT9UV2iyd10NdgtK7Qnh2oJ2Fq66qFTFTKpqVn0AHzx1KJWxfigz/ y56+ksYSRP87D0cVtFtHYqNQ0f0qKrgpMK7LmsEwq7crKX7nTCe2nBE0CDBV4ZzMrAzsEpjJnQs9jfZB
   ```

9. Save the SSO config in Azure AD app and return to Morpheus
Edit the existing Azure AD SAML Integration

Now that we have the required information, we can finalize the Azure AD SAML Integration in Morpheus.

1. Edit the existing Azure AD SAML Integration created in the first step and populate the following:

   **LOGIN REDIRECT URL** Add the SAML Single Sign-On Service URL copied from Azure SSO config.

   **LOGOUT REDIRECT URL** Add the Sign-Out URL copied from Azure SSO config.

   **SAML RESPONSE** Set to “Validate Assertion Signature”, then in the “Public Key” field enter the Public Key value we discussed in the last section.

   **GIVEN NAME ATTRIBUTE NAME** Enter the givenname Namespace url from Azure SSO config: http://schemas.xmlsoap.org/ws/2005/05/identity/claims

   **SURNAME ATTRIBUTE NAME** Enter the emailaddress Namespace url from Azure SSO config: http://schemas.xmlsoap.org/ws/2005/05/identity/claims

   **EMAIL ATTRIBUTE NAME** Enter the surname Namespace url from Azure SSO config: http://schemas.xmlsoap.org/ws/2005/05/identity/claims

Configure Role Mappings

Role mappings will map Azure AD Groups to Morpheus Roles. Azure AD users will be assigned Roles in Morpheus upon signing in based on their Group Membership in Azure AD.

**Important:** Use an Azure Groups Object ID, not Group name, when entering Role Mappings. Example: 7626a4a2-b388-4d9b-a228-72ce9a33bd4b

**DEFAULT ROLE** Role a Azure AD user will be assigned by default upon signing in to Morpheus using this Identity Source.

**REQUIRED AZURE AD GROUP OBJECT ID** Object ID of Azure AD Group a user must be a member of to be authorized to sign in to Morpheus. Users not belonging to this Group will not be authorized to login to Morpheus. This field is optional, and if left blank, any user from the Azure AD App will be able to sign in to Morpheus and will be assigned the Default Role if no Role Mappings match AD Group membership.

**GROUP ASSERTION ATTRIBUTE NAME** Enter http://schemas.microsoft.com/ws/2008/06/identity/claims/groups for Azure AD SSO

**Additional Role Mappings** The existing Roles in Morpheus will be listed. To map a Morpheus Role to an Azure AD Group, enter the Object ID of the desired Azure AD Group in the Role Attribute Value field for the corresponding Morpheus Role.

**Important:** Use an Azure Groups Object ID, not Group name, when entering Role Mappings. Example: 7626a4a2-b388-4d9b-a228-72ce9a33bd4b

**ENABLE ROLE MAPPING PERMISSION** When selected, Tenant users with appropriate rights to view and edit Roles will have the ability to set role mapping for the Identity Source integration. This allows the Tenant user to edit only the role mappings without viewing or potentially editing the Identity Source configuration.

**MANUAL ROLE ASSIGNMENT** When selected, administrators can manually edit Roles for users created through this identity source integration from the user detail page (Administration > Users > Selected user).
Note: For more on Identity Source role mapping permissions, see the associated guide in our KnowledgeBase.

Once populated, select SAVE CHANGES and the SAML identity source integration will be added. The Identity Source can be edited anytime to deactivate or change Role Mappings or other values.

Note: If Role mappings are edited after Azure AD SSO users have signed into Morpheus, currently logged in users will need to log out of Morpheus for the new Role mappings to take effect, when applicable.

Azure Group Lookups

When a user in azure ad has more than 150 group attributes, Azure does not include the group claims in the SAML response, and Morpheus is required to query Microsoft Graph to obtain the users group attribute values. When there are users that are members of more than 150 groups, populate the Azure Group Lookups section in order for those users to be able to use the Azure AD SAML SSO integration, otherwise no groups will be obtained and proper role mappings cannot occur.

AZURE TENANT ID Add Azure AD Tenant ID if user group membership will exceed 150. See Copy Directory (tenant) and Application (client) IDs for information on obtaining an Azure AD Tenant ID

AZURE APP ID Add Azure AD Application (Client) ID if user group membership will exceed 150. See Copy Directory (tenant) and Application (client) IDs for information on obtaining an Azure AD Application (Client) ID

AZURE APP SECRET Add Azure Application (Client) Secret if user group membership will exceed 150. See Generate a Client Secret for information on creating an Azure Application (Client) Secret

ROLE LINK ATTRIBUTE NAME default: http://schemas.microsoft.com/claims/groups.link. This is not normally changed.

 Signing In to Morpheus

When there is an active SAML/Azure AD SSO Identity Source Integration, a new button will appear on the Morpheus login page with the name of the Identity Source Integration as the button title. Example: MORPHEUS SSO. Another button titled “USERNAME AND PASSWORD” is also added for Morpheus account authentication outside of an Identity Source.

- SAML/Azure AD SSO users can log into Morpheus by clicking the SAML button. This will redirect the User to Azure AD app sign in url. If they are currently signed into Azure and authorized, the user will be instantly signed into Morpheus.
• Local Morpheus users can select “USERNAME AND PASSWORD” to sign in with their local credentials as before.

Note: If no local users other than the System Admin have been created, “USERNAME AND PASSWORD” option will not be displayed, only the SAML option.

12.16.4 OneLogin

Adding OneLogin Identity Source Integration

1. Navigate to Administration > Tenants
2. Select the Tenant to add the Identity Source Integration
3. Select IDENTITY SOURCES
4. Select + IDENTITY SOURCE
5. Enter the following:
   TYPE OneLogin
   NAME Name of the Identity Source Integration in Morpheus
   DESCRIPTION Optional Description of the Identity Source
   ONELOGIN SUBDOMAIN
       example: morpheus-dev

   Warning: Please verify the subdomain carefully. An invalid subdomain will cause authentication attempts by OneLogin users to fail.

   ONELOGIN REGION Specify US or EU region
   API CLIENT SECRET OneLogin API Client Secret from the Settings - API section in OneLogin portal
   API CLIENT ID OneLogin API Client ID from the Settings - API section in OneLogin portal
   REQUIRED ROLE Enter a role if OneLogin users logging into morpheus must have at least this OneLogin role to gain access to Morpheus.
   DEFAULT ROLE The default Morpheus Role applied to users created from OneLogin Integration if no other role mapping is specified below
   ROLE MAPPINGS Existing Morpheus Roles will be listed with fields to enter OneLogin Roles to map to. Users with OneLogin roles matching the role mappings will be assigned the appropriate Role(s) in Morpheus when signing in.
   ENABLE ROLE MAPPING PERMISSION When selected, Tenant users with appropriate rights to view and edit Roles will have the ability to set role mapping for the Identity Source integration. This allows the Tenant user to edit only the role mappings without viewing or potentially editing the Identity Source configuration.
   MANUAL ROLE ASSIGNMENT When selected, administrators can manually edit Roles for users created through this identity source integration from the user detail page (Administration > Users > Selected user).
Note: For more on Identity Source role mapping permissions, see the associated guide in our KnowledgeBase.

1. Select SAVE CHANGES and the OneLogin Integration will be added.

Users can now login to Morpheus with OneLogin credentials. The first Login will create a user in Morpheus matching the Username, email and Password from OneLogin. If a REQUIRED ROLE is specified in the Identity Source settings, only users with that Role in OneLogin will be able to login to Morpheus.

Important: OneLogin users will not authenticate in Morpheus if there is an existing Morpheus User with matching username or email address.

12.16.5 Okta

Overview

Morpheus allows users to integrate an Okta deployment for user management and authentication. In Morpheus, identity sources are added on a per-Tenant basis and Morpheus allows you to map Okta user groups to Morpheus user groups. User accounts are automatically created with matching metadata and role permissions when users are authenticated.

Adding an Okta Integration

1. Navigate to Administration > Tenants
2. Select a Tenant
3. Select IDENTITY SOURCES
4. Select + IDENTITY SOURCE
5. Choose TYPE: “Okta”
6. Populate the following, then select SAVE CHANGES:

Name Unique name for authentication type
Description A description for your new Okta Identity Source
Okta URL Your Okta URL
Administrator API Token Your Okta Administrator API Token
Required Group The Okta group that users must be in to have access (optional)
Default Role The default role a user is assigned if no group is listed under an Okta user that maps within the Morpheus Role Mappings section

ENABLE ROLE MAPPING PERMISSION When selected, Tenant users with appropriate rights to view and edit Roles will have the ability to set role mapping for the Identity Source integration. This allows the Tenant user to edit only the role mappings without viewing or potentially editing the Identity Source configuration.

MANUAL ROLE ASSIGNMENT When selected, administrators can manually edit Roles for users created through this identity source integration from the user detail page (Administration > Users > Selected user).
Note: For more on Identity Source role mapping permissions, see the associated guide in our KnowledgeBase.

Now, allowed Okta users can log into Morpheus via their Okta credentials and a user will be automatically generated within Morpheus with matching metadata and mapped Role permissions.

Note: If you’ve created multi-tenant roles, these will also appear here and can be mapped to Okta user groups allowing you to map users to equivalent user groups in Morpheus.

12.17 ITSM

12.17.1 ServiceNow

Overview

IT Service Management (ITSM) is an important area of focus for many organizations. Organizations invested in ServiceNow as an ITSM provider will find that Morpheus integrates tightly with some of the most-used features. After integrating ServiceNow with Morpheus, both environments can be used interchangeably and the results are synced to both places. This guide walks administrators through the process of integrating ServiceNow with Morpheus and how Morpheus can be used to effectively leverage the best of ServiceNow.

Tip: The ServiceNow integration guide is also available as a PDF download, which includes additional example use cases and screenshots.

Add ServiceNow Integration

1. Navigate to Administration > Integrations
2. Select + NEW INTEGRATION
3. Select “ServiceNow” from the dropdown list
4. Add the following:
   NAME A friendly name to describe the ServiceNow integration in Morpheus.
   ENABLED Check “Enabled” to allow consumption of this ServiceNow integration in Morpheus.
   SERVICENOW HOST URL of the ServiceNow instance (ex: https://your.instance.service-now.com), keep in mind you can create multiple ServiceNow integrations in Morpheus if needed.
   USER/PASSWORD A user in ServiceNow that is able to access the REST interface and create/update/delete incidents, requests, requested items, item options, catalog items, workflows, etc. The list of necessary roles includes x_moda_morpheus_ca.integration (available if the Morpheus ServiceNow plugin is installed from the ServiceNow Store), catalog_admin, itil, rest_service, and import_transformer.
   CMDB CUSTOM MAPPING If needed, administrators can opt to populate a specific field in the ServiceNow table and such mapping is identified here with a JSON code snippet. Below is an example that populates the object_id field in the CM database with the Morpheus instance name and two other field examples:
CMDB CLASS MAPPING  Define the mapping between Morpheus server types and ServiceNow CI classes. Select a Morpheus server type from the dropdown menu and a new field will appear in the list. Enter a ServiceNow CI class into the text field to create the association.

CMDB BUSINESS OBJECT  Allows the user to define the table CMDB records are written to if they prefer this over Morpheus default. By default, Morpheus writes to the `cmdb_ci_vm_instance` table.

5. Save Changes

**Important:** Morpheus supports integration with single-domain and multi-domain ServiceNow appliances. In multi-domain installations, a selected ServiceNow company can be mapped to a selected Morpheus Tenant for purposes of exposing Morpheus Library items only to users within a certain company. In this configuration, ServiceNow integrations should be added in each relevant Morpheus Tenant. Further setup steps for exposing Morpheus library items to ServiceNow are included in a later section below.

---

**ServiceNow Configuration Management Database (CMDB)**

ServiceNow CMDB is central to maintaining a complete record of IT infrastructure at many organizations. The Morpheus ServiceNow integration can create and update configuration item (CIs) records as new services are provisioned or existing services are reconfigured. Once a ServiceNow integration is set as the CMDB for a Cloud or Group, CI records are created and managed by Morpheus.

**Setting a CMDB on a Group**

When adding or editing a Morpheus Group, any active ServiceNow integration can be set as the CMDB.

1. Navigate to Infrastructure > Groups
2. Select an existing Group name from the list
3. Click **EDIT**
4. Under “Advanced Options”, select an active ServiceNow integration from the CMDB dropdown menu
5. If desired, select “CMDB DISCOVERY” to create CMDB CI records for discovered (unmanaged) servers that Morpheus automatically onboards to this Group

This setting is also available when creating a Group. Rather than selecting an existing Group in step two above, click + **CREATE** to make a new Group.
Setting a CMDB on a Cloud

When adding or editing a Morpheus Cloud, any active ServiceNow integration can be set as the CMDB.

1. Navigate to Infrastructure > Clouds
2. Select an existing Cloud name from the list
3. Click EDIT
4. Under “Advanced Options”, select an active ServiceNow integration from the CMDB dropdown menu
5. If desired, select “CMDB DISCOVERY” to create CMDB CI records for discovered (unmanaged) servers that Morpheus automatically onboards to this Cloud

This setting is also available when creating a Cloud. Rather than selecting an existing Cloud in step two above, click + ADD to make a new Cloud.

Provisioning and CI Records

With a ServiceNow instance integrated with Morpheus and the instance set as the CMDB for a Morpheus Group or Cloud, we will see CI records created as new resources are provisioned to the Cloud or Group in Morpheus. After the provisioning process has completed, a CI record should exist with a name value equal to the Instance name in Morpheus.

Provisioned and active Instances in Morpheus will have CI records with an “On” state in ServiceNow. After they are deleted in Morpheus, the state value will be rolled to “Terminated” in ServiceNow as expected.

Morpheus will also populate a number of additional fields in ServiceNow including IP address, FQDN and more. Custom views can be created in ServiceNow to expose these fields.

ServiceNow Approval Policies

Morpheus offers its own approval engine out of the box, but some organizations prefer ServiceNow to be their final approval authority. With a ServiceNow instance integrated with Morpheus, administrators can create provision approval policies and tie them to an active ServiceNow integration. With the policy in place, any new provisioning within the policy scope (Global, Group, Cloud, User, or Role) is sent to ServiceNow for approval before provisioning will go ahead in Morpheus. Approvals are synced between the two applications every minute.

Add ServiceNow Provision Approval Policy to a Cloud

**Note:** Any Instance provisioned into a Cloud with an approval policy enabled will not proceed without the required approval.

To add a ServiceNow Approval policy to a Cloud:
1. Navigate to Infrastructure > Clouds
2. Select a Cloud by clicking on the desired Cloud name link
3. Select the POLICIES tab
4. Click + ADD POLICY
5. Select Provision Approval from the type dropdown
6. Optionally enter a description for the Policy

7. Configure the following:

   **APPROVAL INTEGRATION** Select the ServiceNow Integration already configured in Administration > Integrations to use for the approval policy.

   **WORKFLOW** Select the ServiceNow workflow for the approval in ServiceNow (if desired). These workflows are configured and synced in from the ServiceNow Integration.

   **TENANTS (if applicable)** Only required for multi-tenant permission scoping. For the policy to apply to a Subtenant, type the name of the tenant(s) and select the Tenant(s) from the typeahead list.

8. Save Changes

**Add ServiceNow Provision Approval Policy to a Group**

**Note:** Any Instance provisioned into a Group with an approval policy enabled will not proceed without the required approval.

To add a ServiceNow Approval policy to a Group:

1. Navigate to Infrastructure > Groups
2. Select a Group by clicking on the Group name
3. Select the POLICIES tab
4. Click + ADD POLICY
5. Select Provision Approval
6. Optionally enter a description for the Policy
7. Configure the following:

   **APPROVAL INTEGRATION** Select the ServiceNow Integration already configured in Administration > Integrations to use for the approval policy.

   **WORKFLOW** Select the ServiceNow workflow for the approval in ServiceNow (if desired). These workflows are configured and synced in from the ServiceNow Integration.

   **TENANTS (if applicable)** Only required for multi-tenant permission scoping. For the policy to apply to a Subtenant, type the name of the tenant(s) and select the Tenant(s) from the typeahead list.

8. Save Changes

**Using ServiceNow Approval Policies**

Any Instance provisioned into a Cloud or Group with an approval policy enabled will be in a PENDING state until the request is approved.

Instances pending a ServiceNow approval will show “Waiting for Approval” with the Requested Item number and Request number, ex: Waiting for Approval [RITM0010002 - REQ0010002].

ServiceNow approval requests are displayed in Operations > Approvals. Instances pending a ServiceNow approval must be approved in ServiceNow for provisioning to initiate. Approval requests from a ServiceNow approval policy cannot be approved in Morpheus, only approvals originating from Morpheus.
ServiceNow approval requests are displayed in Morpheus under Operations > Approvals. Pending ServiceNow approval requests can be cancelled in Morpheus by selecting the request and then selecting ACTIONS > Cancel.

Once a pending ServiceNow approval request is approved in ServiceNow, the Instance(s) will begin to provision in Morpheus within one minute of being approved in ServiceNow.

**ServiceNow Monitoring Integration Settings**

**Note:** A ServiceNow integration must be already configured in Administration > Integrations to enable ServiceNow monitoring.

The ServiceNow monitoring integration is enabled and configured in Administration > Settings > Monitoring. As long as the “Enabled” switch is activated, Morpheus will report monitoring data to ServiceNow. Configuration selections are described below:

- **Enabled** Enables the ServiceNow monitoring integration
- **Integration** Select from an existing ServiceNow integration in \AdmInt\n- **New Incident Action** The ServiceNow action to take when a Morpheus incident is created
- **Close Incident Action** The Service Now action to take when a Morpheus incident is closed

**Incident Severity Mapping**

<table>
<thead>
<tr>
<th>Morpheus Severity</th>
<th>ServiceNow Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Info</td>
<td>Low/Medium/High</td>
</tr>
<tr>
<td>Warning</td>
<td>Low/Medium/High</td>
</tr>
<tr>
<td>Critical</td>
<td>Low/Medium/High</td>
</tr>
</tbody>
</table>

Once finished working with configuration, click **APPLY**
ServiceNow Service Catalog Integration

In addition to integrating with key ServiceNow features, Morpheus offers a free plugin directly from the ServiceNow Store. Once the plugin is installed, Morpheus Instance Types, Blueprints, and Self-Service Catalog Items can be presented as provisioning options in the ServiceNow catalog for ordering.

The Morpheus plugin supports integration with ServiceNow whether it’s configured for a single tenant or for multiple domains. When both Morpheus and ServiceNow are configured for multiple Tenants, we can create ServiceNow integrations in any relevant Morpheus Tenant and map those to specific companies in ServiceNow. Any exposed library items would only be shared with users in the relevant ServiceNow company. The Morpheus plugin will automatically detect whether the ServiceNow Domain Support–Domain Extensions Installer plugin has been installed and respond accordingly. Additionally, the User Criteria Scoped API plugin must also be enabled on the ServiceNow instance for multi-tenant use.

Depending on the scenario, setup steps for the Morpheus plugin will be slightly different. Setup steps for both single and domain-separated ServiceNow environments are included below.

**Important:** A valid SSL Certificate is required on the Morpheus Appliance for the ServiceNow plugin to be able to communicate with the appliance.

Single-Domain ServiceNow Configuration

1. Install the Morpheus plugin from the ServiceNow store.
   - Refer to the MORPHEUS DATA APPLICATION PLUG-IN FOR SERVICENOW Installation Instructions for plugin installation.
2. Navigate to Morpheus Catalog > Properties
3. Set the following properties:
   - **MID Server** If desired, specify the name of an existing MID server
   - **Morpheus Appliance Endpoint** The full URL to your Morpheus appliance
   - **Username** Morpheus user that the plugin will connect as to the Morpheus API
   - **Password** Password to the above Morpheus account

**Important:** The Morpheus service account integrated with the plugin interacts with the Morpheus appliance through Morpheus API and must have the appropriate Role permissions to complete all provisioning requests from the ServiceNow plugin. Often it’s easiest to make a service account with full administrator rights to avoid failed provisioning. If you’d prefer to create a minimal service account for security reasons, ensure the Role for the service account User has the following permissions:

   - Personas: Standard: Full
   - Personas: Service Catalog: Full
   - Features: Provisioning: Instances: Full
   - Features: Provisioning: Apps: Full
   - Groups: Full rights to all Groups containing Clouds you will expose to ServiceNow
   - Instance Types: Full rights to all Instance Types you will expose to ServiceNow
   - Blueprints: Full rights to all Blueprints you will expose to ServiceNow
• Catalog Item Types: Full rights to all Catalog Item Types you will expose to ServiceNow

Users created from SAML Identity Sources cannot authenticate with the Morpheus API and cannot be used for the ServiceNow plugin.

Multi-Domain ServiceNow Configuration

1. Install the Morpheus plugin from the ServiceNow store.
   • Refer to the MORPHEUS DATA APPLICATION PLUG-IN FOR SERVICENOW Installation Instructions for plugin installation.

2. Navigate to Morpheus Catalog > Multi-Tenant Credentials

3. Set the following properties:

   Morpheus Appliance Endpoint  The full URL to your Morpheus appliance
   Morpheus Tenant ID        The integer database ID for the selected Tenant
   Username                  Morpheus user that the plugin will connect as to the Morpheus API. This user must exist within the Morpheus Tenant being linked to the chosen ServiceNow company
   Password                  The password for the above user
   ServiceNow Company        Select a company from the list to link with the Tenant whose ID was entered above
   MID Server                If desired, specify the name of an existing MID server

Important: The Morpheus service account integrated with the plugin interacts with the Morpheus appliance through Morpheus API and must have the appropriate Role permissions to complete all provisioning requests from the ServiceNow plugin. Often it’s easiest to make a service account with full administrator rights to avoid failed provisioning. If you’d prefer to create a minimal service account for security reasons, ensure the Role for the service account User has the following permissions:

   • Personas: Standard: Full
   • Personas: Service Catalog: Full
   • Features: Provisioning: Instances: Full
   • Features: Provisioning: Apps: Full
   • Groups: Full rights to all Groups containing Clouds you will expose to ServiceNow
   • Instance Types: Full rights to all Instance Types you will expose to ServiceNow
   • Blueprints: Full rights to all Blueprints you will expose to ServiceNow
   • Catalog Item Types: Full rights to all Catalog Item Types you will expose to ServiceNow
Users created from SAML Identity Sources cannot authenticate with the Morpheus API and cannot be used for the ServiceNow plugin.

Adding to ServiceNow Catalog

Once the ServiceNow plugin is installed and configured, items can be added to the ServiceNow catalog from back in Morpheus. Follow the guide below to expose Morpheus Clouds, Library Items, and Blueprints to users in the ServiceNow catalog.

1. Navigate to |AdmInt|
2. Select the relevant ServiceNow integration
3. From the Instances tab we can + ADD CLOUD or + ADD LIBRARY ITEM
4. From the Blueprints tab we can + ADD BLUEPRINT
5. From the Catalog Items tab, we can + ADD CATALOG ITEM
6. Back in ServiceNow, access the Morpheus plugin from the Service Catalog
7. Exposed Morpheus Library Items, Catalog Items, and Blueprints are visible here for ServiceNow users with sufficient role permissions
12.17.2 Cherwell

Add Cherwell Integration

1. Navigate to Administration > Integrations
2. Select **NEW INTEGRATION**
3. Select Cherwell from the dropdown.
4. Add the following:
   
   **NAME**  Name of the Integration in Morpheus.
   **ENABLE** Leave checked to enable the Integration.
   **HOST**  Url of the Cherwell Instance
   **USER**  Enter in username
   **PASSWORD** Above Cherwell user’s password
   **CLIENT KEY**  Provide your Cherwell client key
   **CREATED BY USER**  This is the full name of a user in the Cherwell system. When a new change management record is created in the Cherwell system, this user will be added to the record as the user that created it.
   **START DAYS FROM NOW**  Number of days from now to set proposed start date
   **END DAYS FROM NOW**  Number of days from now to set proposed end date
   **CUSTOM MAPPING**  This is an optional json object that allows the custom setting of the Cherwell fields on the Change Request object.

   **Note:** The keys in the map correspond to the name of the field on the Change Request in Cherwell that you would like to set (see [https://bertram.d.pr/1Ziuhy](https://bertram.d.pr/1Ziuhy) for a reference). In addition, the value in the map corresponds to the value you wish to use. Within the value, Morpheus variables may be used. Here is an example for setting the Description is:

   ```json
   {
   "Description":"Created from Morpheus by ${instance.createdByUsername} in ${zone.name}"
   }
   ```

5. Save Changes

12.17.3 Remedy

PreRequisites

The user used for this integration need to be an Administrator in Remedy or have all the permissions to the form that is outlined in the table below.

<table>
<thead>
<tr>
<th>API Endpoint</th>
<th>Action</th>
<th>BMC Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>/api/arsys/v1/entry/CTM:People</td>
<td>GET</td>
<td>CTM:People</td>
</tr>
<tr>
<td>/api/arsys/v1/entry/COM:Company?q=%27Status%27=%22Enabled%22&amp;fields=values(Company)</td>
<td>GET</td>
<td>COM:Company</td>
</tr>
</tbody>
</table>
### Table 5 – continued from previous page

<table>
<thead>
<tr>
<th>API Endpoint</th>
<th>Action</th>
<th>BMC Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>/api/arsys/v1/entry/User</td>
<td>GET</td>
<td>User</td>
</tr>
<tr>
<td>/api/arsys/v1/entry/Group</td>
<td>GET</td>
<td>Group</td>
</tr>
<tr>
<td>/api/arsys/v1/entry/CHG:Infrastructure%20Change</td>
<td>POST</td>
<td>CHG:Infrastructure</td>
</tr>
<tr>
<td>/api/arsys/v1/entry/CHG:Infrastructure%20Change</td>
<td>PUT</td>
<td>CHG:Infrastructure</td>
</tr>
<tr>
<td>/api/arsys/v1/entry/CHG:Infrastructure%20Change</td>
<td>GET</td>
<td>CHG:Infrastructure</td>
</tr>
<tr>
<td>/api/cmdb/v1.0/instances/BMC.ASSET/BMC.CORE/BMC_DiskDrive</td>
<td>POST</td>
<td>BMC.CORE:BMC_DiskDrive</td>
</tr>
<tr>
<td>/api/cmdb/v1.0/instances/BMC.ASSET/BMC.CORE/BMC_DiskDrive</td>
<td>PATCH</td>
<td>BMC.CORE:BMC_DiskDrive</td>
</tr>
<tr>
<td>/api/cmdb/v1.0/instances/BMC.ASSET/BMC.CORE/BMC_DiskDrive</td>
<td>GET</td>
<td>BMC.CORE:BMC_DiskDrive</td>
</tr>
<tr>
<td>/api/cmdb/v1.0/instances/BMC.ASSET/BMC.CORE/BMC_DiskDrive</td>
<td>DELETE</td>
<td>BMC.CORE:BMC_DiskDrive</td>
</tr>
<tr>
<td>/api/cmdb/v1.0/instances/BMC.ASSET/BMC.CORE/BMC_IPEndpoint</td>
<td>POST</td>
<td>BMC.CORE:BMC_IPEndpoint</td>
</tr>
<tr>
<td>/api/cmdb/v1.0/instances/BMC.ASSET/BMC.CORE/BMC_IPEndpoint</td>
<td>PATCH</td>
<td>BMC.CORE:BMC_IPEndpoint</td>
</tr>
<tr>
<td>/api/cmdb/v1.0/instances/BMC.ASSET/BMC.CORE/BMC_IPEndpoint</td>
<td>GET</td>
<td>BMC.CORE:BMC_IPEndpoint</td>
</tr>
<tr>
<td>/api/cmdb/v1.0/instances/BMC.ASSET/BMC.CORE/BMC_IPEndpoint</td>
<td>DELETE</td>
<td>BMC.CORE:BMC_IPEndpoint</td>
</tr>
<tr>
<td>/api/cmdb/v1.0/instances/BMC.ASSET/BMC.CORE/BMC_Memory</td>
<td>POST</td>
<td>BMC.CORE:BMC_Memory</td>
</tr>
<tr>
<td>/api/cmdb/v1.0/instances/BMC.ASSET/BMC.CORE/BMC_Memory</td>
<td>PATCH</td>
<td>BMC.CORE:BMC_Memory</td>
</tr>
<tr>
<td>/api/cmdb/v1.0/instances/BMC.ASSET/BMC.CORE/BMC_Memory</td>
<td>GET</td>
<td>BMC.CORE:BMC_Memory</td>
</tr>
<tr>
<td>/api/cmdb/v1.0/instances/BMC.ASSET/BMC.CORE/BMC_Memory</td>
<td>DELETE</td>
<td>BMC.CORE:BMC_Memory</td>
</tr>
<tr>
<td>/api/arsys/v1/entry/AST:ComputerSystem</td>
<td>GET</td>
<td>AST:ComputerSystem</td>
</tr>
<tr>
<td>/api/arsys/v1/entry/AST:ComputerSystem</td>
<td>PUT</td>
<td>AST:ComputerSystem</td>
</tr>
<tr>
<td>/api/arsys/v1/entry/AST:ComputerSystem</td>
<td>POST</td>
<td>AST:ComputerSystem</td>
</tr>
<tr>
<td>/api/arsys/v1/entry/AST:IPEndpoint</td>
<td>GET</td>
<td>AST:IPEndpoint</td>
</tr>
<tr>
<td>/api/arsys/v1/entry/AST:IPEndpoint</td>
<td>PUT</td>
<td>AST:IPEndpoint</td>
</tr>
<tr>
<td>/api/arsys/v1/entry/AST:IPEndpoint</td>
<td>POST</td>
<td>AST:IPEndpoint</td>
</tr>
<tr>
<td>/api/arsys/v1/entry/AST:DiskDrive</td>
<td>GET</td>
<td>AST:DiskDrive</td>
</tr>
<tr>
<td>/api/arsys/v1/entry/AST:DiskDrive</td>
<td>PUT</td>
<td>AST:DiskDrive</td>
</tr>
<tr>
<td>/api/arsys/v1/entry/AST:DiskDrive</td>
<td>POST</td>
<td>AST:DiskDrive</td>
</tr>
<tr>
<td>/api/arsys/v1/entry/AST:Processor</td>
<td>GET</td>
<td>AST:Processor</td>
</tr>
<tr>
<td>/api/arsys/v1/entry/AST:Processor</td>
<td>PUT</td>
<td>AST:Processor</td>
</tr>
<tr>
<td>/api/arsys/v1/entry/AST:Memory</td>
<td>GET</td>
<td>AST:Memory</td>
</tr>
<tr>
<td>/api/arsys/v1/entry/AST:Memory</td>
<td>PUT</td>
<td>AST:Memory</td>
</tr>
<tr>
<td>/api/arsys/v1/entry/AST:Memory</td>
<td>POST</td>
<td>AST:Memory</td>
</tr>
<tr>
<td>/api/jwt/login</td>
<td>POST</td>
<td></td>
</tr>
</tbody>
</table>

### Add Remedy Integration

1. Navigate to Administration > Integrations
2. Select **+ NEW INTEGRATION**
3. Select **Remedy** from the dropdown.
4. Add the following:

   **NAME** Name of the Integration in Morpheus.
**ENABLE** Leave checked to enable the Integration.

**REMEDY HOST** Url of the Remedy Instance. e.g: http://xx.xx.xx.xx:8008

**USER** Enter in username

**PASSWORD** Above Remedy user’s password

**COMPANY** The dropdown will populate with values as soon as the auth using the above creds are successful

**APPROVAL USER** Full name of the user as it appear in Remedy. E.g: userid ‘anish’ would have full name as “Anish Abraham”

5. Save Changes

### 12.18 Keys and Certificates

#### 12.18.1 Venafi

**Overview**

Morpheus integrates with Venafi to sync and request SSL certificates

**Add Venafi**

1. Navigate to Administration > Integrations
2. Select **+ NEW INTEGRATION**
3. Enter in the following:
   - Name
   - Venafi Host
   - Username
   - Password
4. Click **SAVE CHANGES**

**Link Venafi To Cloud**

To add Venafi as the *Trust Provider* for a cloud

1. Navigate to Infrastructure > Clouds
2. Select Cloud
3. Select **EDIT**
4. Under *Advanced Options* select the Venafi integration from the *TRUST PROVIDER* dropdown
5. Select **SAVE CHANGE**
12.19 Load Balancers

12.19.1 AzureLB

Add Azure Load Balancer

1. Navigate to Infrastructure > Load Balancers
2. Select + ADD
3. Select Azure Load Balancer
4. Fill in the following:
   - CLOUD  Select the Cloud the Load Balancer will be available for
   - NAME  Name of the Load Balancer in Morpheus
   - DESCRIPTION  Identifying information displayed on the Load Balancer list page.
   - VISIBILITY  Define Multi-Tenant permissions
   - RESOURCE GROUP  Select the Resource Group the Load Balancer will be linked to
5. Save changes

12.19.2 F5 Load Balancers

Add F5 Load Balancer

To add a F5 Load Balancer Integration:
1. Navigate to Infrastructure > Load Balancers
2. Select + ADD
3. Select F5 BigIP
4. Fill in the following:
   - GROUP  Select the Group the Load Balancer will be available for
   - CLOUD  Select the Cloud the Load Balancer will be available for
   - NAME  Name of the Load Balancer in Morpheus
   - DESCRIPTION  Identifying information displayed on the Load Balancer list page.
   - VISIBILITY  Define Multi-Tenant permissions
   - API HOST  IP or resolvable hostname url.
   - API PORT  Typically 8443
   - USERNAME  API user
   - PASSWORD  API user password
   - MANAGEMENT URL  Example: https://10.30.20.31:8443/xui/
Advanced Options (optional)
   - VIRTUAL NAME
• POOL NAME
• SERVER NAME

5. Save Changes

Note: The Morpheus integration with F5 only supports basic authorization. Token-based authorization is not currently supported.

Virtual Servers

Instances attached to an F5 will be listed in the Virtual servers tab. Virtual servers can also be manually added in this section.

Add Virtual Server

1. Navigate to Infrastructure > Load Balancers
2. Select F5 Integration name to drill into the detail page
3. Select + ADD in the VIRTUAL SERVERS tab
4. Fill in the following:
   • NAME Name of the Virtual Server in Morpheus
   • DESCRIPTION Description of the Virtual Server in Morpheus
   • Enabled Uncheck to keep the configuration but disable F5 availability in Morpheus
   • VIP TYPE
     – Standard
     – Forwarding (Layer 2)
     – Forwarding (IP)
     – Performance (HTTP)
     – Performance (Layer 4)
     – Stateless
     – Reject
     – DHCP
     – Internal
     – Message Routing
   • VIP HOSTNAME Enter Hostname of the VIP (optional)
   • VIP ADDRESS Enter IP address for the VIP
   • VIP PORT Enter post used for the VIP
   • SOURCE ADDRESS Enter Virtual Server source address
   • PROTOCOL tcp, udp, or sctp
   • PROFILES Search for and select from available PROFILES
• **POLICIES**  Search for and select from available POLICIES
• **IRULES**  Search for and select from available RULE SCRIPTS
• **PERSISTENCE**
  – cookie
  – dest-addr
  – global-settings
  – hash
  – msrdp
  – sip
  – source-addr
  – ssl
  – universal
• **DEFAULT POOL**  Select from available POOLS

5. Select *SAVE CHANGES*

**Policies**

Policies will be synced and listed in the Policies tab. These policies will be available options when creating Virtual Servers.

**Pools**

**Create Pool**

**NAME**  Name of the POOL in Morpheus

**DESCRIPTION**  Description of the POOL in Morpheus

**BALANCE MODE**

• Round Robin
• Least Connections

**SERVICE PORT**  Specify SERVICE PORT for the POOL

**MEMBERS**  Search for and select from available NODES

**MONITORS**  Search for and select from available Monitors
Profiles

SSL Profiles are synced and will be created when an SSL Certificate is assigned in the Load balancer section when provisioning or editing a Load balancer on an Instance.

Monitors

Create Monitor

NAME  Name of the MONITOR in Morpheus
DESCRIPTION  Description of the MONITOR in Morpheus
PARENT MONITOR  Select from available MONITORS
DESTINATION  Specify Destination, such as *:443. Default is *:*
INTERVAL  Specify Monitor Interval. Default is 5
TIMEOUT  Specify Monitor Timeout. Default is 15
MONITOR CONFIG  Enter monitor config.

Nodes

Create Node

NAME  Name of the NODE in Morpheus
DESCRIPTION  Description of the NODE in Morpheus
ADDRESS  Enter node address
MONITOR  Select from available MONITORS
SERVICE PORT  Specify SERVICE PORT for the NODE

Rule Scripts

Rule Scripts will be synced and listed in the RULE SCRIPTS tab. These rules will be available options when creating Virtual Servers.

12.19.3 Citrix NetScaler
Add NetScaler Integration

To add a NetScaler Load Balancer Integration:

1. Navigate to Infrastructure > Load Balancers
2. Select + ADD
3. Select Citrix NetScaler
4. Fill in the following:
   - **GROUP** * Select the Group the Load Balancer will be available for.
   - **CLOUD** * Select the Cloud the Load Balancer will be available for.
   - **NAME** * Name of the Load Balancer in Morpheus.
   - **DESCRIPTION** Identifying information displayed on the Load Balancer list page.

   **VISIBILITY**
   - Define Tenant Visibility
     - Public: Available to all Tenants.
     - Private: Only available to specified Tenant.
   - **Tenant** If Visibility is set to private, define the Tenant the Load Balancer will be available in.

   **API URL** *
   - URL of the NetScaler API
     - Example: http://10.30.21.55

   **API PORT** *
   - NetScaler API port
     - Example: 80

   **USERNAME** * NetScaler service account username
   **PASSWORD** * NetScaler service account password

   **VIRTUAL NAME**
   - Naming Pattern for new NetScaler Virtual Servers
     - If blank, defaults to \texttt{morph_lb_${loadBalancer.id}}

   **SERVICE NAME**
   - Naming Pattern for new NetScaler Services
     - If blank, defaults to \texttt{morph_service_${container.id}}

   **SERVER NAME**
   - Naming Pattern for new NetScaler Servers
     - If blank, defaults to \texttt{morph_server_${server.id}}
Add Load Balancer to Instance

Load Balancers can be added to Instances during Provisioning or to existing Instances. For Load Balancer settings to appear during provisioning, or for the scale tab to be available on an Instance, the instances Node Type must have a LB port defined.

Note: For Load Balancer settings to appear during provisioning, or for the scale tab to be available on an Instance, the instances Node Type must have a LB port defined.

Add Load Balancer during Provisioning

In the Instance Provisioning wizard, Load Balancers can be configured in the Automation > Load Balancer section.

1. Navigate to Provisioning > Instances.
2. Select + ADD.
3. Select an Instance Type that supports scaling. (ENABLE SCALING (HORIZONTAL) flagged on Instance Type configuration)
4. Proceed with Instance configuration to the Automation section.
5. Fill in the following:
   - **VIP ADDRESS**
     Define IP Address for the Virtual Server
     - Example: 10.30.23.191
   - **VIP PORT**
     Define port for the Virtual Server
     - Example: 80
   - **VIP HOSTNAME**
     Define hostname that will resolve to the VIP IP.
     - Example: jwDemoHaApp59.den.example.com
   - **VIRTUAL SERVICE NAME** Define name for the Virtual Service. Defaults to ${instance.name}
   - **BALANCE MODE**
     Specify balance mode for the VIP
     - Least Connections
     - Round Robin
   - **STICKY MODE**
     Specify sticky session options for the VIP
     - Source IP
     - Cookie
   - **SHARED VIP ADDRESS** Select if VIP is shared, then enter DIRECT VIP ADDRESS
   - **SSL CERT**
SSL Certificate that will be applied to the VIP.

- No SSL
- Select existing Certificate from Infrastructure > Keys & Certs or from a Trust Provider Integration.

**USE EXTERNAL ADDRESS FOR BACKEND NODES**

- Select if traffic from LB to Backend Nodes needs to be sent to the External Addresses, or leave deselected to use Internal Addresses for Backed Nodes.

6. Optionally configure auto-scaling configuration in the Scale section

7. Select NEXT and provision the Instance.

After all nodes in the Instance are provisioned, the LB configuration will be added to the Instance and Virtual Servers, Services and Servers will be created and configured on the NetScaler. The Load Balancer settings and status will be visible in the Instance details page LOAD BALANCER section, with additional details, links, and configurations options available in the SCALE tab.

### 12.20 Logs

#### 12.20.1 Syslog

**Adding Syslog Integration**

1. Navigate to Administration > Settings > Logs
2. Expand the Morpheus logging section
3. Add the Syslog forwarding rules
4. Select **QUICK ADD**

### 12.21 Monitoring

#### 12.21.1 ServiceNow Monitoring Integration

**Note:** A ServiceNow Integration must be already configured in Administration > Integrations to enable the ServiceNow Monitoring Integration. Refer to the *ServiceNow* configuration guide for more information.

- **Enabled** Enables the ServiceNow Monitoring Integration
- **Integration** Select from a ServiceNow Integration added in Administration > Integrations
- **New Incident Action** The Service Now action to take when a Morpheus incident is created.
- **Close Incident Action** The Service Now action to take when a Morpheus incident is closed.

Incident Severity Mapping
12.21.2 AppDynamics

AppDynamics is a very powerful performance and application monitoring tool. It features advanced correlation features and profiling capabilities for a very wide range of application platforms including native Docker support. Due to the level of capabilities of AppDynamics there are more required settings to integrate it with Morpheus.

Configuring The AppDynamics Integration

1. Navigate to Administration > Settings > Monitoring
2. Expand the AppDynamics section
3. Toggle the Enable slider
4. Fill out desired fields
5. Save

Once saved, all hosts will automatically be configured to install the AppDynamics agent.

AppDynamics is capable of being run as a paid SaaS based service as well as an on premise installation and Morpheus supports both configurations. Most input fields related to connecting to AppDynamics provide helpful tips as to what information exactly needs provided and where to acquire it.

12.21.3 NewRelic

Configuring The NewRelic Integration

1. Navigate to Administration > Settings > Monitoring
2. Expand the NewRelics section
3. Toggle the Enable slider
4. Enter License Key to be used when installing the New Relic agent in order for the agent to report data to your New Relic account

Note: The License Key is the 40-character hexadecimal string that New Relic provides when you sign up for your account.
12.22 Networking Integrations

12.22.1 Infoblox

Features

• Network Pools synchronization
• DNS Zone & Zone record synchronization
• Host Record synchronization
• Total & Free IP status bar for networks
• Network Grid and List view with IP Status and records, date and user tracking
• Automatic and manual IP Reservations, DNS A/PTR record creation and deletion
• Use script variables like <%= variableX %> for evaluation of the key data in extended attributes

Adding Infoblox Integration

Note: Making full use of the Morpheus Infoblox integration requires credentials for an Infoblox user account with API access granted, access to list the pools and zones you wish to work with, and rights to create and destroy records. See Infoblox documentation for more information on user rights administration in that product.

1. Navigate to Infrastructure - Network - Integrations
2. Select + ADD > IPAM > Infoblox
3. Enter the following:
Morpheus Documentation

ADD IPAM INTEGRATION

NAME

☑️ ENABLED

URL https://x.x.x.x/wapi/v2.2.1

USERNAME

PASSWORD

THROTTLE RATE 0 ms

☑️ DISABLE SSL SNI VERIFICATION

INVENTORY EXISTING

NETWORK FILTER

ZONE FILTER

TENANT MATCH ATTRIBUTE

IP MODE Static IPs

EXTRA ATTRIBUTES

Accepts a JSON input of custom attributes that can be saved on Host Record in Infoblox. These Must be first defined as extra attributes in Infoblox and values can be injected for the user creating the record and the date of assignment. The available injectable attributes are: `userId`, `username`, and `dateCreated`. They can be injected with `<==>`.
NAME  Name of the Integration in Morpheus
Enabled  Deselect to disable the Integration
URL  Infoblox wapi url. Example: https://x.x.x.x/wapi/v2.2.1

Tip:  The Infoblox wapi version can be found at https://x.x.x.x/wapidoc/

USERNAME  Infoblox user username
PASSWORD  Infoblox user password
THROTTLE RATE  In milliseconds (ms)
DISABLE SSL SNI VERIFICATION  Leave selected to disable SSL SNI Verification
INVENTORY EXISTING  Mark this option to inventory existing network pools from Infoblox
NETWORK FILTER  Filter which networks are synced into Morpheus. Example: Network Filter: [
    network_view=default&*Building=work
]
ZONE FILTER  Filter terms for Zone Records

TENANT MATCH ATTRIBUTE  This can be set to the name of the extended attribute in Infoblox where Morpheus will check for the id of a morpheus tenant. This allows for setting the tenant’s Morpheus id to an extended attribute field on a network view or network in Infoblox, and when the network or view is discovered by morpheus, it will be auto assigned to the right tenant.

IP MODE  Static IPs or DHCP Reservations
EXTRA ATTRIBUTES  Accepts a JSON input of custom attributes that can be saved on host records in Infoblox

4. Select SAVE CHANGES

Upon save the Infoblox IPAM integration will be created and the following will sync:

- Infoblox networks will be synced in and populate in the Infrastructure - Network - IP Pools tab and in the Infoblox detail page under the NETWORK POOLS tab
- Host Records will sync and populate in the Network Pool detail view (select an IP Pool name to view)
- DNS Zones will sync and populate under Infrastructure - Network - Domains and in the Infoblox detail page under the HOSTS tab
- DNS Zone Records will sync and populate

Adding IP Pools to Networks

Morpheus can automatically assign the next available Infoblox IP in an IP/Network Pool and create the corresponding DNS records, as well as remove the records upon teardown. To enable this, add an Infoblox IP/Network Pool to the Network Pool section on a Network(s).

1. Navigate to Infrastructure > Network > Networks
2. Select a Network name and click EDIT
3. In the NETWORK POOL section, search for and select the name of the IP/Network Pool.
   - Gateway, DNS and CIDR must be populated for static/pool IP assignment
   - Select Allow IP Override to allow selecting between DHCP, Static entry and Pool Selection at provision time (if desired)
- Deselect DHCP server if a DHCP server will not be used on the network (only static and/or IP Pool IP assignment)

4. Select **SAVE CHANGES**

**Creating Host Records**

1. Select a Network Pool from *Infrastructure > Network > IP Pools or Infrastructure > Network > Services > Infoblox*
2. Select **+ ADD**
3. Enter the following

![Create Host Record]

- **HOSTNAME**  Hostname for the record
- **IP ADDRESS**  IP address for the Host Record
- **DOMAIN**  Select an Infoblox Zone

- **Create DNS Records**  Select to create DNS A and PTR Records in Infoblox

4. Select **SAVE CHANGES**

**Creating Zone Records**

1. Select a Domain from *Infrastructure > Network > Domains or Infrastructure > Network > Services > Infoblox > Zones*
2. Select **+ ADD**
3. Enter the following
**12.22.2 phpIPAM**

**Configuration**

1. Within phpIPAM dashboard, enable api in Administration > phpIPAM settings > feature settings. Toggle API switch to on and save.

2. Go to Admin > API > create API key.

3. Create unique App ID.

4. Enable read/write/admin access under App Permissions.


**Add phpIPAM integration to Morpheus**

1. Navigate to Infrastructure > Network > Integrations

2. Select + ADD > IPAM > phpIPAM

3. Enter the following:
   - Name
   - **URL** Add /api/ to end of URL ex. http://10.30.20.196/api/
   - **App ID** From phpIPAM API Key
• Username
• Password
• Enable or Disable SSL SNI Verification
• Enter Network Filter

4. Select *SAVE IPAM INTEGRATION*

### 12.22.3 NSX-V

**Overview**

- SUMMARY
- TRANSPORT ZONES
- SWITCHES
- LOGICAL SWITCHES
- FIREWALL
- LOGICAL ROUTERS
- EDGE GATEWAYS

**Add NSX-V Integration**

1. Navigate to *Infrastructure > Network > Integrations*
2. Select Select + *ADD* > VMWare NSX-V
3. Enter the following:
   - **NAME**  Name for the NSX Integration in Morpheus
   - **API HOST**  URL of NSX Manager
   - **USERNAME**  NSX Manager Admin Username
   - **PASSWORD**  NSX Manager Admin password
   - **VMWARE CLOUD**  Select the existing VMware cloud associated with this NSX integration
4. Select *ADD NETWORK INTEGRATION*

Once the NSX Integration is added Morpheus will sync in existing Transport Zones, Logical Switches, and Edge Gateways. New Transport Zones, Logical Switches, and Edge Gateways can be now be created.

**Summary View**

When accessing an NSX-V integration (*Infrastructure > Network > Integrations*), you’re taken to the SUMMARY tab by default. In Morpheus 4.1.2 and later, the NSX-V integration includes an enhanced summary view that includes global, system, and component statuses, as well as enhanced stats. As of Morpheus version 4.1.2, you can also force a manual refresh of the integration details by clicking *ACTIONS* > *Refresh*. 
Create NSX Transport Zone

1. Navigate to *Infrastructure > Network*
2. Select the *Integrations* tab
3. Select the name of NSX-V integration
4. Select the *Transport Zones* tab
5. Select + *CREATE NSX TRANSPORT ZONE*

**NAME**  Name of Transport Zone

**DESCRIPTION**  Description for the Transport Zone

**CLUSTER**  Select the Cluster the Transport Zone will be provisioned to

**REPLICATION MODE**  “multicast”, “unicast”, or “hybrid”
Switches

Morpheus version 4.1.2 adds SWITCHES tab to view switches associated with the selected NSX integration. Information displayed on each switch include the following:

- NAME
- UPLINK PORT
- TYPE
- SWITCH ID
- DESCRIPTION

Create NSX Logical Switch and Edge Gateway

**Important:** Prior to creating a Logical Switch and Edge Gateway, associated External VMware Networks must be configured in Morpheus. Navigate to INFRASTRUCTURE > NETWORK and edit any Distributed Switch Groups that will be used and populate the Gateway, DNS and CIDR.

1. Navigate to INFRASTRUCTURE > NETWORK
2. Select the SERVICES tab
3. Select the name of NSX Integration
4. Select the LOGICAL SWITCHES tab
5. Select + CREATE NSX LOGICAL SWITCH
6. Populate the following for the Logical Switch and Edge Gateway Configurations:
   - **Logical Switch Configuration:**
     - NAME: Name of the Logical Switch
     - DESCRIPTION: Description of the Logical Switch
     - TRANSPORT ZONE: Select an existing Transport Zone
     - CIDR: Add the CIDR for the Logical Switch. Example: 10.30.28.0/24
     - TENANT NAME: Enter Tenant name for the Logical Switch (Optional)
   - **Edge Gateway Configuration:**
     - HOSTNAME: Enter Hostname of the Edge Gateway
     - SIZE: Select Size of the Edge Gateway
EXTERNAL NETWORK  Select the External Network for the Edge Gateway.

**Important:** The Gateway, DNS and CIDR must be populated on an external network for it to be selectable when creating an Edge Gateway.

**IP ADDRESS** Populate IP address to be assigned to the Edge Gateway

**DATA STORE** Select the Datastore for the Gateway

**RESOURCE POOL** Select the Resource Pool for the Gateway

**FOLDER** Select a Folder for the Edge Gateway (optional)

**USERNAME** Enter a Username for the Edge Gateway

**PASSWORD** Enter a Password for the Edge Gateway

**Note:** Password length must be at-least 12 characters and at-max 255 characters. It must contain mix of alphabets with both upper case and lower case, numbers and at-least one special character. Password must not contain username as substring. Character must not consecutively repeat 3 or more times.

7. Select + CREATE

Morpheus version 4.1.2 also extends the details we can see on existing Edge Gateways. First, to view the list of Edge Gateways, navigate to your selected NSX integration, and click on the EDGE GATEWAYS tab. Here you will see a list of existing Edge Gateways, including their NAME and DESCRIPTION values. To see the enhanced details view for your Edge Gateways, click on the name of a selected Edge Gateway.

The new Edge Gateway detail view includes the following tabs:

- **SUMMARY:** Includes general configuration details for the selected Edge Gateway
- **FIREWALL:** Includes firewall configuration detail and includes the ability to create rules
- **DHCP:** Includes details on IP pools
- **ROUTING:** Includes details on configured routes and includes the ability to create routes
Firewall

Morpheus version 4.1.2 adds a FIREWALL tab which allows you to view existing firewall rules as well as create new rules and groups. From the rules summary list, the following fields are displayed for each rule:

- NAME
- TYPE
- POLICY
- DIRECTION
- SOURCE
- DESTINATION
- APPLICATION

Morpheus also allows you to create new firewall groups and new firewall rules.

To create a new group:

1. Click on the ACTIONS button from within the list of firewall rules
2. Click “Create Group”
To create a new rule:

1. Click on the *ACTIONS* button from within the list of firewall rules
2. Click “Create Rule”
Logical Routers

Morpheus version 4.1.2 adds a Logical Routers section to the NSX integration, including the ability to view and create new logical routers. From the LOGICAL ROUTERS tab, a list of logical routers associated with your selected integration is shown. Values displayed for each logical router include the following:

- STATUS
- NAME
- DESCRIPTION

To create a new logical router:

1. Navigate to the LOGICAL ROUTERS tab for the chosen integration
2. Click on + CREATE NSX LOGICAL ROUTER
3. Complete the presented modal
4. Click ADD NETWORK ROUTER
Overview

VMware NSX-T offers network virtualization allowing for creation and management of software-based virtual networks in an efficient and programmatic way. Morpheus offers a full-featured integration with NSX-T, exposing its networking abstractions in the following sections of the Morpheus NSX-T integration:

- SUMMARY
- TRANSPORT ZONES
- SEGMENTS
- FIREWALL
- TIER-1 GATEWAYS
- TIER-0 GATEWAYS

This guide goes through the process of integrating an existing NSX-T installation with Morpheus and working with the associated objects synced in with the integration. For more on installing NSX-T and an overview of its concepts, please review the NSX-T overview documentation provided by VMware.
Add NSX-T Integration to Morpheus

1. Navigate to Infrastructure > Network > Integrations
2. Select Select + ADD > VMWare NSX-T
3. Enter the following:
   - **NAME:** Name for the NSX Integration in Morpheus
   - **API HOST:** URL of the NSX Manager (ex. https://x.x.x.x/api)
   - **USERNAME:** NSX Manager Admin Username
   - **PASSWORD:** NSX Manager Admin password
   - **VMWARE CLOUD:** Select the existing VMware cloud associated with this NSX integration
4. Select **ADD NETWORK INTEGRATION**

Once the NSX Integration is added Morpheus will sync in existing Transport Zones, Segments, firewall groups and rules, and Gateways. We can also manage these synced items from within Morpheus UI, including the ability to create, edit, and delete them.

Summary View

The SUMMARY tab contains the default view when accessing an NSX-T integration. From the summary view we can see the health status of the NSX-T server, and details about interfaces and group status.

Transport Zones

Access Transport Zones by navigating to Infrastructure > Networks > Integrations > (Your NSX-T Integration) > Transport Zones tab. We can delete Transport Zones by clicking on the trash can icon to the far right of each list item. The default view lists each Transport Zone and provides the following information about them:

   - **NAME:** The given name for the Transport Zone
   - **DESCRIPTION:** A given description value (if available)
   - **TRAFFIC TYPE:** “Overlay” or “VLAN”
   - **N-VDS NAME:** The name of the NSX-managed virtual distributed switch
   - **STATUS:** An icon indicating the current status of the Transport Zone
   - **HOST MEMBERSHIP CRITERIA:** “Standard” or “Enhanced Datapath”

Creating NSX-T Transport Zones

1. Navigate to Infrastructure > Network
2. Select the Integrations tab
3. Select the name of NSX-T integration
4. Select the Transport Zones tab
5. Select + **CREATE NSX-T TRANSPORT ZONE**
6. After completing the required fields and any desired optional fields, click + **CREATE**
Segments

Access Segments by navigating to Infrastructure > Networks > Integrations > (Your NSX-T Integration) > Segments tab. We can delete Segments by clicking on the trash can icon to the far right of each list item or edit them by clicking on the pencil icon. The default view lists each Segment and provides the following information about them:

- **STATUS:** An icon indicating the current status of the Transport Zone
- **NAME:** The given name for the Segment
- **TRAFFIC TYPE:** “Overlay” or “VLAN”
- **N-VDS NAME:** The name of the NSX-managed virtual distributed switch
- **STATUS:** An icon indicating the current status of the Transport Zone
- **HOST MEMBERSHIP CRITERIA:** “Standard” or “Enhanced Datapath”

Creating NSX-T Segments

1. Navigate to *Infrastructure > Network*
2. Select the *Integrations* tab
3. Select the name of NSX-T integration
4. Select the *Segments* tab
5. Select *CREATE NSX-T SEGMENT*
6. Complete the fields in the CREATE NETWORK modal
7. Click *SAVE CHANGES*

Note: NSX-T Segments can be scoped to specific Groups and Tenants when creating or editing the Segment.

Firewall

Access firewalls by navigating to Infrastructure > Networks > Integrations > (Your NSX-T Integration) > Firewall tab. We can delete firewall groups by clicking on the trash can item at the end of each row. Additionally each group can be expanded (when applicable) to reveal the firewall rules within the group. Individual rules can be edited or deleted by clicking on pencil or trash can icon at the end of the row. The default view lists each Segment and provides the following information about them:

- **NAME:** The name of the rule or group within Morpheus
- **CATEGORY:** “Ethernet”, “Emergency”, “Infrastructure”, “Environment”, or “Application”
- **ENABLED:** Applies only to rules, the rule is enabled when the check mark is present
- **POLICY:** Applies only to rules, “Allow”, “Drop”, or “Reject”
- **DIRECTION:** Applies only to rules, “In”, “Out”, or “In-Out”
- **SOURCE:** Applies only to rules, “Any”, by default
- **DESTINATION:** Applies only to rules, “Any”, by default
- **APPLICATION:** Applies only to rules, “Any”, by default
Creating NSX-T Firewall Groups

1. Navigate to Infrastructure > Network
2. Select the Integrations tab
3. Select the name of NSX-T integration
4. Select the Firewall tab
5. Select ACTIONS
6. Select Create Group
7. Complete the fields in the CREATE GROUP modal:
   - NAME: The name of the rule or group within Morpheus
   - DESCRIPTION: An optional description value for the group
8. Click SAVE CHANGES

Creating NSX-T Firewall Rules

1. Navigate to Infrastructure > Network
2. Select the Integrations tab
3. Select the name of NSX-T integration
4. Select the Firewall tab
5. Select ACTIONS
6. Select Create Rule
7. Complete the fields in the CREATE RULE modal:
   - NAME: The name of the rule or group within Morpheus
   - DESCRIPTION: An optional description value for the rules
   - ENABLED: Rule is enforced when checked
   - DIRECTION: “In”, “Out”, or “In-Out”
   - SOURCES: “Any”, by default
   - DESTINATIONS: “Any”, by default
   - SERVICES: “Any”, by default
   - PROFILES: “Any”, by default
   - SCOPES: “Any”, by default
   - POLICY: “Allow”, “Drop”, or “Reject”
8. Click CREATE
Morpheus Documentation

Tier-1 Gateways

Access Tier-1 Gateways by navigating to Infrastructure > Networks > Integrations > (Your NSX-T Integration) > Tier-1 Gateways tab. We can edit a Gateway by clicking the pencil icon in each row or delete the Gateway by clicking on the trash can icon. The default page for Tier-1 Gateways displays the following information on each:

- **STATUS**: An icon indicating the status of each gateway
- **NAME**: The given name of the gateway
- **DESCRIPTION**: An optional description value for the gateway

Creating Tier-1 Gateways

1. Navigate to *Infrastructure > Network*
2. Select the *Integrations* tab
3. Select the name of NSX-T integration
4. Select the *Tier-1 Gateways* tab
5. Select *+ CREATE NSX-T TIER-1 GATEWAY*
6. Complete the fields in the ADD NETWORK ROUTER modal:
   - **GROUP**: If desired, scope the Tier-1 Gateway to a Morpheus Group
   - **NAME**: The name of the Tier-1 Gateway within Morpheus
   - **ENABLED**: Tier-1 Gateway is available for use when checked
   - **TIER-0 Gateway**: Select an existing and enabled Tier-0 Gateway
   - **EDGE CLUSTER**: Select an existing Edge Cluster
7. Make selections as needed in the “Route Advertisement” section
8. Click *ADD NETWORK ROUTER*

Tier-0 Gateways

Access Tier-0 Gateways by navigating to Infrastructure > Networks > Integrations > (Your NSX-T Integration) > Tier-0 Gateways tab. We can edit a Gateway by clicking the pencil icon in each row or delete the Gateway by clicking on the trash can icon. The default page for Tier-0 Gateways displays the following information on each:

- **STATUS**: An icon indicating the status of each gateway
- **NAME**: The given name of the gateway
- **DESCRIPTION**: An optional description value for the gateway
Creating Tier-0 Gateways

1. Navigate to Infrastructure > Network
2. Select the Integrations tab
3. Select the name of NSX-T integration
4. Select the Tier-0 Gateways tab
5. Select + CREATE NSX-T TIER-0 GATEWAY
6. Complete the fields in the ADD NETWORK ROUTER modal:
   - GROUP: If desired, scope the Tier-0 Gateway to a Morpheus Group
   - NAME: The name of the Tier-0 Gateway within Morpheus
   - ENABLED: Tier-1 Gateway is available for use when checked
   - HA MODE: “Active Active” or “Active Standby”
   - EDGE CLUSTER: Select an existing Edge Cluster
7. Make selections as needed in the routing and BGP sections
8. Click ADD NETWORK ROUTER

12.22.5 Cisco ACI

Overview

Add ACI as a network and security integration. Inventory your existing ACI configurations. Create networks, bridge domains, application profiles, tenants, endpoint groups, contexts, filters and contracts. Provision instances into new endpoint groups and define security groups that apply contracts on provision.

From Morpheus below can be created:

- Tenants
- ANP's
- EPG's
Add Network Integration

1. Navigate to Infrastructure > Networks > Integrations
2. Select +ADD > Networking > Cisco ACI
3. Populate the following:
   - **NAME**: ACI Integration Name/Label in Morpheus. This is unique to Morpheus and not part of authentication.
   - **URL**: ACI fabric url, eg https://apicdc.company.com
   - **USERNAME**: ACI aaaUser name attribute
   - **PASSWORD**: ACI aaaUser pwd attribute
   - **TENANT**: Populates upon authentication, tenant selection not required
4. Select ADD NETWORK INTEGRATION

Configure Cloud Network Mode

For your ACI Integration to be available during provisioning, ACI needs to be defined on a Cloud or multiple Clouds.

1. Select an existing VMware vCenter Cloud
2. Select EDIT
3. Expand the Advanced Options section
4. Select ACI Integration in NETWORK MODE dropdown
5. Select SAVE
Instance Provisioning

Once ACI is integration to a cloud, it can be used during instance provisioning:

1. From the EPG drop down, either an existing EPG can be selected or a new one can be created. It is the same for ANP, either create a new one or choose an existing.

2. Under ACI security consumes and provides, contracts can be searched when you enter a name. When the provisioning wizard is completed, it will provision the instance and apply the ACI options and Security. This can be viewed under the instance page, or via REST API and CLI.

Blueprint Configuration

- In a Blueprint, you can define the ANP and EPG of each Tier
- Variables can be used for EPG and ANP names.
- This could be useful to create blueprints for dev testing to isolate from prod networks.
- This can be hybrid based on the VMM domains in APIC.
12.22.6 Bluecat

Overview

Morpheus integrates with Bluecat IPAM to scope pools to networks for static IP assignment from Bluecat to your Morpheus Instances.

Adding Bluecat to Morpheus

1. Navigate to Infrastructure > Network > Integrations
2. Click + ADD
3. Select Bluecat
4. Enter in the following information
   - **Name**: Name of the Bluecat Integration in Morpheus
   - **Enabled**: Uncheck to disable sync with the Bluecat endpoint
   - **URL**: URL of the Bluecat server, ex: http://10.30.20.10
   - **Username**: Username of Bluecat API User. API and root level propagating read access required, read/write access required for target Networks and Domains.
   - **Password**: Bluecat User password
   - **Network Filter**: Optionally enter the id of a config, block or network, or comma separated combination of configs, blocks and/or networks.
5. Click **SAVE CHANGES**

The Bluecat Integration will be saved, IP pools will sync in and populate under Infrastructure > Network > IP Pools, and Domain will populate in Infrastructure > Network > Domains. Pools and Domains can also be found in the Bluecat Integration details page, which can be accessed by clicking on the name of the added Bluecat Integration in Infrastructure > Network > Services.

**Important:** *Quick Deployments* must be enabled in Bluecat for Morpheus to create instantly available DNS records when using Bluecat DNS.

Adding IP Pools to Networks

Morpheus can automatically assign the next available Bluecat IP in an IP/Network Pool and create the corresponding DNS records, as well as remove the records upon teardown. To enable this, add an Bluecat IP/Network Pool to the Network Pool section on a Network(s).

1. Navigate to Infrastructure - Network- Networks
2. Select a Network name and EDIT, or select **ACTIONS - Edit**
3. In the **NETWORK POOL** section, search for and select the name of the IP/Network Pool.
   - Gateway, DNS and CIDR must be populated for static/pool IP assignment
   - Select **Allow IP Override** to allow selecting between DHCP, Static entry and Pool Selection at provision time
• Deselect DHCP server if a DHCP server will not be used on the network (only static and/or IP Pool IP assignment)
4. Select SAVE CHANGES

12.22.7 SolarWinds IPAM

Features

• Automate static IP assignment across environments using Solarwinds IPAM
• Network pool sync: Network pools can be set on networks in Morpheus for automated IP allocation and record creation
• Optional Network Pool allocation and record sync. Inventory Existing option syncs all individual IP records and corresponding status. Inventory is not required for provisioning
• Grid and list displays with IP record overlays and color coding for static, available, reserved and transient status
• Manual IP Host record creation from Network Pool detail pages

Adding SolarWinds to Morpheus

1. Navigate to Infrastructure > Network > Integrations
2. Click + ADD
3. Select SolarWinds
4. Enter in the following information
   - **Name**: Name of the SolarWinds Integration in Morpheus
   - **Enabled**: Deselect to disable sync with the SolarWinds endpoint
   - **URL**: URL of the SolarWinds server, ex: http://10.30.20.10:17778
   - **Username**: Username of SolarWinds API User. See the NOTE box below for information on minimum rights requirements
   - **Password**: SolarWinds User password
5. Click SAVE CHANGES

**Note:** At minimum you will need credentials for a user with API and root-level propagating read access, as well as read/write access for target networks and domains. For a quicker solution, you can also use an account with the Power User role in situations where you aren’t concerned with providing only the minimum required access.
Consuming SolarWinds in Morpheus

On saving your new integration, SolarWinds networks will be synced and can be viewed by navigating to Infrastructure > Network > IP POOLS. They’re also viewable from the detail section of the SolarWinds integration at Infrastructure > Network > INTEGRATIONS > (your SolarWinds integration) > NETWORK POOLS.

Host records can also be viewed here by clicking on the name of a SolarWinds network.

Note: Morpheus SolarWinds integration does not support zone record syncing despite the presence of the ZONES tab on the integration detail page. This is a UI feature carried over from other networking integrations and is not supported at this time.
Adding IP Pools to Networks

Morpheus can automatically assign the next available SolarWinds IP in an IP/Network Pool and create the corresponding DNS records. Morpheus will also remove the records upon teardown. To enable this, add an SolarWinds IP/Network Pool to the Network Pool section on a Network(s).

1. Navigate to Infrastructure > Network > Networks
2. Select a Network name and click EDIT
3. In the NETWORK POOL typeahead field, search for and select the name of the selected IP/Network Pool.
   • Gateway, DNS, and CIDR must be populated for static/pool IP assignment
   • Select ALLOW IP OVERRIDE, if desired, to allow selecting between DHCP, static IP address entry, and pool address selection at provision time
   • Deselect DHCP server if a DHCP server will not be used on the network (only static and/or IP Pool IP assignment)
4. Select SAVE CHANGES

Creating Host Records

1. Select a Network Pool from Infrastructure > Network > IP POOLS
2. Click + ADD
3. Enter the following
   HOSTNAME  Hostname for the record
   IP ADDRESS  IP address for the Host Record
4. Select SAVE CHANGES

12.22.8 Unisys Stealth

Introduction

Unisys Stealth is a network security tool for safeguarding sensitive information across shared networks. By creating pre-defined communities of interest (COIs) and curating user access to these groups, the need to create separate networks for handling restricted data is reduced.

Morpheus includes a full integration with Stealth allowing administrators to create and manage COIs, work with configurations and roles, and provision new endpoints into COIs.
Stealth Concepts

- **Communities of Interest (COIs):** A collection of endpoints cryptographically separated so they can only communicate to each other

- **Endpoints:** Any system or device with a Stealth agent

- **Configuration:** Tells the endpoints which authorization methods and services to use for obtaining COI membership

- **Role:** Defines COI membership. Users and groups are assigned to a role which grants access to that role’s COIs

- **Filters:** Customizes Stealth communication. More specifically, filters constrain Stealth communication to specific addresses, ports, or protocols and allow Stealth endpoints to communicate with non-Stealth endpoints

Integrating Stealth with Morpheus

1. Navigate to Infrastructure > Network > Integrations
2. Click + ADD
3. Complete the following fields:
   - **NAME:** A name for this Stealth integration in Morpheus
   - **API HOST:** The address for the server hosting Stealth (ex: https://x.x.x.x:8448)
   - **USERNAME:** A username for the portaladmin, or the user who logs into the web console
   - **PASSWORD:** A password for the account
   - **MANAGER USERNAME:** A username for the manager account
   - **MANAGER PASSWORD:** A password for the manager account
4. Click ADD SECURITY INTEGRATION
Summary View

The default view when accessing a Stealth integration in Morpheus is the Summary view. In addition to basic information about the Stealth server itself, we can see system status, license and service information.
Endpoints

Endpoints are any system or device with a Stealth agent. Stealth endpoints can be provisioned in Morpheus in the same way other cloud resources are provisioned. With Stealth integrated, workloads provisioned on the appointed networks are assigned Stealth configuration and a Stealth role during the provisioning process. Based on a user’s assigned roles and COIs assigned to those roles, only workloads on the appointed COIs will be visible to the user. Additionally, workloads can only see other workloads within their COI.

Note: Machines on the same network which are not Stealth-managed will be able to see and communicate with each other but will not be able to see workloads which are assigned to a Stealth COI.

Endpoints View

The endpoints view will display all available Stealth-managed resources. Endpoints are not created here but will be synced into this view as they are created (through Morpheus provisioning or outside creation). Stealth-managed endpoints can be deleted by clicking the trash can icon at the end of each row in this view.

The following fields are exposed in the endpoints list view:

- DISPLAY NAME
- NAME
- DESCRIPTION
**Configurations**

Configurations in Stealth are the top-level construct and house COIs, roles, groups, users and endpoints. Your Stealth integration will include at least one configuration but often they will include more.

Configurations are primarily created and managed from the Stealth console but we can opt to remove them from Morpheus by clicking the trash can icon at the end of each row on the configurations list page. Configurations are selected along with a Stealth role at provision time in Morpheus.

**Configurations View**

The following fields are exposed in the configurations list view:

- **NAME:** The name of the configuration
- **DESCRIPTION:** A description value for the configuration

**Roles**

Users are placed into roles which are associated with COIs. A user’s role(s) determine which COIs he or she will be able to see and access. Roles are synced into Morpheus once the integration process is complete and can be viewed in the Roles list view. Roles can also be created from the Morpheus integration as described later in this section.

**Roles View**

The following fields are exposed in the roles list view:

- **NAME:** The name of the role
- **DESCRIPTION:** A description value for the role

**Note:** More detail on each item in the roles list can be revealed by clicking on the (i) icon in each row, including the COIs associated with the role.

**Creating Stealth Roles**

1. Navigate to Infrastructure > Network > Integrations > (Your Stealth integration) > Roles
2. Click + CREATE ROLE
3. Complete the following fields:
   - **NAME:** The name for the new role
   - **DESCRIPTION:** A description value for the new role
   - **CONFIGURATION:** Select an existing Stealth configuration to associate with the role
   - **ROLE TYPE:** Identifies how the role is used. Can be Global (for roles used to isolate endpoints and users), Service (for roles used by endpoints in service mode to access an authorization service) or Work-Group (for roles used by endpoints in normal operation)
   - **FILTER SET:** Choose a filter set to apply to the role to allow or deny clear text communication with non-Stealth-managed endpoints
• **COIs**: Select the COIs to be associated with the role

• **PROVISION CHANGES**:

4. Click *ADD ROLE*

![ADD ROLE Form](image)

**COIs (Communities of Interest)**

COIs exist within configurations and create a logical separation between endpoints in separate COIs. Communication between endpoints in the COI is encrypted and those outside the COI are unable to see or access endpoints despite being on the same network.

On completing the integration, Morpheus will sync in existing COIs. COIs can also be created from Morpheus UI which is described later in this section. COIs are deleted by clicking on the trash can icon at the end of each row in the COIs list view.
COIs View

The following fields are exposed in the roles list view:

• **NAME:** The name of the COI
• **DESCRIPTION:** A description value for the COI

Creating Stealth COIs

1. Navigate to Infrastructure > Network > Integrations > (Your Stealth integration) > COIs
2. Click + *CREATE COI*
3. Complete the following fields:
   • **NAME:** The name for the new COI
   • **DESCRIPTION:** A description value for the new COI
   • **TYPE:** Workgroup or Service
   • **DIRECTION:** Default (enables COI to accept inbound and initiate outbound tunnels), Initiate (restricts the COI to only initiate outbound tunnels), or Accept (restricts the COI to only accept inbound tunnels)
4. Click *CREATE COI*
Filters

Filters customize Stealth communication. More specifically, filters constrain Stealth communication to specific addresses, ports, or protocols and allow Stealth endpoints to communicate with non-Stealth endpoints.

Filters are synced into Morpheus when integrating with Stealth and are viewable from the filters list view. They are created and managed from within the Stealth console itself.

When accessing the filters list view, all filter sets are displayed. Each filter set can be expanded to view the individual filters within. Information on each filter is displayed once the filter set has been expanded to reveal the individual filters.

Provisioning with Stealth

In order to provision new Stealth-managed endpoints, Stealth must be integrated with Morpheus as described above. In addition, Stealth must be selected as the Security Server for the cloud you’re provisioning into. Security servers can be selected at the time a new Cloud integration is created or by editing an existing Cloud integration.

Choosing a Cloud Security Server

Assuming the Cloud is already integrated with Morpheus, use the steps below to set the security server and activate Stealth prompts at provision time. The steps to set the security server during the time the cloud is initially integrated with Morpheus is very similar.

1. Navigate to Infrastructure > Clouds > (Your Selected Cloud)
2. Click EDIT
3. Click on Advanced Options to reveal additional selections
4. In the dropdown for SECURITY SERVER, choose an existing Stealth integration

Provisioning to a Stealth-enabled Cloud

Once we have selected our Stealth integration as the security server for at least one Cloud in Morpheus, new Instances (endpoints) can be provisioned and managed by Stealth.

1. Navigate to Provisioning > Instances
2. Click ADD
3. Select the Instance Type, Cloud, and Group making sure to choose a Cloud that has been set up for an existing Stealth integration
4. On the Configure tab of the provisioning wizard, choose a Stealth Configuration and a Stealth Role according to the needs of the machine(s) being provisioning
5. Once the provisioning process is complete, the new Stealth-managed endpoints will be available and restricted based on the Stealth implementation
12.23 Storage

12.23.1 3Par

Adding 3Par Storage Server

1. Select the Infrastructure link in the navigation bar.
2. Select the Storage link in the sub navigation bar.
3. In the SERVERS tab, Click the + ADD button.
4. From the ADD STORAGE SERVER wizard input the following:
   NAME  Name of the Storage Server in Morpheus
TYPE  Select 3Par
URL  URL Of 3Par Server Example : https://192.168.190.201:8008
USERNAME  Add your administrative user account.
PASSWORD  Add your administrative password.
5. Select SAVE CHANGES
The 3Par Storage Server will be added and displayed in the Buckets tab.
Buckets, Files Shares and Storage Groups will be synced in.

12.23.2 AzureStorage

To Add Azure Storage

1. Navigate to Infrastructure > Storage
2. Select + ADD
3. From the New Storage Provider Wizard input the following:
   Name  Name of the storage provider.
   Provider Type  Azure
   Storage Account  Add Storage Account
   Storage Key  Add Storage Key
   Share Name  Add Share Name
   Targets
      • Default Backup Target
      • Default Deployment Archive Target
      • Default Virtual Image Store
4. Save Changes

12.23.3 Dell ECS

Overview

Morpheus integrates with DELL EMC ECS via the ECS api. This allows Morpheus to talk directly to the ECS services.
When you add a ECS Server, Morpheus will sync in the following.
   • Storage Groups
   • Buckets
   • File shares
Users will be able to create the following items within ECS without direct access to the ECS console.
   • Buckets
   • File shares
Storage Servers

The first step in the Dell EMC ECS integration is to add a Dell EMC ECS Storage Server. Once added, Buckets, Files Shares and Storage Groups will be synced in and can be access and managed in Morpheus.

Adding Dell EMC ECS Storage Server

1. Select the Infrastructure link in the navigation bar.
2. Select the Storage link in the sub navigation bar.
3. In the SERVERS tab, Click the + ADD button.
4. From the ADD STORAGE SERVER wizard input the following:
   NAME  Name of the Storage Server in Morpheus
   TYPE  Select Dell EMC ECS
   URL  URL Of DELL EMC ECS Server Example : https://192.168.190.200:4443

   Tip:  The port 4443 is the api port for ECS api. This may be different depending on your configuration

   USERNAME  Add your administrative user account.
   PASSWORD  Add your administrative password.
   S3 SERVICE URL (Optional)  Add your S3 service url Example: http://192.168.190.220:9020

   Note:  S3 SERVICE URL is not required if you are not planning on using ECS S3.

5. Select SAVE CHANGES

The Dell EMC ECS Storage Server will be added and displayed in the Buckets tab.

Buckets

- Buckets will be listed in Infrastructure - Storage - Buckets
  - Buckets can be created and deleted with Infrastructure - Storage Role Permissions
  - Buckets can be browsed with Infrastructure: Storage Browser Role permissions
  - File and folders can be uploaded, downloaded and deleted with Full Infrastructure: Storage Browser Role permissions.
Adding Dell EMC ECS Buckets

Note: A Dell ECS Storage Server must be configured in Infrastructure - Storage - Servers prior to adding a Dell ECS Bucket.

To Add a Dell ECS Storage Bucket:

1. Select the Infrastructure link in the navigation bar.
2. Select the Storage link in the sub navigation bar.
3. In the BUCKETS tab, Click the + ADD button.
4. Select Dell EMC ECS Bucket from the dropdown list.
5. From the NEW BUCKET Wizard input the following:
   
   NAME  Name of the Bucket in Morpheus.
   
   STORAGE SERVICE Select existing Dell EMC ECS Storage Server (configured in Infrastructure - Storage - Servers)
   
   BUCKET NAME Enter a name for the new Dell ECS bucket.
   
   USER Your Dell EMC ECS S3 user account
   
   SECRET KEY
   
   Your Dell EMC ECS S3 Secret Example: jW+pFyAptSS5FuEqKwt44xlpM/2
   
   NAMESPACE Select Dell EMC ECS Namespace for the Bucket
   
   STORAGE GROUP Select a Dell EMC ECS Storage Group
   
   Default Backup Target Sets this bucket as the default backup target when creating Backups. If selected the option to update existing Backup configuration to use this Bucket will be presented.
   
   Archive Snapshots Enabled to export VM snapshots to this Bucket when creating VMware Backups, after which the snapshot will be removed from the target hypervisor.
   
   Default Deployment Archive Target Sets this Bucket as the default storage target when uploading Deployment files in the Deployments section.
   
   Default Virtual Image Store Sets this bucket as the default storage target when uploading Virtual Images from the Virtual Images section, importing Images from Instance Actions, creating Images with the Image Builder and when creating new images from Migrations.
   
   RETENTION POLICY
   
   None Files in the Bucket will not be automatically deleted or backed up.
   
   Backup Old Files
   
   This option will backup files after a set amount if time and remove them from the bucket.
   
   DAYS OLD Files older than the set number of days will be automatically backed up to the selected Backup Bucket.
   
   BACKUP BUCKET Search for and select the Bucket the files will be backed up to.
   
   DELETE OLD FILES
   
   This option will delete files from this bucket after a set amount of days.
DAYS OLD  Files older than the set number of days will be automatically deleted from the Bucket.

6. Select SAVE CHANGES

The Bucket will be created and displayed in the Buckets tab.

- To browse, upload, download, or delete files from this Bucket, select the name of the Bucket.
- To edit the Bucket, select the edit icon or select the name of the Bucket and select ACTIONS - EDIT.

**Warning:** Repointing a bucket that is in use may cause loss of file references. Ensure data is mirrored first.

- To delete a Bucket, select the trash icon or select the name of the Bucket and select DELETE.

**Warning:** When deleting a Bucket, all Deployment Versions and Backups associated with the Bucket will be deleted.

---

**Add Dell EMC ECS File Shares**

To Add a Dell EMC ECS File Share:

1. Select the Infrastructure link in the navigation bar.
2. Select the Storage link in the sub navigation bar.
3. In the FILE SHARES tab, Click the + ADD button.
4. Select Dell EMC ECS Share from the dropdown list
5. From the NEW FILE SHARE Wizard input the following:
   - **NAME** Name of the File Share in Morpheus.
   - **STORAGE SERVICE** Select existing Dell EMC ECS Storage Server (configured in Infrastructure - Storage - Servers)
   - **SHARE PATH** Enter Dell EMC ECS Share Path  Example: ecs-file-share-1
   - **USER** Dell EMC ECS User
   - **SECRET KEY** Dell EMC ECS Secret key
   - **Volume Size** Specify volume size for the File Share (in MB)
   - **Allowed IP’s** Specify IP Addresses to limit accessibility to the File Share
     - Leave blank for open access Click the + symbol to the right of the first ALLOWED IPS field to add multiple IP’s
   - **NAMESPACE** Select Dell EMC ECS Namespace (synced)
   - **STORAGE GROUP** Select Dell EMC ECS Storage Group (synced)
   - **Default Backup Target** Sets this File Share as the default backup target when creating Backups. If selected the option to update existing Backup configuration to use this File Share will be presented.

---

12.23. Storage
Archive Snapshots  Enabled to export VM snapshots to this File Share when creating VMware Backups, after which the snapshot will be removed from the source Cloud.

Default Deployment Archive Target  Sets this File Share as the default storage target when uploading Deployment files in the Deployments section.

Default Virtual Image Store  Sets this File Share as the default storage target when uploading Virtual Images from the Virtual Images section, importing Images from Instance Actions, creating Images with the Image Builder and when creating new images from Migrations.

RETENTION POLICY

None  Files in the File Share will not be automatically deleted or backed up.

Backup Old Files

This option will backup files after a set amount if time and remove them from the File Share.

DAYS OLD  Files older than the set number of days will be automatically backed up to the selected Backup File Share.

BACKUP File Share  Search for and select the File Share the files will be backed up to.

DELETE OLD FILES

This option will delete files from this File Share after a set amount of days.

DAYS OLD  Files older than the set number of days will be automatically deleted from the File Share.

6. Select SAVE CHANGES

The File Share will be created and displayed in the File Shares tab.

- To browse, upload, download, or delete files from this File Share, select the name of the File Share.
- To edit the File Share, select the edit icon or select the name of the File Share and select ACTIONS - EDIT.

**Warning:** Repointing a File Share that is in use may cause loss of file references. Ensure data is mirrored first.

- To delete a File Share, select the trash icon or select the name of the File Share and select DELETE.

**Warning:** When deleting a File Share, all Deployment Versions and Backups associated with the File Share will be deleted.

12.23.4 Isilon

Add Dell EMC Isilon Storage Server

**Important:** Enable insecure mode on the NFS settings. This allows non-root ports to be used. Setting the insecure/privileged mode will require a restart of the Isilon nodes.

1. Select the Infrastructure link in the navigation bar.
2. Select the Storage link in the sub navigation bar.
3. In the SERVERS tab, Click the + ADD button.

4. From the ADD STORAGE SERVER wizard input the following:
   - NAME  Name of the Storage Server in Morpheus
   - TYPE  Select Dell EMC Isilon
   - USERNAME  Add your administrative user account.
   - PASSWORD  Add your administrative password.
   - PROVISION USER  Select Provision User
   - PROVISION GROUP  Select Provision Group
   - ROOT PATH
     - Enter Root Path  Example: \\n
5. Select SAVE CHANGES

The Dell EMC Isilon Storage Server will be added and displayed in the Buckets tab.
Buckets, Files Shares and Storage Groups will be synced in.

Add Dell EMC Isilon File Share

To Add a Dell EMC Isilon File Share:
1. Select the Infrastructure link in the navigation bar.
2. Select the Storage link in the sub navigation bar.
3. In the FILE SHARES tab, Click the + ADD button.
4. Select Dell EMC Isilon Share from the dropdown list
5. From the NEW FILE SHARE Wizard input the following:
   - NAME  Name of the File Share in Morpheus.
   - STORAGE SERVICE  Select existing Dell EMC Isilon Storage Server (configured in Infrastructure - Storage - Servers)
   - SHARE PATH
     - Enter Dell EMC Isilon Share Path  Example: ecs-file-share-1
   - Volume Size  Specify volume size for the File Share (in MB)
   - Allowed IP’s
     - Specify IP Addresses to limit accessibility to the File Share
       - Leave blank for open access  Click the + symbol to the right of the first ALLOWED IPS field to add multiple IP’s
   - NAMESPACE  Select Dell EMC Isilon Namespace (synced)
   - STORAGE GROUP  Select Dell EMC Isilon Storage Group (synced)
   - Default Backup Target  Sets this File Share as the default backup target when creating Backups. If selected the option to update existing Backup configuration to use this File Share will be presented.
**Morpheus Documentation**

**Archive Snapshots** Enabled to export VM snapshots to this File Share when creating VMware Backups, after which the snapshot will be removed from the source Cloud.

**Default Deployment Archive Target** Sets this File Share as the default storage target when uploading Deployment files in the Deployments section.

**Default Virtual Image Store** Sets this File Share as the default storage target when uploading Virtual Images from the Virtual Images section, importing Images from Instance Actions, creating Images with the Image Builder and when creating new images from Migrations.

**RETENTION POLICY**

None Files in the File Share will not be automatically deleted or backed up.

Backup Old Files

This option will backup files after a set amount if time and remove them from the File Share.

- **DAYS OLD** Files older than the set number of days will be automatically backed up to the selected Backup File Share.

- **BACKUP File Share** Search for and select the File Share the files will be backed up to.

DELETE OLD FILES

This option will delete files from this File Share after a set amount of days.

- **DAYS OLD** Files older than the set number of days will be automatically deleted from the File Share.

6. Select **SAVE CHANGES**

The File Share will be created and displayed in the File Shares tab.

- To browse, upload, download, or delete files from this File Share, select the name of the File Share.

- To edit the File Share, select the edit icon or select the name of the File Share and select **ACTIONS - EDIT**.

**Warning:** Repointing a File Share that is in use may cause loss of file references. Ensure data is mirrored first.

- To delete a File Share, select the trash icon or select the name of the File Share and select **DELETE**.

**Warning:** When deleting a File Share, all Deployment Versions and Backups associated with the File Share will be deleted.

### 12.24 Supported Integration Versions

Morpheus supports an extensive range of software integrations and versions past and present. Current iterations of Amazon AWS, Microsoft Azure, Google Cloud Platform, Digital Ocean, HPE OneView, OpenTelekom Cloud, IBM Bluemix, Softlayer and UpCloud are all supported.

In addition, Morpheus is verified to work with, but not limited to:
### 12.24.1 Integrations

**Note:** Current iterations of Amazon AWS, Microsoft Azure, Google Cloud Platform, Digital Ocean, HPE OneView, OpenTelekom Cloud, IBM Bluemix, Softlayer and UpCloud are all supported.

<table>
<thead>
<tr>
<th>Integration</th>
<th>Supported Version(s)</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ansible</td>
<td>2.7.x</td>
<td></td>
</tr>
<tr>
<td>Ansible Tower</td>
<td>3.8.x</td>
<td></td>
</tr>
<tr>
<td>App Dynamics</td>
<td>4.5.x</td>
<td></td>
</tr>
<tr>
<td>Azure Stack</td>
<td>2002 back to 1908</td>
<td>2019-03-01-hybrid api-profile version used which is supported in 1908 and later Azure Stack versions</td>
</tr>
<tr>
<td>Cisco ACI</td>
<td>3.10</td>
<td></td>
</tr>
<tr>
<td>Citrix Netscaler</td>
<td>v12.1</td>
<td></td>
</tr>
<tr>
<td>Commvault</td>
<td>v11 sp 19</td>
<td></td>
</tr>
<tr>
<td>F5 Big-IP</td>
<td>11.4+</td>
<td></td>
</tr>
<tr>
<td>Infoblox</td>
<td>Latest Versions Supported</td>
<td></td>
</tr>
<tr>
<td>Jenkins</td>
<td>2.x</td>
<td></td>
</tr>
<tr>
<td>Kubernetes</td>
<td>1.x</td>
<td></td>
</tr>
<tr>
<td>Microsoft Hyper-V</td>
<td>2012R2, 2016, 2019</td>
<td></td>
</tr>
<tr>
<td>Nutanix AHV</td>
<td>5.0 - 5.10 Note: Prism Central is not a supported endpoint</td>
<td>In 5.5 - 5.7 if Prism Central is managing Prism Element, image creation will not function due to PC Image Management.</td>
</tr>
<tr>
<td>Openstack</td>
<td>Latest Versions Supported</td>
<td>When creating an OpenStack integration, select the latest available from the OS Version dropdown menu when running a later version</td>
</tr>
<tr>
<td>Rubrik</td>
<td>4.2</td>
<td></td>
</tr>
<tr>
<td>SCVMM</td>
<td>2016, 2019</td>
<td></td>
</tr>
<tr>
<td>ServiceNow</td>
<td>Orlando, Paris, Quebec, Rome</td>
<td></td>
</tr>
<tr>
<td>Terraform</td>
<td>v0.11.x, v0.12.18+, 0.13.x, 0.14.x</td>
<td></td>
</tr>
<tr>
<td>vCloud Director</td>
<td>8.20, 9.1, 9.5, 9.7, 10.0, 10.2</td>
<td>vCD 9.7+ supported on API v31, vCD 10.2+ supported on API v34.0</td>
</tr>
<tr>
<td>Veeam</td>
<td>9.5u3, 9.5u4, 10, 11</td>
<td></td>
</tr>
<tr>
<td>VMware ESXi</td>
<td>5.5, 6.0, 6.5, 6.7, 7</td>
<td></td>
</tr>
<tr>
<td>VMware Fusion</td>
<td>8, 9, 10+</td>
<td></td>
</tr>
<tr>
<td>VMware NSX</td>
<td>-V, -T v3.1.1</td>
<td></td>
</tr>
<tr>
<td>VMware vCenter</td>
<td>5.5, 6.0, 6.5, 6.7, 7</td>
<td></td>
</tr>
<tr>
<td>XenServer</td>
<td>7.x</td>
<td></td>
</tr>
</tbody>
</table>
Note: Non-listed versions may be compatible but are not verified.

Note: Non-listed versions may be compatible but are not verified.

If you have any specific requirements please contact support@morpheusdata.com
v5.3.4 RELEASE NOTES

Note: Items appended with 5.x.x are also included in that version

13.1 Navigation Updates

v5.3.4 contains major changes to the UI navigation structure. The following table lists updated paths for affected sections.

Note: API endpoints are not affected by the UI navigation changes
<table>
<thead>
<tr>
<th>Target</th>
<th>Old Path</th>
<th>New Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blueprints</td>
<td>provisioning &gt; blueprints</td>
<td>library &gt; blueprints</td>
</tr>
<tr>
<td>Automation</td>
<td>provisioning &gt; automation</td>
<td>library &gt; automation</td>
</tr>
<tr>
<td>Tasks</td>
<td>provisioning &gt; automation &gt; tasks</td>
<td>library &gt; automation &gt; tasks</td>
</tr>
<tr>
<td>Workflows</td>
<td>provisioning &gt; automation &gt; workflows</td>
<td>library &gt; automation &gt; workflows</td>
</tr>
<tr>
<td>Executions</td>
<td>provisioning &gt; automation &gt; executions</td>
<td>provisioning &gt; executions</td>
</tr>
<tr>
<td>Scale Thresholds</td>
<td>provisioning &gt; automation &gt; executions</td>
<td>library &gt; automation &gt; scale thresholds</td>
</tr>
<tr>
<td>Power Scheduling</td>
<td>provisionig &gt; automation &gt; power scheduling</td>
<td>library &gt; automation &gt; power scheduling</td>
</tr>
<tr>
<td>Execute Scheduling</td>
<td>provisioning &gt; automation &gt; execute scheduling</td>
<td>library &gt; automation &gt; execute scheduling</td>
</tr>
<tr>
<td>Automation Integrations</td>
<td>provisioning &gt; automation &gt; integrations</td>
<td>library &gt; integrations</td>
</tr>
<tr>
<td>Security Packages</td>
<td>provisioning &gt; jobs &gt; security packages</td>
<td>library &gt; templates &gt; security packages</td>
</tr>
<tr>
<td>Virtual Images</td>
<td>provisioning &gt; virtual images</td>
<td>library &gt; virtual images</td>
</tr>
<tr>
<td>Library</td>
<td>provisionig &gt; library</td>
<td>library</td>
</tr>
<tr>
<td>Instance Types</td>
<td>provisionig &gt; library &gt; instance types</td>
<td>library &gt; blueprints &gt; instance types</td>
</tr>
<tr>
<td>Layouts</td>
<td>provisioning &gt; library &gt; layouts</td>
<td>library &gt; blueprints &gt; layouts</td>
</tr>
<tr>
<td>Node Types</td>
<td>provisionig &gt; library &gt; node types</td>
<td>library &gt; blueprints &gt; node types</td>
</tr>
<tr>
<td>Option Types (Inputs)</td>
<td>provisionig &gt; library &gt; option types</td>
<td>library &gt; options &gt; inputs</td>
</tr>
<tr>
<td>Option Lists</td>
<td>provisionig &gt; library &gt; option lists</td>
<td>library &gt; options &gt; option types</td>
</tr>
<tr>
<td>File Templates</td>
<td>provisionig &gt; library &gt; file templates</td>
<td>library &gt; templates &gt; file templates</td>
</tr>
<tr>
<td>Scripts</td>
<td>provisionig &gt; library &gt; scripts</td>
<td>library &gt; templates &gt; script templates</td>
</tr>
<tr>
<td>Spec Templates</td>
<td>provisionig &gt; library &gt; spec templates</td>
<td>library &gt; templates &gt; spec templates</td>
</tr>
<tr>
<td>Cluster Layouts</td>
<td>provisionig &gt; library &gt; cluster layouts</td>
<td>library &gt; blueprints &gt; cluster layouts</td>
</tr>
<tr>
<td>Catalog/Self Service</td>
<td>tools &gt; self service</td>
<td>library &gt; blueprints &gt; catalog items</td>
</tr>
<tr>
<td>Service Catalog</td>
<td>service catalog persona</td>
<td>provisioning &gt; catalog &amp; service catalog persona</td>
</tr>
<tr>
<td>Logs</td>
<td>logs</td>
<td>monitoring &gt; logs</td>
</tr>
</tbody>
</table>

### 13.2 New Features

**API & CLI**

- Added BGP configuration for Tier-0 routers via Morpheus API and CLI \(^5.2.12\)
- Added static route configuration for Tier-0 and Tier-1 routers via Morpheus API and CLI \(^5.2.12\)
- Improved NSX-T Tier-0 and Tier-1 Gateway configuration via Morpheus API \(^5.2.12\)
- Snapshot support added to billing API
- Virtual Image support added to billing API

**Amazon**

- EKS now supported for all regions with AWS EKS services. Added us-west-1, `ap-east-1`, `ap-south-1`, `ap-northeast-3`, `ca-central-1`, `eu-south-1`, `me-south-1`, `sa-east-1`, `sa-gov-east-1` & `us-gov-west-1`
Morpheus Documentation

Azure

- Updated Azure costing sync to account for Azure CSP customers using Azure Plan 5.2.12
- When using Azure global clouds, available storage accounts are now filtered by the location of the resource group. Previously this list was unfiltered and provisioning could fail if the resource group and storage account were in different locations

Clusters

- Add Cluster and Add Host Wizards now show pricing information on the confirmation page of the wizard, as the Add Instance Wizard does

Dashboard

- Added performance improvements for Morpheus Dashboard (UI and calls to the Dashboard API) in specific scenarios where Morpheus is managing a very high number of workloads 5.2.11

Inputs

- Added new Text Area Input-type. Users can determine the size of the text area by specifying the number of rows

Morpheus Worker

- The Morpheus worker can now also be used as a proxy server between the Morpheus appliance and on-prem Cloud hosts. See the install guide for more details

NSX

- Added UI tab for NSX-T DHCP management (Infrastructure > Networks > Integrations > Selected NSX-T integration > DHCP tab) 5.2.11
- Added ability to specify a member group to be associated with NSX-T load balancer server pools 5.2.12
- Added capability to create and manage BGP neighbors for NSX-T routers 5.2.12
- Added support for configuring DHCP on NSX-T routers. When adding or editing an NSX-T router (Infrastructure > Networks > Routers > Selected NSX-T router > EDIT button), expand the IP address management section and configure DHCP options 5.2.11
- Fixed NSX-T distributed firewall missing source and destination types in Morpheus UI 5.2.12
- Source and destination IP addresses for distributed firewall rules (of any category) are now synced back to Morpheus 5.2.11
- Sync, create and manage NSX-T DHCP relays 5.2.11
- Sync, create and manage NSX-T DHCP servers 5.2.11

Plugins

- Added ability to create network-type plugins for performing CRUD operations on networks and subnets. See the Morpheus Developer Portal for more information.
- Added plugin support for Delete Approval policies
- Added plugin support for Reconfigure Approval Policies
- Added plugin support for associating virtual images with node types

Policies

- Added approve delete policies, these can be tied into internal (Morpheus) approvals or approvals through a ServiceNow integration
• Added reconfigure approval policies, which tie into either internal (Morpheus) approvals or approvals through a ServiceNow integration

Reports

• Added Tag Compliance Inventory report to show VMs which are outside of existing tag compliance policies

Security

• jknack/handlebars.java updated to 4.3.0 (CVE-2021-23369)

Service Catalog

• Self-Service Catalog provisioning is now available from the standard Persona (Provisioning > Catalog) in addition to the dedicated Persona it has always existed in.

ServiceNow

• CMDB sync times significantly improved
• ServiceNow RITM and CI records are now updated even when provisioning fails
• object_id now set correctly for discovered servers so that matches can be made rather than duplicates when discovery is enabled both in Morpheus and ServiceNow

UI

• After receiving a password reset email and submitting the form to reset the password, the user is redirected to the login screen rather than logged into the product. This ensures two-factor authentication is still honored if set.
• Errors are now surfaced into the History tab of the Instance detail page if issues occur when taking Snapshots in supported Clouds
• Localization features added, including a global language settings and override capabilities for individual users
• Reorganized main application menu. The Library, which was previously under Provisioning, is now a top-level section. Service Catalog provisioning can now be done in the Standard Persona in addition to the Service Catalog Persona. Many more smaller changes

VMware

• The root Folder (/) is now exposed in VMware Cloud Resources sections, allowing the same configuration and access control as sub-folders. Previously configuration and access settings were only exposed for sub-folders

13.3 Fixes

API & CLI

• API calls to get all servers or to get a specific server no longer contain duplicate zone or plan keys
• Added additional prompts to the network-routers add CLI workflow to enable selection of Edge Clusters and/or Tier-0 Gateways for NSX-T Tier-1 and Tier-0 Gateways
• Fixed an issue that caused GET calls for specific networks, network proxies, and network routers not to work properly for Subtenant users
• Fixed an issue that prevented custom networks from being created through Morpheus API
• Message of the Day (MOTD)-type Policies are now returned when issuing GET requests for policies 5.2.11

• Resizing network interface counts via Morpheus API no longer causes VMs to reboot under certain conditions 5.2.12

• The `clone` API endpoint now accepts `tag` and `label` payloads correctly. Previously they needed to be issued using a legacy format which caused confusion 5.2.12

• The content (script) of PowerShell Tasks is now displayed correctly when creating or viewing such Tasks in Morpheus CLI 5.2.12

• Users can now add Layouts to default Instance Types via Morpheus API and CLI 5.2.12

• When issuing GET calls for specific Instances, controller information is now populated in the response 5.2.11

• When issuing a Tenant delete call to Morpheus API, the `removeResources` flag is now `true` by default. Previously, this was `false` by default 5.2.12

• When making a GET call for all Instances or for a specific Instance, Morpheus-generated system tags are no longer returned 5.2.12

• When provisioning an Instance or getting a specific Instance via API, the `labels` and `tags` objects are now returned even when there are no labels or tags

Amazon

• Amazon plans are now synced rather than seeded into the product by Morpheus. This should ensure any currently-valid plan is available

• Disks added to VMs after provisioning are now deleted along with the VM at teardown time. Previously disks added later would remain 5.2.12

• Updates made to base Ubuntu 18 image for AWS 5.2.11

Ansible

• Fixed an issue which caused Ansible integrations not to inherit the “No Proxy” configuration in global Appliance Settings (Administration > Settings > Appliance) 5.2.12

Apps

• Corrected an issue that caused Instance counts on Apps to appear incorrectly to users which weren’t the owner of the App 5.2.12

• Fixed an issue where App Instances would default to one CPU core at provision time rather than the default number of CPU cores indicated on the Blueprint 5.2.11

• When provisioning multi-tier Apps, environment variables are now set at a consistent time following App completion to ensure data accuracy 5.2.12

Automation

• Reassigning an Instance from the Primary Tenant to a Subtenant will no longer break Ansible Task execution in certain cases 5.2.11

Azure Stack

• Removed the ability to select certain unsupported disk types from the provisioning wizard. Selecting these types would cause the provisioning to fail if the user did not know those types were not allowed 5.2.11

Azure

• Adding resource pools to Azure Clouds which are scoped to all regions now works correctly
• Fixed an issue that caused Instance or server details (plan, datastore, etc.) not to display corrected when reconfiguring an Instance or server that was previously converted to managed 5.2.12

• The Edit Instance dialog can now be used to change the Group on a SQL Server DBaaS on Azure Instance 5.2.12

• When provisioning to Azure using ARM Spec Templates, a “pending” string is no longer temporarily appended to server names during the provisioning process which caused DNS issues in some cases 5.2.12

BIND DNS

• Improved form validation when creating a BIND DNS integration. Previously 500 errors would be thrown or some fields would disappear when attempting to submit the form

Backups

• Backup “Total Size” is no longer reported incorrectly in the UI when it exceeds 1 TB in size 5.2.12

• Execute timings for scheduled backup jobs now update immediately in the UI on saving changes to the schedule. Previously the UI change could take a short time which caused confusion 5.2.12

Blueprints

• The expand and contract button for configuration options now works correctly. Previously it defaulted to the expanded state and could not be contracted 5.2.11

Buckets

• Fixed an issue that could cause non-Amazon S3 buckets to fail on creation when specific string sequences were contained in the endpoint URL 5.2.11

Catalog

• Removed some default ElasticSearch Layouts which contained outdated versions and failed provisioning under certain scenarios

Chef

• Improved validation on the Create Chef Integration modal. The validity of the Chef server URL is now verified before saving the new integration 5.2.12

• Improved validation on the success of Chef bootstrap task execution 5.2.12

Clone

• Fixed an issue that could cause NICs to be reordered during the clone process which created connectivity issues 5.2.12

• Removed “autoCluster” as Datastore selection when a different Cloud is selected as target Cloud for the new clone. This is because the datastore might not be reachable from a different destination cloud and cause provisioning failures 5.2.12

Costing

• Fix issue where duplicate invoice records were generated for first occurrence of an invoice in a period 5.2.12

ESXi

• The number of CPU cores on discovered ESXi VMs is now synced correctly 5.2.11

File Templates
• Fixed location shown in node type displaying old value after updating the paths of associated file template 5.2.12

Github

• Github integrations now sync correctly for appliances configured to route traffic through a global proxy 5.2.12

Groups

• Fixed an issue where Groups with no assigned Clouds would be able to see managed and discovered VMs in any Cloud 5.2.11

Guidance

• Corrected an issue that would cause incorrect guidance to be given for Azure Instances 5.2.12

Hosts

• Under certain conditions, the platform for discovered servers could be reported incorrectly. This has been fixed 5.2.12

Identity Sources

• Fixed an issue that caused errors to be thrown when configuring a logout redirect URL for Azure AD SSO identity source integrations 5.2.12

Instances

• Fixed an issue that caused details not to be loaded in properly to a reconfigure modal after converting a discovered VM with multiple disks to managed 5.2.12
• Fixed an issue that caused errors to appear and made it impossible to add a new node to an Instance which had all of its nodes removed 5.2.12
• Fixed an issue where networks would not be set correctly on a node added to an Instance when existing nodes had multiple networks, including IPAM networks 5.2.12
• When provisioning multi-NIC Instances, it could take time for additional network interface information to populate in Morpheus. This has been corrected 5.2.12

Invoices

• Invoices are no longer being created for workloads which were awaiting provisioning approval, then cancelled or deleted 5.2.12

KVM

• Fixed an issue which would cause the Instance wizard not to advance under specific configurations due to missing datastore information even when a datastore was selected 5.2.12

Kubernetes

• Fixed issues with AKS and EKS Create Cluster modals, including field marked required having no validation
• useGuestCustomization flag now set to true when provisioning Kubernetes hosts into vCD using IP Pools, even when FORCE GUEST CUSTOMIZATION is unchecked, to ensure proper provisioning

Localization

• Missing string definitions added 5.2.12

NSX-T
• Certain errors are no longer surfaced into the logs when NSX-T integrations are refreshed 5.2.11
• Certain errors are no longer triggered when NSX-T integrations are refreshed 5.2.11
• Created NSX-T load balancer profiles are now selectable from virtual servers 5.2.11

NSX

• Fix NSX-T sync issue where segments (networks) were being disassociated from sub-tenant zones and re-associated to master tenant zones 5.2.12
• Fixed an issue causing duplicate NSX-T networks to by synced into Morpheus under certain conditions. Once the update is applied the duplicate networks will take approximately ten minutes to be removed 5.2.12
• Fixed issue with NSX-V logical router DHCP relay creation 5.2.12
• Fixed network ip pools not listing when creating NSX-T networks/segments 5.2.12 5.2.11
• Improved validation errors in UI when adding or editing an invalid uplink interface for a DLR or Edge Router 5.2.12
• The server address field is no longer a required field when creating NSX-T DHCP servers 5.2.12

Network

• Added validation to API calls to create or edit network proxies to ensure names are unique 5.2.11
• Fixed an issue causing network groups not to be handled properly on Instance or VM reconfigure 5.2.11
• Fixed an issue that caused Tenant permissions not to be set up properly for subnets in Sub-tenants 5.2.11
• Fixed an issue that caused old IP addresses not to be freed up in some scenarios when a new network and IP pool was selected on Instance reconfigure 5.2.11
• Fixed an issue that could cause NICs to be relabeled when adding a network to an Instance or server via reconfigure 5.2.11
• Fixed an issue that could cause the first network interface in the list to be automatically set as the primary during Cloud sync, even if the user had set another to be primary 5.2.12

Node Types

• AMI selection field for Amazon Node Types is now a Typeahead field. Previously, in environments with access to very large numbers of AMIs, it would not be possible to edit the AMI selection in certain scenarios due to the size of the dropdown menu 5.2.12

Nutanix

• Improved process for cleaning up IP pools when Nutanix clouds are deleted 5.2.11

OpenStack

• When Primary Tenant admins set an OpenStack Cloud and associated load balancer to be private to a Tenant, Users in the Tenant can now view load balancer detail pages 5.2.12
• When reconfiguring OpenStack Instances with multiple disks, disks no longer change size without user input in certain scenarios 5.2.11

Option Lists
• Added form validation so that invalid Option Lists could not be saved 5.2.12

• Morpheus user objects and object attributes are now accessible in LDAP-type Option Lists 5.2.11

• Validation added for JSON and CSV-based manual Option Lists. Previously these forms would accept invalid JSON and CSV which would cause the Option List not to function correctly 5.2.12

**Oracle Cloud**

• Fixed an issue that caused Oracle Cloud Flex Plan workload costs to report as significantly more expensive than they should have 5.2.12

• Fixed an issue that could cause Morpheus Agent to not be installed on Windows boxes in Oracle cloud 5.2.11

• Increased timeout on Oracle Cloud agent install to 1 Hour to account for long Windows startup times 5.2.12

**Plans & Pricing**

• Corrected an issue that caused Plans to appear differently when reconfiguring from the server detail page vs the Instance detail page 5.2.11

• Corrected some default plans which showed incorrect resource counts (core, etc.) in plan descriptions when compared to the same plan in the target cloud 5.2.12

• Improved UI warning messages and handling when attempting to reconfigure an Instance beyond the custom range of core, memory, or storage configured on its plan 5.2.12

**Policies**

• Added more validation on Policy creation. Policies now require a unique name and additional validation has been added to ensure uniqueness of the type, config and scope combination 5.2.12

• Max Cores Policies now include cores in the master node in the total cores count. Previously only worker node cores were counted toward the policy

• Policies scoped to a Tenant are no longer removed if the Tenant is deleted. The Policy now remains in Morpheus but is no longer scoped to the non-existent Tenant 5.2.12

**PowerDNS**

• Fixed an issue that limited the PowerDNS Zones List Page to just the first 25 zone entries 5.2.12

**Provisioning**

• Changes made to Cloud filtering during provisioning which will prevent users from being able to select Clouds which should not be applicable to the selected Instance Type and/or Group in certain cases 5.2.12

• Corrected an issue that caused Inputs (Option Types) not to appear correctly when provisioning from an ARM-based Spec Template which was sourced from an integrated repository 5.2.12

• Fixed issue with $sequence variable reiteration on 35 when using copies and “Reuse Naming Sequence Numbers” is enabled 5.2.11

**Proxies**

• Fixed an issue preventing proxies from being set correctly on SLES and OpenSUSE 5.2.11

**Reports**
• Corrected an issue that could cause inaccurate cost values to be shown on the Tenant Cost Report 5.2.12

• Fixed an issue that caused mismatched columns when opting for CSV output of the Cloud Migration Report 5.2.12

• Fixed an issue where Reports or Analytics dashboards could show clouds as having more discovered VMs than they would actually show from the Cloud detail page 5.2.11

Security

• Hid passwords to some Morpheus-owned service accounts (Twilio, Postmark, etc.) which were shared previously in application.groovy but are no longer needed by customers 5.2.11

• Includes important security fixes which were first corrected in patch releases for 5.2.11 (v5.2.11-2) and 5.3.3 (v5.3.3-2) 5.2.12

• Percent symbols (%) are now escaped correctly in usernames when logging in 5.2.12

• Subtenant users who do not have access to private Primary Tenant networks can no longer see network information by manually adding network ID (zoneId) filters to URLs

• The Tenant name and database ID are no longer shown in the return payload when sending a POST request to initiate a new user session 5.2.11

• Users can no longer view Instance Types owned by other Tenants by adding arbitrary Instance Type ID values to request URLs 5.2.12

• Users with “Infrastructure: Network Integrations” permissions set to “None” no longer see the Integrations tab in Infrastructure > Networks 5.2.12

Service Catalog

• Fixed an issue that could cause Inputs to appear in a different order than they are set on the Catalog Item configuration

• Fixed an issue which could cause errors to be thrown when certain special characters were passed in an Input when provisioning a Service Catalog item

ServiceNow

• Cleaned up some CMDB sync-related errors that were appearing in logs after ServiceNow sync

• Fixed an issue causing some ServiceNow traffic not to go through a configured global proxy 5.2.12

• Fixed an issue where the workflow indicated on a ServiceNow approval policy would not be honored during App provisioning 5.2.11

• When exposing a Cloud to a new ServiceNow integration for provisioning which already has a CMDB server association, this association is no longer overwritten to set the new ServiceNow appliance as the Cloud’s associated CMDB 5.2.11

Storage

• After reconfiguring an Instance to alter storage details, this information is now refreshed live on the Storage tab without requiring a page refresh 5.2.12

Tags

• Fixed an issue which caused tags not to be set when provisioning to Azure Stack Clouds 5.2.12

Tasks
• Additional validation added when editing a Task to ensure the Task name is still unique prior to attempting to save changes. This change prevents 500 errors if the Task name has been editing to no longer be unique. 5.2.11

• Fixed an issue causing Ansible Tasks to fail and Morpheus UI to crash if the Ansible integration is connecting to Git over SSH during Task execution. 5.2.11

• Fixed an issue that caused remote-target Tasks to always fail under specific conditions. 5.2.11

Tenants

• Fixed Tenant deletion issues caused by network pool associations not being automatically removed. 5.2.12

UI

• Advanced table view added to Zone Records List Page (Infrastructure > Networks > Integrations > selected integration > Zone Records tab). 5.2.12

• After completing the process of resetting a forgotten password, Subtenant users are redirected to the Subtenant login page rather than the login page for the Primary Tenant. 5.2.12

• Expand arrows now work correctly on the History page (Operations > Activity > History) and the look of the page has been updated to match other history and executions list pages.

• Fixed an issue where 500 errors could be thrown when editing global cloud-init settings (Administration > Settings > Provisioning) as a Subtenant administrator under certain conditions.

• The “Location” column in the VMs table on the Instance Detail Page has been renamed “Address(es)” to avoid potential confusion with other Location properties. 5.2.12

• When added or editing a Task, the SUDO checkbox is now consistently located under the CONTENT field. Previously, the placement of the checkbox was inconsistent.

• When restarting a virtual machine from the Instance detail page (Provisioning > Instances), the confirmation message now refers to a “node” rather than a “container” to prevent confusion. 5.2.12

VMware

• Fixed a sporadic issue where automatic downscale features could leave VMs in vCenter despite being removed from Morpheus. 5.2.11

• Fixed an issue that caused Instance snapshots not to be deleted properly. 5.2.11

• Fixed an issue that caused VMware clouds with only discovered VMs and Snapshots to not delete properly. 5.2.11

• Fixed an issue that could cause folder and resource pool selections not to be honored and the VM provisioned into the datacenter root in very specific scenarios. 5.2.11

• Fixed an issue that prevented VMware Clouds from being deleted in specific cases. 5.2.12

• Fixed an issue where Instances provisioned with multiple NICs could show incorrect MAC addresses and network assignment would fail.

• Fixed an issue where reconfiguring Instances with many disks could cause the individual disks to report incorrect sizes requiring the user to input them manually prior to executing the reconfigure. 5.2.11

• Fixed failed backups and snapshots remaining in “in progress” state. 5.2.12

• VMware Guest Customizations no longer override the keyboard layout to en-us which caused confusion for users who may have set the layout differently on their images.

13.3. Fixes
• When discovering VMs on VMware, for example, we are now setting the OS Information to a specific value such as CentOS 64-bit, CentOS 8 64-bit, or Windows Server 2016, as appropriate 5.2.12

• When provisioning an MKS cluster into VMware, guest customization is always used when IP pools are being used rather than DHCP to avoid issues 5.2.12

**Veeam**

• Disabled Veeam backup integrations will no longer appear as backup targets in Instance and App provisioning wizards 5.2.11

**Virtual Images**

• Fixed an issue where Virtual Image conversion processes would consistently fail under certain conditions 5.2.11

• Uploading OVA image files to NSFv3 file share buckets will no longer stop after the first file under certain conditions, such as when they contain multiple TAR files 5.2.12

**Whitelabel**

• Fixed an issue that caused the filename of the primary Tenant logo image to appear in the Subtenant settings are even if the Subtenant had successfully applied their own logo image (which displays correctly) 5.2.11

**Wiki**

• Wiki notes are no longer lost when an Instance is assigned to a different Tenant 5.2.12

**Workflows**

• Attempting to delete a Workflow which is associated with a Layout, now surfaces a helpful UI warning that the action can’t be completed rather than throwing a 500 error 5.2.12

• Fixed an issue that could cause errors to be thrown when running a Workflow containing WinRM Tasks with an execute context of “None” 5.2.12

• Fixed an issue which prevented some Inputs from being reordered if additional Inputs were added later after the Workflow was initially saved 5.2.12

• The failure of a post-provisioning workflow task is now reflected in the instance state (warning) and workflow and task states (error) 5.2.12

**XenServer**

• Fixed an issue where networks were not changed correctly when reconfiguring Xen Instances to change networks 5.2.11

**vCloud Director**

• Corrected an issue that could cause vCD plan resizing to fail when updating the number of max cores and cores per socket 5.2.11

• Fixed agent not installing when ICMP is blocked 5.2.12

• Fixed an issue that could cause Kubernetes clusters not to honor their associated custom plans in some cases when provisioned to vCD 5.2.12

• Fixed an issue where editing Instances in vCD clouds would cause 500 errors (though the changes would be successfully saved) 5.2.11

• Fixed issue with header parsing when connecting to vCD through load balancer 5.2.12

• The Resources tab of a VCD cloud detail page now is properly displaying vApp names in the Pools section 5.2.12
• When reconfiguring vCD Instances with multiple disks, disks no longer change size without user input in certain scenarios 5.2.11

13.4 Appliance & Agent Updates

Appliance

• Fixed upgrade issue with SLES 12/15 where morpheus-ctl command was removed during rpm post removal. Note this does not fix previous rpm post removal scripts and rpm -U ... --force will still need to be ran when upgrading to 5.2.12 on SLES 12/15. 5.2.12

• Java upgraded to 8u312-b07 5.2.12
• MySQL upgraded to 5.7.35 5.2.12
• Nginx upgraded to 1.20.1 5.2.12
• Optimizations added to improve page load times 5.2.11
• RabbitMQ upgraded to 3.9.8 5.2.12
• Tomcat upgraded to 9.0.54 5.2.12
• morpheus-playbooks configuration updated to use Cloudfront instead of s3 bucket url 5.2.12
V5.3.4 COMPATIBILITY & BREAKING CHANGES

When installing and upgrading to Morpheus v5.3.4, refer to the following to ensure compatibility.

14.1 Breaking Changes

- 4.2.1+: Appliance: OS: Ubuntu 14.04 has reached its end of life (EOL) and is no longer supported as a Morpheus Appliance Host Operating System. Any Morpheus Appliance running on 14.04 must be upgraded to 16.04, 18.04 or 20.04 BEFORE upgrading to 4.2.1+. Upgrades on 14.04 will not succeed
- 4.2.1+: Clouds: VirtualBox, VirtuSteam, and MetaCloud Cloud Types are no longer supported or available
- 4.2.1+: Puppet: Morpheus integration now supports version 6+. Puppet versions prior to 6 are no longer supported
- 4.2.1+: Tasks: Python: Virtual environment are now used for Python Tasks. Note: virtualenv is required on all Appliance App nodes
- 4.2.4: For appliances with externalized MySQL databases, due to MySQL deprecation of the “EDT” timezone you may need to update your database timezone to UTC or another compatible value. If this is not done, you will receive errors referencing timezone and Morpheus will not start. Morpheus should handle this change automatically for all-in-one appliances.
- 5.0.0+: When upgrading to 5.0.0+ from 4.x.x, any bearer tokens that have been generated are deleted which requires users to request new bearer tokens
- 5.2.1 & 4.2.5: API: Metadata: Metadata tags now referred to as tags and labels now referred to as labels. Previously metadata tags were referred to as metadata and labels were referred to as tags
- 5.2.3+: codeready (codeready-builder-for-rhel-8-x86_64-rpms) repo access required for RHEL 8+ Appliances, replacing the previous PowerTools/powertools requirement
- 5.2.6, 5.3.1: Appliance & Agent java version updated to 8u292-b10. jdk8u292 disables TLS 1.0 and 1.1 by default
- 5.2.9: OpenStack v2 Identity API is deprecated as of v5.2.9 (and is removed as of v5.3.3)
- 5.3.2+: Provisioning → Deployments has been moved to Provisioning → Code → Deployments
- 5.3.2+: The local code repository path moved from /var/opt/morpheus/morpheus-ui/repo to /var/opt/morpheus/morpheus-local/repo to reduce potential shared storage issues and performance restrictions. The reconfigure process creates the folders and sets the paths in application.yml, no manual intervention is needed unless symlinks exist on /var/opt/morpheus/morpheus-ui/repo/git which will need to be removed prior to reconfiguring 5.3.2. The old /var/opt/morpheus/morpheus-ui/repo path will be automatically deleted in a future release but can be manually recursively deleted at any time for storage reclamation.
• 5.3.3: Support for OpenStack v2 Identity API is removed
• 5.3.4: Major UI navigation structure changes. Refer to the Navigation Updates reference table

14.2 Morpheus Application OS

Morpheus can be installed on the following platforms. Please note the table below is for Morpheus Application OS support, not Morpheus Agent OS Support.

**Important:** Existing Morpheus Appliances on 14.04 must upgrade to 16.04, 18.04 or 20.04 PRIOR to upgrading to v4.2+.

**Note:** If CentOS 8.2 is pinned to 8.2.2004 vault, the PowerTools repository will need to be pinned to 8.2.2004 to access freerdp-libs 2.0.0

<table>
<thead>
<tr>
<th>OS</th>
<th>Version(s)</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Linux</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>CentOS</td>
<td>7.x, 8.x</td>
<td>If CentOS 8.2 is pinned to 8.2.2004 vault, the PowerTools repository will need to be pinned to 8.2.2004 to access freerdp-libs 2.0.0</td>
</tr>
<tr>
<td>Debian</td>
<td>9, 10, 11</td>
<td>FreeRDP 2.0 is not compatible with Debian 9. guacd will remain at 1.0.0 for Appliances running on Debian 9.</td>
</tr>
<tr>
<td>RHEL</td>
<td>7.x, 8.x</td>
<td></td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server (SLES)</td>
<td>12, 15</td>
<td></td>
</tr>
<tr>
<td>Ubuntu</td>
<td>16.04, 18.04, 20.04</td>
<td>14.04 is no longer supported for Appliance OS. Existing Appliances on 14.04 must upgrade to 16.04, 18.04 or 20.04 PRIOR to upgrading to v4.2.1+. Note: 14.04 is still supported by the Morpheus Agent.</td>
</tr>
</tbody>
</table>

14.3 Services

14.3.1 v5.3.4 Service Version Changes

• Java upgraded to 8u312-b07 5.2.12
• MySQL upgraded to 5.7.35 5.2.12
• Nginx upgraded to 1.20.1 5.2.12
• RabbitMQ upgraded to 3.9.8 5.2.12
• Tomcat upgraded to 9.0.54 5.2.12
14.3.2 v5.3.4 Service Version Compatibility

When externalizing MySQL, Elasticsearch and/or RabbitMQ services, the following versions are compatible with version Morpheus v5.3.4.

<table>
<thead>
<tr>
<th>Service</th>
<th>Compatible Branch</th>
<th>Morpheus Installer Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>MySQL</td>
<td>v5.7</td>
<td>v5.7.35</td>
</tr>
<tr>
<td>MySQL (FIPS)</td>
<td>v5.7</td>
<td>v5.7.35</td>
</tr>
<tr>
<td>Percona</td>
<td>5.7, WSREP 31</td>
<td>n/a</td>
</tr>
<tr>
<td>Elasticsearch</td>
<td>v7.x</td>
<td>v7.8.1</td>
</tr>
<tr>
<td>RabbitMQ</td>
<td>v3.5-3.9</td>
<td>v3.9.8</td>
</tr>
<tr>
<td>Tomcat</td>
<td>v9.0.54</td>
<td></td>
</tr>
<tr>
<td>Nginx</td>
<td></td>
<td>v1.20.1</td>
</tr>
<tr>
<td>OpenSSL</td>
<td></td>
<td>1.1.1k, 1.0.2u (FIPS)</td>
</tr>
<tr>
<td>Java</td>
<td></td>
<td>v8u312-b07</td>
</tr>
<tr>
<td>Java (macOS agent)</td>
<td></td>
<td>v8u302-b08</td>
</tr>
</tbody>
</table>

14.4 Security

14.4.1 CVEs Addressed

- CVE-2021-23369

14.5 Upgrade Paths & Methods

The following table shows supported version upgrade paths and methods.

- Some Features and Fixes in the From version may not be included in the To version due to From version being released after the To version.
## 14.6 Integrations

**Note:** Current iterations of Amazon AWS, Microsoft Azure, Google Cloud Platform, Digital Ocean, HPE OneView, OpenTelekom Cloud, IBM Bluemix, Softlayer and UpCloud are all supported.

<table>
<thead>
<tr>
<th>Integration</th>
<th>Supported Version(s)</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ansible</td>
<td>2.7.x</td>
<td></td>
</tr>
<tr>
<td>Ansible Tower</td>
<td>3.8.x</td>
<td></td>
</tr>
<tr>
<td>App Dynamics</td>
<td>4.5.x</td>
<td></td>
</tr>
<tr>
<td>Azure Stack</td>
<td>2002 back to 1908</td>
<td>2019-03-01-hybrid api-profile version used which is supported in 1908 and later Azure Stack versions</td>
</tr>
<tr>
<td>Cisco ACI</td>
<td>3.10</td>
<td></td>
</tr>
<tr>
<td>Citrix Netscaler</td>
<td>v12.1</td>
<td></td>
</tr>
<tr>
<td>Commvault</td>
<td>v11 sp 19</td>
<td></td>
</tr>
<tr>
<td>F5 Big-IP</td>
<td>11.4+</td>
<td></td>
</tr>
<tr>
<td>Infoblox</td>
<td>Latest Versions Supported</td>
<td></td>
</tr>
<tr>
<td>Jenkins</td>
<td>2.x</td>
<td></td>
</tr>
<tr>
<td>Kubernetes</td>
<td>1.x</td>
<td></td>
</tr>
<tr>
<td>Microsoft Hyper-V</td>
<td>2012R2, 2016, 2019</td>
<td></td>
</tr>
<tr>
<td>Nutanix AHV</td>
<td>5.0 - 5.10 Note: Prism Central is not a supported endpoint</td>
<td>In 5.5 - 5.7 if Prism Central is managing Prism Element, image creation will not function due to PC Image Management.</td>
</tr>
<tr>
<td>Openstack</td>
<td>Latest Versions Supported</td>
<td>When creating an OpenStack integration, select the latest available from the OS Version dropdown menu when running a later version</td>
</tr>
<tr>
<td>Rubrik</td>
<td>4.2</td>
<td></td>
</tr>
<tr>
<td>SCVMM</td>
<td>2016, 2019</td>
<td></td>
</tr>
<tr>
<td>ServiceNow</td>
<td>Orlando, Paris, Quebec, Rome</td>
<td></td>
</tr>
<tr>
<td>Terraform</td>
<td>v0.11.x, v0.12.18+, 0.13.x, 0.14.x</td>
<td></td>
</tr>
<tr>
<td>vCloud Director</td>
<td>8.20, 9.1, 9.5, 9.7, 10.0, 10.2 vCD 9.7+ supported on API v31, vCD 10.2+ supported on API v34.0</td>
<td></td>
</tr>
<tr>
<td>Veeam</td>
<td>9.5u3, 9.5u4, 10, 11</td>
<td></td>
</tr>
<tr>
<td>VMware ESXi</td>
<td>5.5, 6.0, 6.5, 6.7, 7</td>
<td></td>
</tr>
<tr>
<td>VMware Fusion</td>
<td>8, 9, 10+</td>
<td></td>
</tr>
<tr>
<td>VMware NSX</td>
<td>-V, -T v3.1.1</td>
<td></td>
</tr>
<tr>
<td>VMware vCenter</td>
<td>5.5, 6.0, 6.5, 6.7, 7</td>
<td></td>
</tr>
<tr>
<td>XenServer</td>
<td>7.x</td>
<td></td>
</tr>
</tbody>
</table>
Note: Non-listed versions may be compatible but are not verified.