# Contents

## 1 Getting Started
- 1.1 Requirements .................................................. 1
- 1.2 Installation .................................................... 6
- 1.3 Initial Appliance Setup ........................................ 11
- 1.4 Upgrading ...................................................... 13
- 1.5 Advanced Configuration ....................................... 14
- 1.6 High Availability Configuration .............................. 18
- 1.7 Morpheus CLI .................................................. 33
- 1.8 Morpheus Agent ............................................... 41
- 1.9 Morpheus Discovery ........................................... 43
- 1.10 morpheus-ctl tips ............................................ 44

## 2 Provisioning
- 2.1 Requirements .................................................. 47
- 2.2 Provisioning Concepts ......................................... 53
- 2.3 Instances ....................................................... 54
- 2.4 Remote Console ............................................... 57
- 2.5 Apps ............................................................. 62
- 2.6 Blueprints ....................................................... 68
- 2.7 Automation ..................................................... 73
- 2.8 Virtual Images ................................................ 86
- 2.9 Library .......................................................... 91
- 2.10 Migrations ..................................................... 101
- 2.11 Deployments .................................................. 105

## 3 Infrastructure
- 3.1 Groups .......................................................... 109
- 3.2 Clouds ............................................................ 112
- 3.3 Hosts .............................................................. 115
- 3.4 Network .......................................................... 121
- 3.5 Load Balancers ................................................ 130
- 3.6 F5 Load Balancers ............................................. 134
- 3.7 Storage ............................................................ 137
- 3.8 Key Pairs & Certificates ...................................... 157
- 3.9 PXE Boot ........................................................ 157

## 4 Administration .................................................. 163
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1 Tenants</td>
<td>163</td>
</tr>
<tr>
<td>4.2 Identity Sources</td>
<td>180</td>
</tr>
<tr>
<td>4.3 Plans &amp; Pricing</td>
<td>182</td>
</tr>
<tr>
<td>4.4 Roles</td>
<td>186</td>
</tr>
<tr>
<td>4.5 Users &amp; User Groups</td>
<td>191</td>
</tr>
<tr>
<td>4.6 Integrations</td>
<td>195</td>
</tr>
<tr>
<td>4.7 Policies</td>
<td>195</td>
</tr>
<tr>
<td>4.8 Provisioning Settings</td>
<td>201</td>
</tr>
<tr>
<td>4.9 Monitoring Settings</td>
<td>203</td>
</tr>
<tr>
<td>4.10 Backup Settings</td>
<td>205</td>
</tr>
<tr>
<td>4.11 Logging Settings</td>
<td>206</td>
</tr>
<tr>
<td>4.12 Appliance Settings</td>
<td>207</td>
</tr>
<tr>
<td>5 Monitoring</td>
<td>215</td>
</tr>
<tr>
<td>5.1 Overview</td>
<td>215</td>
</tr>
<tr>
<td>6 Logs</td>
<td>221</td>
</tr>
<tr>
<td>6.1 Overview</td>
<td>221</td>
</tr>
<tr>
<td>6.2 Integrations</td>
<td>222</td>
</tr>
<tr>
<td>6.3 Exporting Logs</td>
<td>222</td>
</tr>
<tr>
<td>6.4 Agent Logs</td>
<td>223</td>
</tr>
<tr>
<td>6.5 Morpheus Server Logs</td>
<td>223</td>
</tr>
<tr>
<td>6.6 Activity Log</td>
<td>224</td>
</tr>
<tr>
<td>6.7 morpheus-ssl nginx logs</td>
<td>224</td>
</tr>
<tr>
<td>7 Backups</td>
<td>227</td>
</tr>
<tr>
<td>7.1 Initial Backups Setup</td>
<td>227</td>
</tr>
<tr>
<td>7.2 Configuring Backups during Provisioning</td>
<td>228</td>
</tr>
<tr>
<td>7.3 Summary</td>
<td>229</td>
</tr>
<tr>
<td>7.4 Backups</td>
<td>229</td>
</tr>
<tr>
<td>7.5 Managing Backups</td>
<td>231</td>
</tr>
<tr>
<td>8 Operations</td>
<td>235</td>
</tr>
<tr>
<td>8.1 Dashboard</td>
<td>235</td>
</tr>
<tr>
<td>8.2 Reports</td>
<td>235</td>
</tr>
<tr>
<td>8.3 Analytics</td>
<td>237</td>
</tr>
<tr>
<td>8.4 Guidance</td>
<td>240</td>
</tr>
<tr>
<td>8.5 Scheduling</td>
<td>241</td>
</tr>
<tr>
<td>8.6 Approvals</td>
<td>244</td>
</tr>
<tr>
<td>8.7 Usage</td>
<td>247</td>
</tr>
<tr>
<td>8.8 Activity</td>
<td>248</td>
</tr>
<tr>
<td>8.9 Health</td>
<td>249</td>
</tr>
<tr>
<td>9 Services</td>
<td>253</td>
</tr>
<tr>
<td>9.1 Cypher</td>
<td>253</td>
</tr>
<tr>
<td>9.2 Archives</td>
<td>255</td>
</tr>
<tr>
<td>10 Integration Guides</td>
<td>259</td>
</tr>
<tr>
<td>10.1 Automation</td>
<td>259</td>
</tr>
<tr>
<td>10.2 Backups</td>
<td>280</td>
</tr>
<tr>
<td>10.3 Clouds</td>
<td>283</td>
</tr>
<tr>
<td>10.4 Containers</td>
<td>373</td>
</tr>
<tr>
<td>10.5 Deployment</td>
<td>380</td>
</tr>
<tr>
<td>10.6 DNS</td>
<td>380</td>
</tr>
<tr>
<td>10.7 Identity Management</td>
<td>384</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>10.8 ITSM</td>
<td>394</td>
</tr>
<tr>
<td>10.9 Keys and Certificates</td>
<td>400</td>
</tr>
<tr>
<td>10.10 Load Balancers</td>
<td>401</td>
</tr>
<tr>
<td>10.11 Logs</td>
<td>404</td>
</tr>
<tr>
<td>10.12 Monitoring</td>
<td>405</td>
</tr>
<tr>
<td>10.13 Networking</td>
<td>406</td>
</tr>
<tr>
<td>10.14 Service Discovery</td>
<td>416</td>
</tr>
<tr>
<td>10.15 Storage</td>
<td>417</td>
</tr>
<tr>
<td>10.16 Supported Integration Versions</td>
<td>424</td>
</tr>
<tr>
<td>11 Troubleshooting</td>
<td>425</td>
</tr>
<tr>
<td>11.1 Common Ports &amp; Requirements</td>
<td>425</td>
</tr>
<tr>
<td>11.2 Morpheus Agent Install Troubleshooting</td>
<td>427</td>
</tr>
<tr>
<td>11.3 Remote Console</td>
<td>431</td>
</tr>
<tr>
<td>11.4 Deleting Instances</td>
<td>436</td>
</tr>
<tr>
<td>11.5 Cannot Login</td>
<td>438</td>
</tr>
<tr>
<td>11.6 Morpheus UI not loading after upgrade or reconfigure</td>
<td>439</td>
</tr>
<tr>
<td>11.7 Unable to Provision a Custom Image</td>
<td>440</td>
</tr>
<tr>
<td>11.8 Restart a Morpheus Installation</td>
<td>441</td>
</tr>
<tr>
<td>11.9 Variables</td>
<td>441</td>
</tr>
<tr>
<td>11.10 Blank Dashboard</td>
<td>447</td>
</tr>
<tr>
<td>11.11 Unable to Delete Tenant</td>
<td>448</td>
</tr>
<tr>
<td>11.12 CLI Troubleshooting</td>
<td>448</td>
</tr>
<tr>
<td>11.13 Troubleshooting Ansible</td>
<td>449</td>
</tr>
<tr>
<td>11.14 How to un-manage an Instance/VM/Host</td>
<td>450</td>
</tr>
<tr>
<td>12 Release Notes</td>
<td>453</td>
</tr>
<tr>
<td>12.1 v3.6.1</td>
<td>453</td>
</tr>
<tr>
<td>12.2 v3.6.0</td>
<td>455</td>
</tr>
<tr>
<td>12.3 v3.5.3</td>
<td>464</td>
</tr>
<tr>
<td>12.4 v3.4.4</td>
<td>468</td>
</tr>
<tr>
<td>12.5 v3.5.2</td>
<td>470</td>
</tr>
<tr>
<td>12.6 v3.4.3</td>
<td>472</td>
</tr>
<tr>
<td>12.7 v3.5.1</td>
<td>473</td>
</tr>
<tr>
<td>12.8 v3.4.2</td>
<td>475</td>
</tr>
<tr>
<td>12.9 v3.5.0</td>
<td>477</td>
</tr>
<tr>
<td>12.10 v3.4.1</td>
<td>480</td>
</tr>
<tr>
<td>12.11 v3.4.0</td>
<td>482</td>
</tr>
<tr>
<td>12.12 v3.3.2</td>
<td>484</td>
</tr>
<tr>
<td>12.13 v3.3.1</td>
<td>489</td>
</tr>
<tr>
<td>12.14 v3.3.0</td>
<td>493</td>
</tr>
<tr>
<td>12.15 v3.2.2</td>
<td>497</td>
</tr>
<tr>
<td>12.16 v3.2.1</td>
<td>500</td>
</tr>
<tr>
<td>12.17 v3.2.0</td>
<td>503</td>
</tr>
<tr>
<td>12.18 v3.1.5</td>
<td>507</td>
</tr>
<tr>
<td>12.19 v3.1.4</td>
<td>507</td>
</tr>
<tr>
<td>12.20 v3.1.3</td>
<td>508</td>
</tr>
<tr>
<td>12.21 v3.1.2 &amp; v2.12.5</td>
<td>509</td>
</tr>
<tr>
<td>12.22 v3.1.1</td>
<td>511</td>
</tr>
<tr>
<td>12.23 v3.1.0</td>
<td>511</td>
</tr>
<tr>
<td>12.24 v3.0.1</td>
<td>512</td>
</tr>
<tr>
<td>12.25 v2.12.4</td>
<td>513</td>
</tr>
<tr>
<td>12.26 v2.12.3</td>
<td>514</td>
</tr>
<tr>
<td>12.27 v2.12.2</td>
<td>515</td>
</tr>
</tbody>
</table>
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 vm’s and containers. To get started some base requirements are recommended:

1.1.1 Base Requirements

- **Operating System:** Ubuntu 14.04 /16.04 or CentOS/RHEL greater than 7.0.
- **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)
- **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.**
- **Access to base yum and apt repos**
- **An Appliance License is required for any operations involving provisioning.**
- **Internet Connectivity (optional)**
  - To download from Morpheus’ public docker repositories and system Virtual Image catalog
  - Offline installation require installing the offline package in addition to the regular installation package.

**Note:** Access to base yum and apt repos is still required for offline installations.
• VM and Host Agent Install (optional)
  – Inbound connectivity access from provisioned vm’s and container hosts on ports 443 (Agent install and communication) and 80 (Linux Agent installs via yum and apt)
  – 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 Admin->Settings.

Note: Ubuntu 16.10 and Amazon Linux are not 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 and stats and user uploaded and imported data require adequate space on the Morpheus Appliance(s) per Appliance Configuration and activity.

Important: It is the customers responsibility to ensure adequate storage space per configuration and use case.

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 none NFS Storage providers, 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 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 a Morpheus configuration with locally installed ElasticSearch, 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 or Instances reporting logs, log frequency, and log retention count.

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 vm’s 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 Admin->Settings). When the agent is started it automatically makes this connection and securely authenticates. Therefore, it is necessary for all vm’s and docker based hosts that are managed by morpheus to be able to reach the appliance server ip on port 443.

Morpheus also utilizes SSH (Port 22) and Windows Remote Management (Port 5985) to initialize a server. This includes sending remote command instructions to install the agent. It is actually possible for Morpheus to operate without agent connectivity (though stats and logs will not function) and utilize SSH/WinRM to perform operations. Once the agent is installed and connections are established SSH/WinRM communication will stop. This is why an outbound requirement exists for the appliance server to be able to utilize port 22 and 5985.

Note: In newer versions of morpheus this outbound connectivity is not mandatory. The agent can be installed by hand or via Guest Process API’s on cloud integrations like VMware.

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)
- Redis (Cache 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</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></td>
<td>SSH</td>
<td>Linux</td>
<td>Appliance</td>
<td>Node</td>
<td>22</td>
<td>DNS Resolution from node to appliance url Virtual Images configured 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 Virtual Images configured WinRM Enabled on Virtual Image (winrm quickconfig)</td>
</tr>
<tr>
<td>Cloud-init</td>
<td>Linux</td>
<td>Linux</td>
<td></td>
<td></td>
<td></td>
<td>Cloud-init installed on template/image Cloud-init settings populated in User Settings or in Admin -&gt; Provisioning Agent install mode set to Cloud-Init in Cloud Settings</td>
</tr>
<tr>
<td>Cloudbase-init</td>
<td>Windows</td>
<td>Windows</td>
<td></td>
<td></td>
<td></td>
<td>Cloudbase-init installed on template/image Cloud-init settings populated in User Settings or in Admin -&gt; Provisioning Agent install mode set to Cloud-Init in Cloud Settings</td>
</tr>
<tr>
<td>VMtools</td>
<td>All</td>
<td>All</td>
<td></td>
<td></td>
<td></td>
<td>VMtools installed on template Cloud-init settings populated in Morpheus user settings or in Administration -&gt; Provisioning when using Static IP’s Existing User credentials entered on Virtual Image when using DHCP 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) Cloud-init/Cloudbase-init installed on template/image Cloud-init settings populated in Morpheus user settings or in Administration -&gt; Provisioning</td>
</tr>
<tr>
<td>VMware Tools</td>
<td>All</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>
</tbody>
</table>
1.2 Installation

Morpheus comes packaged as a debian or yum based package. It can be installed on a single on/off premise linux based host or configured for high availability and horizontal scaling. Morpheus is currently only supported on Ubuntu 14.04, Ubuntu 16.04, CentOS 7.0 or newer, and RHEL 7.0 or newer based hosts.

Note: You can view our offline installation guide at offline-installer.

1.2.1 Ubuntu

To get started installing Morpheus on Ubuntu (14.04 currently) 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 might also be advisable to verify that 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.

2. Next simply download the relevant .deb package for installation. This package can be acquired from your account rep or via a free trial request from .

   Tip: Use the `wget` command to directly download the package to your appliance server. i.e. `wget https://downloads.gomorpheus.com/path/to/package.deb` THIS IS NOT THE PACKAGE URL. The package URL can be acquired from your account rep or via a free trial request from

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

   ```bash
   sudo dpkg -i morpheus-appliance_x.x.x-1.amd64.deb
   sudo morpheus-ctl reconfigure
   ```

4. 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 post install settings that can be viewed in the Advanced section of the guide.

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.
1.2.2 CentOS

To get started installing Morpheus on CentOS a few preparatory items should be addressed first.

1. Configure firewalld to allow access from users on port 80 or 443 (Or remove firewall if not required).

2. Make sure the machine is self resolvable to its own hostname.

   **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.

3. Next simply download the relevant .rpm package for installation. This package can be acquired from your account rep or via a free trial request from.

   **Tip:** Use the `wget` command to directly download the package to your appliance server. i.e. `wget https://downloads.gomorpheus.com/path/to/package.rpm` **THIS IS NOT THE PACKAGE URL.** The package URL can be acquired from your account rep or via a free trial request from

4. 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
   sudo morpheus-ctl reconfigure
   ```

5. 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 post install settings that can be viewed in the Advanced section of the guide.

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 RHEL

To get started installing Morpheus on RHEL 7 a few prerequisite items are required.

1. Configure firewalld to allow access from users on port 80 or 443 (Or remove firewall if not required).
2. Make sure the machine is self resolvable to its own hostname.
3. For RHEL, In order for the guacamole service (remote console) to properly install some additional optional repositories first need added.
   - RHEL 7.x Amazon: `yum-config-manager --enable rhui-REGION-rhel-server-optional`
   - 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.

**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.

The RedHat Enterprise Linux 7 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.

```
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.

```
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 your account rep or via a free trial request from .

**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:

```
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:

```
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 post install settings that can be viewed in the Advanced section of the guide.

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.

1.2.4 Additional Options

There are several additional configuration options during installation that may be performed. For example, Morpheus provides convenient options for uploading your own SSL certificates as well as externalizing several dependent services.

System Defaults

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
  - 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
  - Redis: /var/log/morpheus/redis
- **User-defined install/config:** /etc/morpheus/morpheus.rb

SSL Certificates

The default installation generates a self-signed SSL certificate. To implement a third-party certificate:

1. Copy the private key and certificate to /etc/morpheus/ssl/your_fqdn_name.key and /etc/morpheus/ssl/your_fqdn_name.crt respectively.
2. 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.

3. Next simply reconfigure the appliance and restart nginx:
   ```bash
   sudo morpheus-ctl reconfigure
   sudo morpheus-ctl restart nginx
   ```
Additional Configuration Options

There are several other options available to the /etc/morpheus/morpheus.rb file that can be useful when setting up external service integrations or high availability:

```ruby
mysql['enable'] = false
mysql['host'] = '52.53.240.28'
mysql['port'] = 10004
mysql['morpheus_db'] = 'morpheusdb01'
mysql['morpheus_db_user'] = 'merovingian'
mysql['morpheus_password'] = 'Wm5n5gXqXCe9v52'
rabbitmq['enable'] = false
rabbitmq['vhost'] = 'zion'
rabbitmq['queue_user'] = 'dujour'
rabbitmq['queue_user_password'] = '5tfg9n2iBifzW5c'
rabbitmq['host'] = '54.183.196.152'
rabbitmq['port'] = '10008'
rabbitmq['stomp_port'] = '10010'
redis['enable'] = false
redis['host'] = '52.53.240.28'
redis['port'] = 10009
elasticsearch['enable'] = false
elasticsearch['cluster'] = 'nebuchadnezzar'
elasticsearch['es_hosts'] = {'52.53.214.68' => 10003}
```

These settings allow one to externally configure and scale mysql, elasticsearch, redis, and rabbitmq which is critical for a high availability setup.

1.3 Initial Appliance Setup

1.3.1 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 longs 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 different url per cloud integration.
1. 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 Admin -> Settings page, where you will add your License Key.

1.3.2 Login Methods

Master Tenant

- Enter username or email 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.

1.3.3 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 - Provisioning. It is recommended to define these settings after installation unless credentials are defined per Virtual Image for Provisioning.
1.3.4 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.

1.4 Upgrading

Morpheus provides a very simple and convenient upgrade process. In most cases it is simply a matter of installing the new package on top of itself and reconfiguring the services.

**Important:** All services except the morpheus-ui must be running during a reconfigure. The morpheus-ui also must be restarted or stopped and started during an upgrade. Failure to do so will result in errors.

1.4.1 Debian / Ubuntu

Simply download the latest package or request the latest package from your account service representative.
Then run the install process as follows:

```
sudo dpkg -i morpheus-appliance_x.x.x-1.amd64.deb
sudo morpheus-ctl stop morpheus-ui
sudo morpheus-ctl reconfigure
sudo morpheus-ctl start morpheus-ui
```

This typically is enough to complete a full upgrade. Databases will automatically be migrated upon restart of the application and service version upgrades will automatically be applied.

### 1.4.2 CentOS / RHEL

Yum based package upgrades are a little different. In this case we want to run a `rpm -U` command as the package manager is slightly different.

```
sudo rpm -U morpheus-appliance-x.x.x-1.x86_64.rpm
sudo morpheus-ctl stop morpheus-ui
sudo morpheus-ctl reconfigure
sudo morpheus-ctl start morpheus-ui
```

**Tip:** Sometimes it may be necessary to restart all appliance services on the host. In order to do this simply type `sudo morpheus-ctl restart`. This will restart ALL services.

### 1.4.3 Deploy WAR file

**Download the war file**

```
wget <url>
```

**Move the file**

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

**Change permissions**

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

**Restart UI**

```
morpheus-ctl restart morpheus-ui
```

### 1.5 Advanced Configuration

Morpheus provides more advanced configuration capabilities, including High Availability configurations, and support for tougher network environments with offline installation and Proxy configurations.
1.5.1 Offline Installer

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

Offline Installer 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 offline packages must be downloaded from another system and transferred to the Morpheus Appliance server.

**Note:** The offline package is linked 1-to-1 to the appliance release. For example the offline package for 2.12.2-1 should be used with the appliance package 2.12.2-1

Offline Install

**Ubuntu**

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

   ```
   wget http://example_url/morpheus-appliance_package_url.deb
   wget http://example_url/morpheus-appliance_package_offline_url.deb
   ```

2. Install the appliance package. DO NOT run morpheus-ctl reconfigure yet.

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

3. Install the offline package using dpkg -i morpheus-appliance-offline_2.12.2~rc1-1_all.deb.

   ```
   sudo dpkg -i morpheus-appliance-offline_version_all.deb
   ```

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

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

5. 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.
CentOS

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

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

2. Install the appliance package. DO NOT run morpheus-ctl reconfigure yet.

   ```
   sudo rpm -i morpheus-appliance_version_amd64.rpm
   ```

3. Install the offline package using rpm -i morpheus-appliance-offline_2.12.2~rc1-1_all.rpm

   ```
   sudo rpm -i morpheus-appliance-offline_version_all.rpm
   ```

4. Set the Morpheus UI applaicne 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
   ```

5. 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.

1.5.2 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 Admin -> 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 aa 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 hosts 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.

1.5.3 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:

1.5. Advanced Configuration
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 10.1.2.2 morpheus -p < /tmp/morpheus_backup.sql
Enter password:
```

The data form 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
```

### 1.6 High Availability Configuration

#### 1.6.1 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.

**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 5.6.10) 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. (8gb) 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 clustered based queuing system and needs at least 3 instances for HA configurations. This is due to elections in the failover scenariosrabbitmq 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. 4–8gb of Memory is recommended to start.

**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, Tomcat, and Redis (to be phased out at a later date). 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.
1.6.2 Database Tier

Morpheus needs a database to connect to. 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.

If you’re not as familiar with WSREP and prefer replication, some of our customers prefer to configure a failover connection to a MariaDB or MySQL based Master/Master Replication cluster. Less often used, though still a viable option, is MySQL based NDB Clustering. Wonderful guides for each of these HA and DR based database management strategies can be found here: https://www.percona.com/doc/percona-xtradb-cluster/LATEST/index.html

Requirements

Note: Morpheus idiomatically connects to database nodes over 3306

Once you have your database installed and configured:
1. Create the Database you will be using with morpheus.

```sql
mysql> CREATE DATABASE morpheusdb;
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.

```sql
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.

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

mysql> GRANT SELECT, PROCESS, SHOW DATABASES, SUPER ON *.* TO 'morpheusdbuser'@'$source_ip'
    -> IDENTIFIED BY PASSWORD 'secretpasshere';

mysql> FLUSH PRIVILEGES;
```

4. Checking Permissions for your user.

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

### 1.6.3 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](https://www.rabbitmq.com/ha.html) and [https://www.rabbitmq.com/clustering.html](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: [https://www.rabbitmq.com/install-rpm.html#downloads](https://www.rabbitmq.com/install-rpm.html#downloads)

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

```bash
rabbitmq-plugins enable rabbitmq_stomp

rabbitmqctl set_policy -p morpheus --apply-to queues --priority 1 statCommands
    -> "statCommands.*" '{expires:1800000}'

rabbitmqctl set_policy -p morpheus --apply-to queues --priority 1
    -> morpheusAgentActions "morpheusAgentActions.*" '{expires:1800000}'
```

### 1.6.4 Elasticsearch

Install 3 node Elasticsearch Cluster on Centos 7
Important: This is a sample configuration only. Customer configurations and requirements will vary.

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:
   ```
   sudo yum install java-1.8.0-openjdk.x86_64
   ```
   To verify your JRE is installed and can be used, run the command:
   ```
   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)
   ```

Installation

To install Elasticsearch please use the following instructions
Once installed, to make sure Elasticsearch starts and stops automatically, add its init script to the default runlevels with the command:
```
sudo systemctl enable elasticsearch.service
```}

Configuring Elastic

Now that Elasticsearch and its Java dependencies have been installed, it is time to configure Elasticsearch.
The Elasticsearch configuration files are in the /etc/elasticsearch directory. There are two files:
```
sudo vi /etc/elasticsearch/elasticsearch.yml
```

elasticsearch.yml Configures the Elasticsearch server settings. This is where all options, except those for logging, are stored, which is why we are mostly interested in this file.

logging.yml Provides configuration for logging. In the beginning, you don’t have to edit this file. You can leave all default logging options. You can find the resulting logs in /var/log/elasticsearch by default.

The first variables to customize on any Elasticsearch server are node.name and cluster.name in elasticsearch.yml. As their names suggest, node.name specifies the name of the server (node) and the cluster to which the latter is associated.
Important: Make sure to uncomment each of the following listed below in /etc/elasticsearch/elasticsearch.yml

Node 1

```yaml
cluster.name: morpheusha1
node.name: "morpheuses1"
network.host: enter the IP of the node ex: 10.30.22.130
http.port: 9200
discovery.zen.ping.unicast.hosts: ["10.30.20.91","10.30.20.149","10.30.20.165"]
```

Node 2

```yaml
cluster.name: morpheusha1
node.name: "morpheuses2"
network.host: enter the IP of the node ex: 10.30.22.130
http.port: 9200
discovery.zen.ping.unicast.hosts: ["10.30.20.91","10.30.20.149","10.30.20.165"]
```

Node 3

```yaml
cluster.name: morpheusha1
node.name: "morpheuses3"
network.host: enter the IP of the node ex: 10.30.22.130
http.port: 9200
discovery.zen.ping.unicast.hosts: ["10.30.20.91","10.30.20.149","10.30.20.165"]
```

For the above changes to take effect, you will have to restart Elasticsearch with the command:

```
sudo service elasticsearch restart
```

Next restart the network with the command:

```
sudo service network restart
```

Testing

To make sure Elasticsearch is running use the following commands


1.6.5 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:
3. After installing and prior to reconfiguring, edit the `morpheus.rb` file

```
sudo vi /etc/morpheus/morpheus.rb
```

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['stomp_port'] = '61613'
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}  
```

1. Reconfigure Morpheus

```
sudo morpheus-ctl reconfigure
```

1.6.6 Storage

When Morpheus is in a High Availability configuration the required Local Storage File Shares will need to be copied to a shared file system so that all nodes within the Morpheus cluster is able to connect to assets.

**Assets**

- White label images
- Uploaded virtual images
- Deploy uploads
- Ansible Plays
- Terraform
- Morpheus backups
Tip: Backups, deployments and virtual images can be overridden within the Morpheus-UI. You can find more information on storage here: Storage

To copy the \texttt{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 \texttt{/var/opt/morpheus/}
4. Backup morpheus-ui directory by running the command below. This will create a new directory in \texttt{/var/opt/morpheus/} called morpheus-ui-bkp and copy the contents of morpheus-ui into the new directory
   
   \begin{verbatim}
   cp -r morpheus-ui morpheus-ui-bkp
   \end{verbatim}

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

   \begin{verbatim}
   mv morpheus-ui /nfs/appliance-files/
   \end{verbatim}

6. Mount your shared storage volume to \texttt{/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

   \begin{verbatim}
   cp -r morpheus-ui morpheus-ui-bkp
   \end{verbatim}

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

1.6.7 3 Node with Externalized DB Configuration

Assumptions

This guide assumes the following:

- There is an externalized database running for Morpheus to access.
- The database service is a MySQL dialect (MySQL, MariaDB, Galera, etc.)
- A database has been created for Morpheus as well as a user and proper grants have been run for the user. Morpheus will create the schema.
- 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 \texttt{/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.
Steps

1. First begin by downloading the requisite Morpheus packages either to the nodes or to your workstation for transfer. These packages need to be made available on the nodes you wish to install Morpheus on.

```
[root@app-server-1 ~]# wget https://example/path/morpheus-appliance-ver-1.el7.x86_64.rpm
[root@app-server-1 ~]# wget https://example/path/morpheus-appliance-offline-ver-1.noarch.rpm
```

2. Once the packages are available on the nodes they can be installed. Make sure that no steps beyond the rpm install are run.

```
[root@app-server-1 ~] rpm -i morpheus-appliance-ver-1.el7.x86_64.rpm
[root@app-server-1 ~] rpm -i morpheus-appliance-offline-ver-1.noarch.rpm
```

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}
```

(continues on next page)
elasticsearch['node_name'] = 'morpheus1'
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'] = 'morpheus2'
elasticsearch['host'] = '0.0.0.0'
rabbitmq['host'] = '0.0.0.0'
rabbitmq['nodename'] = 'rabbit@node02'
mysql['enable'] = false
mysql['host'] = '10.100.10.112'
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'] = 'morpheus3'
elasticsearch['host'] = '0.0.0.0'
rabbitmq['host'] = '0.0.0.0'
rabbitmq['nodename'] = 'rabbit@node03'
mysql['enable'] = false
mysql['host'] = '10.100.10.113'
mysql['morpheus_db'] = 'morpheusdb'
mysql['morpheus_db_user'] = 'morpheus'
mysql['morpheus_password'] = 'password'

Note: If you are running MySQL in a Master/Master configuration we will need to slightly alter the mysql['host'] line in the morpheus.rb to account for both masters in a failover configuration. As an example: mysql['host'] = '10.100.10.111:3306,10.100.10.112'. Morpheus will append the ‘3306’ port to the end of the final IP in the string, which is why we leave it off but explicitly type it for the first IP in the string. The order of IPs matters in that it should be the same across all three Morpheus Application Servers. As mentioned, this will be a failover configuration for MySQL in that the application will only read/write from the second master if the first master becomes unavailable. This way we can avoid commit lock issues that might arise from a load balanced Master/Master.

4. Run the reconfigure on all nodes

[root@app-server-1 ~] 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.
5. Select one of the nodes to be your Source Of Truth (SOT) for RabbitMQ clustering. We need to copy the secrets for RabbitMQ, copy the erlang cookie and join the other nodes to the SOT node.

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

```
[root@app-server-1 ~] cat /etc/morpheus/morpheus-secrets.json

"rabbitmq": {
    "morpheus_password": "***REDACTED***",
    "queue_user_password": "***REDACTED***",
    "cookie": "***REDACTED***"
},
```

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

```
[root@app-server-1 ~]# cat /opt/morpheus/embedded/rabbitmq/.erlang.cookie
# 754363AD864649RD63D28
```

6. Once this is done run a reconfigure on the two nodes that are NOT the SOT nodes.

```
[root@app-server-2 ~] morpheus-ctl reconfigure
```

**Note:** This step will fail. This is ok, and expected. If the reconfigure hangs then use Ctrl+C to quit the reconfigure run and force a failure.

7. Subsequently we need to stop and start Rabbit on the NOT SOT nodes.

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

```
[root@app-server-2 ~]# morpheus-ctl stop rabbitmq
[root@app-server-2 ~]# morpheus-ctl start rabbitmq
[root@app-server-2 ~]# PATH=/opt/morpheus/sbin:/opt/morpheus/sbin:/opt/morpheus/←embedded/sbin:/opt/morpheus/embedded/bin:$PATH
[root@app-server-2 ~]# rabbitmqctl stop_app
Stopping node 'rabbit@app-server-2' ...
[root@app-server-2 ~]# rabbitmqctl join_cluster rabbit@app-server-1
Clustering node 'rabbit@app-server-2' with 'rabbit@app-server-1' ...
[root@app-server-2 ~]# rabbitmqctl start_app
Starting node 'rabbit@app-server-2' ...
```

8. Now make sure to reconfigure

```
[root@app-server-2 ~] morpheus-ctl reconfigure
```

9. Once the Rabbit services are up and clustered on all nodes they need to be set to HA/Mirrored Queues:

```
[root@app-server-2 ~]# rabbitmqctl set_policy -p morpheus --priority 1 --apply-to all ha ".*" '{"ha-mode": "all"}"
```
10. The last thing to do is restart the Morpheus UI on the two nodes that are NOT the SOT node.

```
[root@app-server-2 ~]# morpheus-ctl restart morpheus-ui
```

If this command times out then run:

```
[root@app-server-2 ~]# morpheus-ctl kill morpheus-ui
[root@app-server-2 ~]# morpheus-ctl start morpheus-ui
```

11. 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@app-server-2 ~]# morpheus-ctl tail morpheus-ui
```

12. Lastly, we need to ensure that Elasticsearch is configured in such a way as to support a quorum of 2. We need to do this step on EVERY NODE.

```
[root@app-server-2 ~]# echo "discovery.zen.minimum_master_nodes: 2" >> /opt/morpheus/embedded/elasticsearch/config/elasticsearch.yml
[root@app-server-2 ~]# morpheus-ctl restart elasticsearch
```

**Note:** For moving `/var/opt/morpheus/morpheus-ui` files into a shared volume make sure ALL Morpheus services on ALL three nodes are down before you begin.

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

13. Permissions are as important as is content, so make sure to preserve directory contents to the shared volume.

14. Subsequently you can start all Morpheus services on all three nodes and tail the Morpheus UI log file to inspect errors.

### 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@app-server-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@app-server-old ~]# cat /etc/morpheus/morpheus-secrets.json
```

```json
{
  "mysql": {
    "root_password": "***REDACTED***",
    "morpheus_password": "***REDACTED***",
    "ops_password": "***REDACTED***"
  },
  "rabbitmq": {
    "morpheus_password": "***REDACTED***",
    "queue_user_password": "***REDACTED***",
```

(continues on next page)
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 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.

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@app-server-1 ~]# morpheus-ctl stop morpheus-ui
[root@app-server-2 ~]# morpheus-ctl stop morpheus-ui
[root@app-server-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@app-server-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 it require minor manual intervention. Regardless, it is considered best practice when recovering a restart to perform some manual health checks.

```
[root@app-server-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;
```

(continues on next page)
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.

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@app-server-2 ~]# curl localhost:9200/_cat/nodes
app-server-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@app-server-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@app-server-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@app-server-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@app-server-2 ~]# curl localhost:9200/_cat/nodes
app-server-1 10.100.10.121 9 53 0.31 d * morpheus1
localhost 127.0.0.1 4 30 0.32 d m morpheus2
app-server-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@app-server-1 ~]# /opt/morpheus/embedded/lib/erlang/erts-5.10.4/bin/epmd -daemon
```

And then restarting RabbitMQ:

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

And then restarting the Morpheus UI service:

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

Again, it is always advisable to monitor the startup to ensure the Morpheus Application is starting without error.
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@app-server-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.

### 1.7 Morpheus CLI

#### 1.7.1 Installing on Linux

The Morpheus CLI is a ruby based CLI that provides a lot of functionality out of the box and is rapidly growing in coverage to be able to perform every task that can be performed in the Morpheus UI. It is also a great way to get started in exploring the Morpheus API and understanding some of the data model aspects.
**Installation**

A Prerequisite to running the CLI is to have ruby 2.2.0+ installed (2.3.0 recommended). To install Ruby please follow these instructions:

ruby-prerequisite

Once the ruby runtime is installed simply use rubygems to install the CLI

```ruby
gem install morpheus-cli
```

Once the gem is installed all cli commands can be run on the shell via morpheus.

### 1.7.2 Installing on Windows

The morpheus cli is capable of running on many platforms due to its ruby runtime. This includes windows based platforms. To get started, we must first ensure ruby is running on the windows machine in question. To do this please visit ruby-prerequisite and download at least Ruby version 2.2.0 (2.3.3 recommended).

**Note:** When installing ruby on windows, make sure the options are selected for adding the ruby binaries to your PATH.

Now that ruby is installed, simply open a PowerShell window and run

```sh
gem install morpheus-cli --no-ri --no-rdoc
```

A list of installed dependencies should start sliding by the screen. Once this has completed the CLI setup is complete. Now all that must be done is configuring the cli to point to an appliance for use.

```shell
morpheus remote add myapp https://applianceUrl
morpheus remote use myapp
morpheus login
```

Credentials are used to acquire an access token which is then stored in the users home directory in a folder called `.morpheus`. Now all commands provided by the CLI are available for use just as if running in a *nix based environment.

### 1.7.3 Setup

The first thing that needs to be done after installing the cli is pointing the cli to the appliance. The CLI can be pointed at many appliances and uses the RESTful OAUTH public developer apis to perform tasks. To set this up simply add a remote appliance with the morpheus remote add command.

```shell
morpheus remote add myappliance https://applianceUrl
morpheus remote use myappliance
morpheus login
```

There are several commands available when dealing with configuration of remote appliances. To see what commands are available just type

```sh
morpheus remote
```
Getting Started

To get started with the morpheus CLI its helpful to use morpheus shell. The shell provides a handy shell with history and some autocomplete features for learning to use it. All commands mentioned prefixed with morpheus can be omitted since we are in shell mode.

To confirm that we are hooked into the appliance properly lets check our authentication information:

```
morpheus> whoami
Current User
==================
ID: 1
Account: Labs (Master Account)
First Name: Demo
Last Name: Environment
Username: Example
Email: Example@morpheusdata.com
Role: System Admin

Remote Appliance
==================
Name: demo
Url: https://demo.morpheusdata.com
Build Version: 2.10.0
```

Fantastic! We are now ready to start our adventure in the Morpheus CLI. If this command fails please be sure to verify the appliance url entered previously is correct, and also verify the provided credentials are correctly entered.

While the CLI is relatively young there are a ton of features provided with it that can make it very convenient for working with morpheus. There are several base commands with subcommands within for example. Lets look at what happens when we simply type `morpheus` on the command line:

```
Usage: morpheus [command] [options]

Commands:
  remote
  login
  logout
  whoami
  groups
  clouds
  hosts
  load-balancers
  shell
  tasks
  workflows
  deployments
  instances
  apps
  app-templates
  deploy
  license
  instance-types
  security-groups
  security-group-rules
  accounts
```

(continues on next page)
As you can see the cli is split into sections. Each of these sections has subcommands available for performing certain actions. For example lets look at `morpheus instances`

```
morpheus> instances
Usage: morpheus instances [list,add,remove,stop,start,restart,backup,run-workflow,
˓→stop-service,start-service,restart-service,resize,upgrade,clone,envs,setenv,delenv]
˓→[name]
```

These commands typically make it easier to figure out what command subsets are available and the CLI documentation can provide helpful information in more depth on each command option.

**Provisioning**

To get started provisioning instances from the CLI a few prerequisite commands must be setup in the CLI. First we must decide what Group we want to provision into. We can first get a list of available groups to use by running `morpheus groups list`

```
morpheus> groups list
Morpheus Groups
==================
= Automation - denver
=> Demo - Multi
= Morpheus AWS - US-West
= Morpheus Azure - US West
= Morpheus Google - Auto
= morpheus-approvals -
= Nick-Demo - Chicago
= San Mateo Hyper-V - San Mateo, CA
= San Mateo Nutanix - San Mateo, CA
= San Mateo Openstack - San Mateo, CA
= San Mateo Servers - San Mateo, CA
= San Mateo UCS - San Mateo, CA
= San Mateo Vmware - San Mateo, CA
= San Mateo Xen - San Mateo, CA
= snow-approvals -
= SoftLayer - Dallas-9
```

In the above example the currently active group is Demo as can be seen by the `=>` symbol to the left of the group name. To switch groups simply run:

```
morpheus groups use "San Mateo Xen"
```

This now becomes the active group we would like to provision into. Another thing to know before provisioning is we do have to also specify the cloud we want to provision into. This does require the cloud be in the group that is currently active. To see a list of clouds in the relevant group simply run:
morpheus clouds list -g [groupName]

This will scope the clouds command to list only clouds in the group specified.

Morpheus makes it very easy to get started provisioning via the CLI. It provides a list of instance-types that can be provisioned via the `instance-types list` command. Let's get started by provisioning an Ubuntu virtual machine.

```
morpheus> instances add

Usage: morpheus instances add TYPE NAME
   -g, --group GROUP Group
   -c, --cloud CLOUD Cloud
   -O, --option OPTION Option
   -N, --no-prompt Skip prompts. Use default values for all optional fields.
   -j, --json JSON Output
   -d, --dry-run Dry Run, print json without making the actual request.
   -r, --remote REMOTE Remote Appliance
   -U, --url REMOTE API Url
   -u, --username USERNAME Username
   -p, --password PASSWORD Password
   -T, --token ACCESS_TOKEN Access Token
   -C, --nocolor ANSI
   -V, --debug Print extra output for debugging.
   -h, --help Prints this help

morpheus> instances add ubuntu MyInstanceName -c "San Mateo Vmware"

morpheus> instances add ubuntu -c "San Mateo Vmware" dre-test

Layout ['?'] for options]: ?
   * Layout [-O layout=] - Select which configuration of the instance type to be provisioned.

Options
--------------------
   * Docker Ubuntu Container [104]
   * VMware VM [105]
   * Existing Ubuntu [497]

Layout ['?'] for options]: VMware VM
Plan ['?'] for options]: ?
   * Plan [-O servicePlan=] - Choose the appropriately sized plan for this instance

Options
--------------------
   * Memory: 512MB Storage: 10GB [10]
   * Memory: 2GB Storage: 20GB [12]
   * Memory: 4GB Storage: 40GB [13]
   * Memory: 8GB Storage: 80GB [14]
   * Memory: 24GB Storage: 240GB [16]
   * Memory: 32GB Storage: 320GB [17]

(continues on next page)
As can be seen in the example above, the CLI nicely prompts the user for input on required options for provisioning this particular instance type within this particular cloud. It provides capabilities of adding multiple disks and multiple networks in this scenario. It is also possible to skip these prompts and provision everything via one command line syntax by using the `-O optionName=value` syntax:

```
morpheus> instances add ubuntu MyInstanceName -c "San Mateo Vmware" -O
˓
layout=105 -O servicePlan=10 -O rootVolume.datastoreId=autoCluster
```

This will cause morpheus cli to skip prompting for input on these prompts. All inputs have an equivalent `-O` option that can be passed. To see what that option argument is simply enter `?` on the input prompt to get specifics.

Now your VM should be provisioning and status can be checked by simply typing `morpheus instances list`. 

38 Chapter 1. Getting Started
List Arguments

Most of the list command types can be queried or paged via the cli. To do this simply look at the help information for the relevant list command

```
morpheus> instances list -h
Usage: morpheus [options]
-g, --group GROUP     Group Name
-m, --max MAX          Max Results
-o, --offset OFFSET    Offset Results
-s, --search PHRASE    Search Phrase
-S, --sort ORDER       Sort Order
-D, --desc             Reverse Sort Order
-j, --json             JSON Output
-r, --remote REMOTE    Remote Appliance
-U, --url REMOTE       API Url
-u, --username USERNAME Username
-p, --password PASSWORD Password
-T, --token ACCESS_TOKEN Access Token
-C, --nocolor          ANSI
-V, --debug            Print extra output for debugging.
-h, --help             Prints this help
```

1.7.4 Ruby Installation

Step 1 – Installing Requirements

First of all, we need to install all required packages for ruby installation on our system using the following command.

```
yum install gcc-c++ patch readline readline-devel zlib zlib-devel libyaml-devel
    --libffi-devel openssl-devel make bzip2 autoconf automake libtool bison iconv-devel
    --sqlite-devel
```

Step 2 – Install RVM

Install the latest stable version of RVM on your system using the following command. This command will automatically download all required files and install on your system.

```
curl -sSL https://rvm.io/mpapis.asc | gpg --import -
curl -L get.rvm.io | bash -s stable
```

Also, run below command to load the RVM environment.

```
source /etc/profile.d/rvm.sh
rvm reload
```

Step 3 – Verify Dependencies

Now use the following command to verify all dependencies are properly installed. This will install any missing dependencies on your system.
Step 4 – Install Ruby 2.5

After completing setup of RVM environment lets install Ruby language using the following command. Change Ruby version to below command you need to install.

```bash
rvm install 2.5
```

[Sample Output]

Searching for binary rubies, this might take some time.
No binary rubies available for: centos/7/x86_64/ruby-2.5.1.
Continuing with compilation. Please read ‘rvm help mount’ to get more information on binary rubies.
Checking requirements for centos.
Requirements installation successful.
Installing Ruby from source to: /usr/local/rvm/rubies/ruby-2.5.1, this may take a while depending on your cpu(s)...
---> extracting ruby-2.5.1 to /usr/local/rvm/src/ruby-2.5.1.......
---> configuring...............................................................
---> post-configuration..
---> installing............................
---> making binaries executable..
---> downloading rubygems-2.7.7
---> extracting rubygems-2.7.7...............................................
---> removing old rubygems........
---> installing rubygems-2.7.7-------------------------------
---> gemset created /usr/local/rvm/gems/ruby-2.5.1@global
---> importing gemset /usr/local/rvm/gemsets/global.gems..............................
---> generating global wrappers......
---> gemset created /usr/local/rvm/gems/ruby-2.5.1
---> importing gemsetfile /usr/local/rvm/gemsets/default.gems evaluated to an empty gem list
---> generating default wrappers......
---> adjusting #shebangs for (gem irb erb ri rdoc testrb rake).
Install of ruby-2.5.1 - #complete
Ruby was built without documentation, to build it run: rvm docs generate-ri

Step 5 – Setup Default Ruby Version

First of all, check the currently installed ruby versions on your system. So that we can find which version is using currently by the system and which is set to default.
rvm list
ruby-2.3.5 [ x86_64 ]
ruby-2.4.2 [ x86_64 ]
* ruby-2.4.4 [ x86_64 ]
=> ruby-2.5.1 [ x86_64 ]
# => - current
# *= - current && default
# * = default

After that use rvm command to set up the default ruby version to be used by applications.

rvm use 2.5 --default
Using /usr/local/rvm/gems/ruby-2.5.1

Step 6 – Verify Active Ruby Version

Using following command you can check the current ruby version is used.

ruby --version
ruby 2.5.1p57 (2018-03-29 revision 63029) [x86_64-linux]

Step 7 – Install Morpheus CLI

gem install morpheus-cli

1.8 Morpheus Agent

The Morpheus Agent is an important and powerful facet of Morpheus as a orchestration tool. Though it is not required (one unique capability of our platform vs. some of the competitors out there), it is recommended for use as it brings with it a lot of insightful benefits. Not only does it provide statistics of 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. The Morpheus Agent is very lightweight and secure.

Note: The agent is not required by Morpheus to become a managed instance. If you don’t have the agent installed we try to aggregate stats but it can vary based on the cloud and can be limited or inaccurate.

The Morpheus Agent 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 things 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 up with regards to the agent while demonstrating its security benefits as well as 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.

1.8.1 Key Agent Features

- Provides key enhanced statistics (disc usage, CPU usage, network, disc IO)
• Handles log aggregation
• Provides a command bus to where Morpheus doesn’t need to get credentials to access a box. Can still run workflows if credentials are changed
• SSH agent can be disabled and still get access to the box
• Agent can be installed over Cloud Init for internetless situations
• The Morpheus agent is optional
• Makes a single connect that’s persistence over HTTPS web socket and runs as a service
• Health checks for Linux (not available on windows)
• No inbound Ports
• Agent buffers and compresses logs and sends them in chunks to minimize packets
• Can be configured to collect logs and send them somewhere
• Linux agent can be shrunk and should be less then .2% peak (Windows less 97 kb)
• Run workflows, Have expiration/shutdown policies and can help reign in environments amongst other things
• Accepts commands, can execute commands, write files, and manipulate firewall

1.8.2 Morpheus Agent Support

Microsoft Windows

Note: if you require tls 1.2 then .net 4.5 should be installed.

• Windows Server 2008R2 (Requires .Net 4.3 framework)
• Windows Server 2012
• Windows Server 2012R2
• Windows Server 2016
• Windows Server 2019
• Windows 10 PRO

Redhat Based linux Distrubition:

• Redhat 6.6
• Redhat 7.x
• CentOS 6.x
• CentOS 7.x
• Oracle 6.x
• Oracle 7.x
Debian Based Linux Distributions:

- Ubuntu 14.04.x
- Ubuntu 16.04.x
- Ubuntu 18.04.x (Only supported for VM, not docker host)
- Debian 8.x
- Debian 9.x

Unix Based Operating Systems:

- MacOS Mojave
- MacOS High Sierra
- MacOS Sierra

1.9 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:** Work loads 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)
1.10 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**  This list 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, redis, 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:

<table>
<thead>
<tr>
<th>General Commands:</th>
</tr>
</thead>
<tbody>
<tr>
<td>cleanse</td>
</tr>
<tr>
<td>Delete <em>all</em> morpheus data, and start from scratch.</td>
</tr>
<tr>
<td>help</td>
</tr>
<tr>
<td>Print this help message.</td>
</tr>
<tr>
<td>reconfigure</td>
</tr>
<tr>
<td>Reconfigure the application.</td>
</tr>
<tr>
<td>show-config</td>
</tr>
<tr>
<td>Show the configuration that would be generated by reconfigure.</td>
</tr>
<tr>
<td>uninstall</td>
</tr>
<tr>
<td>Kill all processes and uninstall the process supervisor (data will be preserved).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Service Management Commands:</th>
</tr>
</thead>
<tbody>
<tr>
<td>graceful-kill</td>
</tr>
<tr>
<td>Attempt a graceful stop, then SIGKILL the entire process group.</td>
</tr>
<tr>
<td>hup</td>
</tr>
<tr>
<td>Send the services a HUP.</td>
</tr>
<tr>
<td>int</td>
</tr>
<tr>
<td>Send the services an INT.</td>
</tr>
<tr>
<td>kill</td>
</tr>
<tr>
<td>Send the services a KILL.</td>
</tr>
<tr>
<td>once</td>
</tr>
<tr>
<td>Start the services if they are down. Do not restart them if they stop.</td>
</tr>
<tr>
<td>restart</td>
</tr>
<tr>
<td>Stop the services if they are running, then start them again.</td>
</tr>
<tr>
<td>service-list</td>
</tr>
<tr>
<td>List all the services (enabled services appear with a *.)</td>
</tr>
<tr>
<td>start</td>
</tr>
<tr>
<td>Start services if they are down, and restart them if they stop.</td>
</tr>
<tr>
<td>status</td>
</tr>
<tr>
<td>Show the status of all the services.</td>
</tr>
<tr>
<td>stop</td>
</tr>
<tr>
<td>Stop the services, and do not restart them.</td>
</tr>
<tr>
<td>tail</td>
</tr>
<tr>
<td>Watch the service logs of all enabled services.</td>
</tr>
</tbody>
</table>

(continues on next page)
term
  Send the services a TERM.

Elasticsearch Commands:

  elastic-utility
    Backup/Restore ElasticSearch data

Firewall Commands:

  firewall-enable-blocking
    Enables firewall blocking mode.
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.

2.1 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 lots 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.

2.1.1 VM Provision Steps

While an infinite number of steps can happen when provisioning an Instance or App using a 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 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 TOLLS 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.

2.1.2 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 scrip 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 upon 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 Images that has Cloud Init Enabled? checked on the Virtual Record in Morpheus but does not have cloud-init install 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 -> 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 n 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 configure 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 of the Windows Image has been sys-prepped. If enabled Morpheus will inject Unattend.xml through the Nutanix API (v3+ only)

**Important:** Provisioning a Virtual Images that has Cloud Init Enabled? checked on the Virtual Record in Morpheus but does not have cloud-init install will result in immediate provisioning failure.

**Important:**  For Linux images without Cloud-Init, and 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.

2.1.3 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 Admin -> 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 Admin -> 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 (Admin -> 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.

• 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 Provisioning - 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 configure, 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 Provisioning -> 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 Provisioning -> 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 Provisioning -> Virtual Images section.
Cloud-Init agent install mode

- Cloud-Init is configured in Admin -> Provisioning section
- Provisioned image/blueprint has Cloud-Init (linux) or Cloudbase-Init (windows) installed

2.2 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.

2.2.1 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.

2.2.2 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 deliniate 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).

2.2.3 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 injest “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.

### 2.2.4 Apps

On top of all the previous concept, 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 like Consul.

### 2.2.5 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.

### 2.3 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 statistic 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.
2.3.1 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 Provisioning -> 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).

2.3.2 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
Morpheus Documentation, Release 3.6.1

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.

Console  Access the instance or container via a client-less Console supporting SSH, RDP, VNC, and even hypervisor level remote consoles.

2.3.3 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 associated VM’s or Containers and cannot be undone. To delete instances without deleting associated VM’s, delete the VM from the Infrastructure section and uncheck “Remove Infrastructure” while checking “Remove Associated Instances” in the delete modal options.

**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/Restart Service**  Stops, Starts or Restarts the service associated with the Instance Type.

**Stop/Start/Restart Server**  Stops, Starts or Restarts the Virtual Machine.

**Lock/Unlock Instance**  A locked instance cannot be deleted until it is unlocked.

**Import As Image**  Creates a Virtual Image Blueprint from the Instance at its current state and adds it to the Virtual Image library with corresponding metadata.
**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 Provisioning -> Automation section.

**Run Script**  Presents Script options and immediately executes selected Script on the Instance. Scripts can be created in the Provisioning -> Library section.

**Apply Template**  Presents Template options and immediately applies selected Template to the Instance. Templates can be created in the Provisioning -> 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 Notes section for adding useful information about the Instance. Notes can be added by selecting the ADD NOTES button on the bottom of Instance Detail pages. Existing notes can be edited by selecting the EDIT NOTES.

---

**Tip:** Markdown Syntax is supported in Instance Notes.

---

**2.4 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.
## 2.4.1 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.

## 2.4.2 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.

### 2.4.3 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.

### 2.4.4 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 proccess: `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 connection will resemble:

```
guacd[24725]: INFO: Creating new client for protocol "ssh"
guacd[24725]: INFO: Connection ID is "$24f67856-f050-4a17-83eb-9101g0cd8869"
guacd[24743]: INFO: Current locale does not use UTF-8. Some characters may not...render correctly.
guacd[24743]: INFO: User "$63102f19-eff4-412e-b1f9-718405f55782" joined...
...connection "$24f67856-f050-4a17-83eb-9101g0cd8869" (1 users now present)
guacd[24743]: INFO: Auth key successfully imported.
guacd[24743]: INFO: SSH connection successfully established.
```

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`

### 2.5 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 Provisioning -> Blueprints or from Existing Apps.

#### 2.5.1 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:** Blueprints must be created in Provisioning -> Blueprints. to appear as options when creating 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.
2.5.2 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
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.
2.5.3 Exporting JSON or YAML

1. Navigate to Provisioning -> Apps
2. On an existing App, select ACTIONS -> EXPORT
3. Select YAML or JSON in the top right.
4. Select the Configurations to include in the Export by clicking on a Configuration. Selected Configurations will be highlighted.
5. Select the DOWNLOAD CONFIGURATION button.

6. The Blueprint Export file will be downloaded to your computer as `{app_name}-config.json` or `{app_name}-config.yaml`.

**Tip:** JSON or YAML can also be Viewed, Edited, Copied, or Exported by selecting ACTIONS -> EDIT on an App and clicking the RAW section in the Edit App modal.
2.5.4 Provisioning Apps via API

A quick example of how this works: https://d.pr/i/yxsW7t
2.6 Blueprints

2.6.1 Overview

With the release of Morpheus version 3, a new app blueprint builder was developed from scratch and extended to support a vast array of configurations even with programmatic markup or (Infrastructure as Code) capabilities.

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.

Some unique capabilities of the YAML/JSON based Morpheus blueprint structure is it’s 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 or group the app is being provisioned in as a target. The environment can also be used as a scope. Maybe the “development” environment doesn’t need as many horizontally scaled nodes (for example) 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 Cloud Formation 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
      instances:
    Database:
      tier:  
        bootOrder: 0
        instances:
```

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 object structure.

Configuration Scopes

Another capability of Morpheus App Blueprint structure is its configuration scoping. This allows properties to be overridden based on the apps 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.

```yaml
name: Simple Nginx
type: morpheus
tiers:
  Web:
    instances:
      - instance:
          type: docker
          name: Sample Nginx
    clouds:
      AWS Cali:
        instance:
          layout:
            code: docker-1.7-single
        config:
          dockerImageVersion: latest
          dockerRegistryId: ''
          dockerImage: nginx
        plan:
          code: container-128
    environments:
      Production:
        groups:
          All Clouds Demo:
            clouds:
              AWS Cali:
                plan:
                  code: container-256
```

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 users 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 lets look at a Blueprint that deploys a single nginx container to a target cloud:

```yaml
name: Simple Nginx
type: morpheus
tiers:
  Web:
    linkedTiers: []
    instances:
      - instance:
          type: docker
          name: Sample Nginx
    clouds:
      AWS Cali:
        instance:
          layout:
```

(continues on next page)
Theres 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 option types 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.
2.6.2 Creating App Blueprints

1. Navigate to Provisioning -> 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 by selecting the Lock icon next to the Field. Locking prevent the field from being editable when provisioning an App using the Blueprint.
   • 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.
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. Create or Edit a Blueprint
2. Select the RAW section on the top of the APP BLUEPRINT modal.
3. Select JSON or YAML in the top right of the RAW section.
4. Select the EXPORT button.
5. Select the Configurations to include in the Export by clicking on a Configuration. Selected Configurations will be highlighted.
6. Select the DOWNLOAD CONFIGURATION button.
7. The Blueprint Export file will be downloaded to your computer as {template_name}-config.json or {template_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.

2.7 Automation

 Provisioning -> 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 are combined into workflows, which can be selected to run at provision time or executed on existing instances via Actions -> Run Workflow.

2.7.1 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.

### Add a Task

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

### Edit a Task

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.

### Delete a Task

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 Types

<table>
<thead>
<tr>
<th>Task Type</th>
<th>Task Description</th>
<th>Task Target</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>Instance or Host</td>
<td>Existing Ansible Integration</td>
<td>Provisioning: Tasks</td>
</tr>
<tr>
<td>Chef boot-strap</td>
<td>Executes Chef bootstrap and run list. Chef Integration required</td>
<td>Instance or Host</td>
<td>Existing Chef Integration</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>None</td>
<td>Provisioning: Tasks</td>
</tr>
<tr>
<td>HTTP</td>
<td>Executes REST call for targeting external API’s.</td>
<td>URL specified in Task</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>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>None</td>
<td>Provisioning: Tasks</td>
</tr>
<tr>
<td>Library Script</td>
<td>Creates a Task from an existing Library Script (Provisioning -&gt; Library -&gt; Scripts)</td>
<td>Instance or Host</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 (Provisioning -&gt; Library-&gt; Templates)</td>
<td>Instance or Host</td>
<td>Existing Library Templates</td>
<td>Provisioning: Tasks</td>
</tr>
<tr>
<td>Local Shell Script</td>
<td>Executes Bash script locally (on Morpheus app node)</td>
<td>Local</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>Instance or Host</td>
<td>Existing Puppet Integration</td>
<td>Provisioning: Tasks</td>
</tr>
<tr>
<td>Python Script (jython)</td>
<td>Executes Python script locally (on Morpheus app node)</td>
<td>Local</td>
<td>None</td>
<td>Provisioning: Tasks</td>
</tr>
<tr>
<td>Remote Shell Script</td>
<td>Executes Bash script against the Instance or Host the Task or Workflow is ran on</td>
<td>Instance or Host</td>
<td>None</td>
<td>Provisioning: Tasks</td>
</tr>
<tr>
<td>Restart</td>
<td>Restarts target VM/Host/Container and confirms status before executing next task in Workflow</td>
<td>Instance or Host</td>
<td>None</td>
<td>Provisioning: Tasks</td>
</tr>
<tr>
<td>SSH Script</td>
<td>Execute Bash script against IP specified in Task.</td>
<td>IP specified in Task</td>
<td>None</td>
<td>Provisioning: Tasks</td>
</tr>
<tr>
<td>WinRM Script</td>
<td>Execute Powershell script against IP specified in Task.</td>
<td>IP specified in Task</td>
<td>None</td>
<td>Provisioning: Tasks</td>
</tr>
</tbody>
</table>
**Ansible Playbook**

**Description** Runs an Ansible playbook. Ansible Integration required

**Target** Instance or Host

**Role Permissions** Provisioning: Tasks

**Task Configuration**

- **NAME** Name of the Task
- **CODE** Unique code name for api, cli, and variable reference
- **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 Ref’s 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**

**Description** Executes Chef bootstrap and run list. Chef Integration required

**Target** Instance or Host

**Role Permissions** Provisioning: Tasks

**Task Configuration**

- **NAME** Name of the Task
- **CODE** Unique code name for api, cli, and variable reference
- **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**

**Description**  Executes Groovy Script locally (on app node)

**Target**  Local App Node

**Role Permissions**  Provisioning: Tasks Provisioning: Tasks - Script Engines

**Task Configuration**

- **NAME**  Name of the Task
- **CODE**  Unique code name for api, cli, and variable reference
- **RESULT TYPE**
  - Single Value
  - Key/Value Pairs
  - JSON
- **SCRIPT**  Contents of Groovy Script to execute

**HTTP (api)**

**Description**  Executes REST call for targeting external API’s.

**Target**  URL specified in Task

**Role Permissions**  Provisioning: Tasks

**Task Configuration**

- **NAME**  Name of the Task
- **CODE**  Unique code name for api, cli, and variable reference
- **RESULT TYPE**
  - Single Value
  - Key/Value Pairs
  - JSON
- **URL**  http or https url for 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
Table 2: **Http Header examples**

<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>

**JavaScript**

**Description**  
Executes Javascript locally (on app node)

**Target**  
Local App Node

**Role Permissions**  
Provisioning: Tasks Provisioning: Tasks - Script Engines

**Task Configuration**

- **NAME**  
Name of the Task

- **CODE**  
Unique code name for api, cli, and variable reference

- **RESULT TYPE**
  - Single Value
  - Key/Value Pairs
  - JSON

- **SCRIPT**  
Contents of Javascript to execute

**jRuby Script**

**Description**  
Executes Ruby script locally (on app node)

**Target**  
Local App Node

**Role Permissions**  
Provisioning: Tasks Provisioning: Tasks - Script Engines

**Task Configuration**

- **NAME**  
Name of the Task

- **CODE**  
Unique code name for api, cli, and variable reference

- **RESULT TYPE**
  - Single Value
  - Key/Value Pairs
  - JSON

- **SCRIPT**  
Contents of jRuby Script to execute
**Library Script**

**Description** Creates a Task for an existing Library Script (Provisioning -> Library -> Scripts)

**Target** Instance or Host

**Role Permissions** Provisioning: Tasks

**Task Configuration**

- **NAME** Name of the Task
- **CODE** Unique code name for api, cli, and variable reference
- **RESULT TYPE**
  - Single Value
  - Key/Value Pairs
  - JSON
- **SCRIPT** Search for and select existing Library Script

---

**Library Template**

**Description** Creates a Task for an existing Library Template (Provisioning -> Library-> Templates)

**Target** Instance or Host

**Role Permissions** Provisioning: Tasks

**Task Configuration**

- **NAME** Name of the Task
- **CODE** Unique code name for api, cli, and variable reference
- **TEMPLATE** Search for and select existing Library Template

---

**Local Script**

**Local Shell Script**

**Description** Executes Bash script locally (on Morpheus app node)

**Target** Local App Node

**Role Permissions** Provisioning: Tasks Provisioning: Tasks - Script Engines

**Task Configuration**

- **NAME** Name of the Task
- **CODE** Unique code name for api, cli, and variable reference
- **RESULT TYPE**
• Single Value
• Key/Value Pairs
• JSON

**GIT REPO**  Select a Git Repo which can be referenced in the Script.

**GIT REF**  Specify git ref such as branch

**SCRIPT**  Bash Script to execute. If a Git Repo is specified, files in the repo can be called in the script.

---

**Puppet Agent Install**

**Description**  Executes Puppet Agent bootstrap, writes puppet.conf and triggers agent checkin. Puppet Integration required

**Target**  Instance or Host

**Role Permissions**  Provisioning: Tasks

**Task Configuration**

**NAME**  Name of the Task

**PUPPET MASTER**  Select Puppet Master from existing Puppet Integration

**PUPPET NODE NAME**  Enter Puppet Node Name. Variables supported eg. "<%= instance.name %>

**PUPPET ENVIRONMENT**  Enter Puppet Env. eg. production

---

**Python Script (jython)**

**Description**  Executes Python script locally (on app node)

**Target**  Local App Node

**Role Permissions**  Provisioning: Tasks Provisioning: Tasks - Script Engines

**Task Configuration**

**NAME**  Name of the Task

**CODE**  Unique code name for api, cli, and variable reference

**TYPE**  Python Script (jython)

**RESULT TYPE**
• Single Value
• Key/Value Pairs
• JSON

**SCRIPT**  Python Script (jython) Script to execute
Remote Shell Script

**Description**  Executes Bash script against the Instance or Host the Task or Workflow is ran on

**Target**  Instance or Host

**Role Permissions**  Provisioning: Tasks

**Task Configuration**

- **NAME**  Name of the Task
- **CODE**  Unique code name for api, cli, and variable reference
- **RESULT TYPE**
  - Single Value
  - Key/Value Pairs
  - JSON
- **SCRIPT**  Enter Bash Script to execute

Restart

**Description**  Specifically for use in Workflows after a task that requires a restart, the Restart task executes a restart on the target Instance or Host. Morpheus will wait until the restart is complete to execute the next task in the workflow phase.

**Target**  Instance or Host

**Role Permissions**  Provisioning: Tasks

**Task Configuration**

- **NAME**  Name of the Task
- **CODE**  Unique code name for api, cli, and variable reference

SSH Script

**Description**  Execute Bash script against IP specified in Task.

**Target**  IP specified in Task

**Role Permissions**  Provisioning: Tasks

**Task Configuration**

- **NAME**  Name of the Task
- **CODE**  Unique code name for api, cli, and variable reference
- **RESULT TYPE**
  - Single Value
• Key/Value Pairs
• JSON
  
  **IP ADDRESS**  IP Address of the ssh task target
  **PORT**  SSH port for ssh task target (22 default)
  **KEY**  Select existing Keypair for key auth
  **USERNAME**  Username for ssh task target
  **PASSWORD**  Password for ssh task target
  **SCRIPT**  Enter Bash Script to execute

### WinRM Script

![Windows Remote Management](image)

**Description**  Execute Powershell script against IP specified in Task.

**Target**  IP specified in Task

**Role Permissions**  Provisioning: Tasks

### Task Configuration

- **NAME**  Name of the Task
- **CODE**  Unique code name for api, cli, and variable reference
- **RESULT TYPE**
  - Single Value
  - Key/Value Pairs
  - JSON
- **IP ADDRESS**  IP Address of the WinRM task target
- **PORT**  SSH port for WinRM task target (5985 default)
- **USERNAME**  Username for WinRM task target
- **PASSWORD**  Password for WinRM task target
- **SCRIPT**  Enter Script to execute

### Task Results

**Overview**

Task Results allow Tasks to use the output from preceding Tasks in the same Workflow via results variables.

### Configure Tasks

In script type tasks, if **RESULT TYPE** is set, Morpheus will store the Task's output as a variable.
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.

---

Examples

**Single Value using Task Code**

Source Task Config

<table>
<thead>
<tr>
<th>NAME</th>
<th>Var Code (single)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CODE</td>
<td>single</td>
</tr>
<tr>
<td>RESULT TYPE</td>
<td>Single Value</td>
</tr>
<tr>
<td>SCRIPT</td>
<td><code>echo &quot;string value&quot;</code></td>
</tr>
</tbody>
</table>

Source Task Output  
string value

Results Task using task code in variable

- Results Task Script  
  `echo "single: <%=results.single%>"`

- Results Task Output  
  single: string value

**Single Value using Task Name**

Source Task Config

<table>
<thead>
<tr>
<th>NAME</th>
<th>Var Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>CODE</td>
<td>none</td>
</tr>
<tr>
<td>RESULT TYPE</td>
<td>Single Value</td>
</tr>
<tr>
<td>SCRIPT</td>
<td><code>echo &quot;string value&quot;</code></td>
</tr>
</tbody>
</table>

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  keyval
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.keyval%>"
Results Task Output  keyval: [flash:bang, ping:pong]
Results Task for a single value
Results Task Script  echo "keyval value: <%=results.keyval.flash%>"
Results Task Output  keyval value: bang

JSON
Source Task Config
NAME  Var Code (json)
CODE  json
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.json%>"
Results Task Output  json: [ping:pong, flash:bang]
Results Task for a single value
Results Task Script  echo "json value: <%=results.json.ping%>"
Results Task Output  json value: pong

Results are available for all tasks executed in a workflow. For example, instead of using just one Task's results in another Task, we can use all of the Task Results from the tasks above in a single task inside a workflow.

Multiple Task Results
Results Task Script

echo "single: <%=results.single%>"
echo "task name: <%=results["Var Code"]%>"
echo "keyval: <%=results.keyval%>"
echo "keyval value: <%=results.keyval.flash%>"
echo "json: <%=results.json%>"
echo "json value: <%=results.json.ping%>"

Results Task Output

single: string value
task name: string value
keyval: [flash:bang, ping:pong]
2.7.2 Workflows

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 button.
5. From the New Workflow Wizard input a name for the workflow.
6. Optionally input a description.
7. Expand the execution phases to add tasks to, and type the name of a created task and click the task when it appears to add.
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. Click the Save Changes button to save.

Workflow Execution Phases

For VM’s, Pre-Provision and Provision execute after the VM is running. Pre-Provision can be used for a blueprint so it is added before a script 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 up. Post-Provision will execute after the entire provisioning process is complete.

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.

2.8 Virtual Images

Provisioning -> Virtual Images

2.8.1 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.

Important: Invalid Image Settings cause provisioning failures. Morpheus syncs in as much meta-data as possible for synced images, they still need to be properly configure 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.

2.8.2 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.

2.8.3 Configuring Virtual Images

System Images

System 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. It is highly recommended to populate the Administration -> Provisioning -> Cloud-Init section with user data prior to provisioning, as the user and password/key will be added to all Instances provisioned from System Images. Users can also be added during provisioning in the Add User provisioning wizard section.
**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 *Actions - Edit* in the Virtual Images list, or *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 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.
   - **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 or Guest Customizations are used, credentials are defined in Administration -> 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 n 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.
   - **Create Image**: Select FILE to select or drag and drop image file, or 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. No impact on single-tenant environments.
Auto Join Domain? Enable to have instances provisioned with this image auto-join configured domains (Windows only, domain controller must be configure 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.

Trial Version Enable to automatically re-arm the expiration on Windows Trial Images during provisioning.

Enabled Sysprep? Applicable to Nutanix Only. Enable of the Windows Image has been sys-prepped. If enabled Morpheus will inject Unattend.xml through the Nutanix API (v3+ only)

3. 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.

### 2.8.4 Provisioning Images

When provisioning a System Image for the first time, Morpheus will download and stream the image from S3 to the source Cloud if the image is not local to the Cloud. The Image will also be cached on the Morpheus Appliance under /var/opt/morpheus/vm/vmcache. Subsequent provisions of the image will use the created template in the Cloud or the cached local Image if the images does not exist in the selected Cloud, in which case the cached Image will be copied to the Cloud.

When using Images that already exist in the destination cloud, such as synced, marketplace, or previously copied images, no image transfer between the Morpheus Appliance and destination cloud will take place.

Note: The Morpheus Appliance must be able to download from Amazon S3 when provisioning System Images for the first time.

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.

### 2.8.5 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
   - VirtualBox
   - VirtualBox (vdi)
   - 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 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.
   - **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 or Guest Customizations are used, credentials are defined in *Administration -> 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.

**Create Image** Select FILE to select or drag and drop image file, or 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. No impact on single-tenant environments.

**Auto Join Domain?** Enable to have instances provisioned with this image auto-join configured domains (Windows only, domain controller must be configure 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.

**Trial Version** Enable to automatically re-arm the expiration on Windows Trial Images during provisioning.

**Enabled Sysprep?** Applicable to Nutanix Only. Enable of the Windows Image has been sys-prepped. If enabled Morpheus will inject Unattend.xml through the Nutanix API (v3+ only)

---

**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 *Administration -> 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.

2.9 Library

2.9.1 Overview

The Library section is used to add virtual images as custom instances to the provisioning catalog. The Library Section is composed of:

- Instance Types
- Layouts
- Node Types
- Option Types
- Option Lists
- File Templates
- Scripts

Uploaded or synced images from the virtual images section are added to nodes, a node or multiple nodes are added to layouts, and layouts are added to Instance Types. Scripts and File Templates can be attached to nodes, with phased execution options for scripts.
Adding an Instance Type creates a new Library Item category. Multiple layouts can be added to an instance type, and these layout can have different nodes attached. The instance 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**  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

**Icon**  Suggested Dimensions: 150 x 51

**Visibility**

• Private- Only accessibly by assigned Accounts/Tenants
• Public- accessible by all Accounts/Tenants

**Environment Prefix** Used for exportable environment variables when tying instance types together environment Variables in app contexts. If not specified a name will be generated

**Enable Scaling (Horizontal)** Enables load balancer assignment and auto-scaling features

**Supports 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.

**Note:** Custom Instance Types do not display logs on the instance page. Logs will only show on the VM page.
2.9.3 Node Types

The following fields are for all node technology types:

- Name
- Short Name
- Version
- Category
- Technology (Alibaba, Amazon, Azure, Docker, ESXi, Fusion, Google, Hyper-V, KVM, Nutanix, OpenStack, Oracle VM, SCVMM, UpCloud, vCloud Director, VMware, Xen)
- Environment Variables

The Options fields will change depending on the Technology option selected.

For VM provisioning technology options, select an image from the VM Image dropdown, which is populated from the Virtual Images Section and will include images uploaded into Morpheus, and 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.

For Docker, type in the name and version of the Docker Image and select the integrated registry.

**Expose Ports** To open port on the node, select “Add Port” and enter the name and port to expose. The Load Balancer http, https or tcp setting is only required when attaching to load balancers.

Example port configuration:

<table>
<thead>
<tr>
<th>NAME</th>
<th>PORT</th>
<th>LB</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>8000</td>
<td>HTTP</td>
</tr>
<tr>
<td>Collector</td>
<td>8088</td>
<td>None</td>
</tr>
<tr>
<td>Forwarder</td>
<td>9997</td>
<td>None</td>
</tr>
<tr>
<td>KVstore</td>
<td>8191</td>
<td>None</td>
</tr>
<tr>
<td>TCP</td>
<td>1514</td>
<td>None</td>
</tr>
<tr>
<td>Custom</td>
<td>1515</td>
<td>None</td>
</tr>
</tbody>
</table>

### 2.9.4 Scripts & File Templates

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.
Upon save the Node Type will be created, and available for adding to layouts.

### 2.9.5 Layouts

Layouts are added to Instance types, and will be presented under the Configuration Options dropdown in the Provisioning Wizard for that Instance type.

**Instance Type** Select the Instance Type to add the new Layout to. Custom Instance Types must already be created and one layout cannot be added to multiple instance types, or change Instance Types after creation.

**Name** The name the layout will present as in the Configuration Options dropdown in 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 in selected while provisioning.

**Description** Description of the layout

**Technology** Technology determines which cloud this layout will be available for.

**Environment Variables** Custom evars to be added to the instance when provisioned.
Nodes  Single or multiple nodes can be added to a Layout by searching for and selecting the node(s). An example of a layout with multiple nodes is the Hyper-V MySQL Master/Slave layout pictured below (note this is the Layout detail screen after the layout has been created.)

Multi-node Layout example:

Upon save, the layout will be attached to the selected Instance Type, and available when provisioning that Instance Type for the appropriate cloud technology.

2.9.6 Option Types

Option Types allow you to create additional fields within the provisioning wizard.
These field entries can then be used in scripts and templates using our variable naming convention (more here).
2.9.7 Option List

Much like Option Types, 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 either be manually entered CSV or JSON or they can be dynamically compiled from REST calls via GET or POST requests.
Your new Library Item is now ready for provisioning. Multiple Layouts, Versions and Technology types can be added to a single Instance Type.
2.10 Migrations

2.10.1 Migration Types

Hypervisor to Hypervisor

**Store** Morpheus will create a snapshot of existing VM and upload the snapshot to virtual image directory. Images that have been uploaded to the Virtual Images library can be converted to VHD, QCOW2, RAW and VMDK formats and then re-provisioned.

**New** Morpheus will create a snapshot of an existing VM, convert from source format to required destination format, and then provision the VM into the target environment.

**Source** VMWare, Openstack, Xen, Nutanix* Azure* Hyper-V* ( *in-development)

**Destination** Softlayer, Openstack, Metapod, Xen, Amazon, VMWare, ESXi, Nutanix, Hyper-V Supported OS Type: Windows or Linux

**Service Impact** Disruptive Migration

Virtual Image Extract

The Virtual Image extract capabilities allow for a virtual image to be extracted and stored in the virtual image repository or the image can be migrated into a cloud.

**Source** Any Cloud

**Destination** SoftLayer (Only)

**Supported OS Type** Windows

**Service Impact** Non Disruptive

**Requirements** Requires a separate disk or network share to store the image during conversion process. Capacity of the disk or network share should be sized appropriately to support the data that will be exported.

Live Stream

**Note:** Live Stream is deprecated

Live Stream is a linux only streaming process that will take a snapshot of a volume and allow it to be streamed to a destination linux system that is either existing or new. The destination linux must already exist and it can either be a managed or unmanaged VM in Morpheus . The destination will be overwritten from a root level perspective.

**Source** Any Cloud

**Destination** Morpheus

**Supported OS Type** Linux (Only)

**Service Impact** Non Disruptive

**Requirements** Requires the Linux host/guest to be configured for LVM and that free space of the capacity to be streamed is available. A destination linux host/guest must be available to receive the stream.
2.10.2 Add Migration

1. Select the Provisioning link in the navigation bar.
2. Select the Migrations link in the sub-navigations bar.
3. Click the Add Migration button.
4. From the Create Migration Wizard select the type of migration, then click the Next button.

Depending on the Migration Type selected input the following, then click the Next button.

- Hypervisor to Hypervisor * Select Cloud, and Server * Input Host, Remote Port, Username, and Password
- Live Stream * Select Platform, Existing or New, Cloud, and Server * Input Host, SSH Port, SSH User, SSH Password, Public Key, and Logical Volume Device. * Enter Destination details, then click the Next button.

5. Finalize your configuration if needed, then click the complete button.

2.10.3 Manually Start Migration

If you chose to not run your migration in the Create Migration Wizard then you will be able to manually start the migration.

1. Select the Provisioning link in the navigation bar.
2. Select the Migrations link in the sub-navigations bar.
3. Click the actions dropdown of the row of the migration you wish start, and select Run.

2.10.4 Remove Migration

1. Select the Provisioning link in the navigation bar.
2. Select the Migrations link in the sub-navigations bar.
3. Click the actions dropdown of the row of the migration you wish remove, and select Remove.

2.10.5 VMware to AWS Migration

Requirements

When performing a Hypervisor to Hypervisor migration from VMware to AWS, there are some requirements that must be met:

1. Add S3 Storage Provider to Morpheus
2. Set Image Transfer Store in you AWS cloud(s) settings in Morpheus
3. Create VM Import Service roles in your AWS account (not in Morpheus )
4. Storage Provider selected for migration destination must be set as a Local Storage Provider (not AWS)
Add S3 Storage Provider

In the `Infrastructure-> Storage` section, select `+ADD` and enter the same AWS Access key and Secret Key used to create your AWS cloud in Morpheus. Then add the S3 bucket name that the migration image(s) will be added to.

Set Image Transfer Store

Under `Infrastructure -> Clouds`, select your AWS cloud and click `EDIT`. Expand the Advanced Options section and for `IMAGE TRANSFER STORE` select the AWS S3 Storage Provider you created previously and then Save.

Add VM Import Service

Tip: Refer to the AWS document below to add the required VM Import Service role in AWS: http://docs.aws.amazon.com/vm-import/latest/userguide/import-vm-image.html

VM Import requires a role to perform certain operations in your account, such as downloading disk images from an Amazon S3 bucket. You must create a role named vmimport with a trust relationship policy document that allows VM Import to assume the role, and you must attach an IAM policy to the role.

To create the service role

Create a file named `trust-policy.json` with the following policy:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": { "Service": "vmie.amazonaws.com" },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals":{
          "sts:Externalid": "vmimport"
        }
      }
    }
  ]
}
```

You can save the file anywhere on your computer. Take note of the location of the file, because you’ll specify the file in the next step.

Use the `create-role` command to create a role named vmimport and give VM Import/Export access to it. Ensure that you specify the full path to the location of the `trust-policy.json` file.

```
aws iam create-role --role-name vmimport --assume-role-policy-document file://trust-policy.json
```

Create a file named `role-policy.json` with the following policy, where disk-image-file-bucket is the bucket where the disk images are stored:
Use the following put-role-policy command to attach the policy to the role created above. Ensure that you specify the full path to the location of the role-policy.json file.

```bash
aws iam put-role-policy --role-name vmimport --policy-name vmimport --policy-document file://role-policy.json
```

For more information about IAM roles, see IAM Roles in the IAM User Guide.

**Storage Providers**

Set the “Storage Provider” in the migration wizard destination as a Local Storage type, or leave as Select to use the Morpheus Appliance.

A local image must be created by Morpheus prior to S3 upload. A Local Storage provider can be used if one had been added in the Infrastructure-> Storage section. Simply leaving the Storage Provider setting as “select” will create an image on the Morpheus appliance, provided sufficient storage existing on the Morpheus appliance drive.

**Important:** Setting AWS as the Destination Storage Provider will result in a migration failure.

These settings will allow a successful migration from VMware to AWS using the Morpheus migration wizard.
2.11 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.

2.11.1 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 -> 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, its 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.

2.11.2 Deploying to an Instance

Now that a version has been added to a deployment it is easy to push that deploy out to any instance provisioned within Morpheus. Simply navigate to the specific Instance that 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.

2.11.3 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 Admin -> Provisioning once a storage provider is created within the account.

2.11.4 Add Deployment

1. Select the Provisioning link in the navigation bar.
2. Select the Deployments link in the sub-navigation bar.
3. Click the Add button.
4. Enter a Name for the deployment and a description (optional)
5. Click the Save Changes button to save.

2.11.5 Add Version

1. Select the Provisioning link in the navigation bar.
2. Select the Deployments link in the sub-navigation bar.
3. Click the Name of the deployment you would like to add a version to.
4. Click the Add Version button.
5. From the Add Version Wizard select the deployment type.
6. Input the Version of the deployment.
7. 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.

8. Click the Save Changes button to save.

2.11.6 Edit Deployment

1. Select the Provisioning link in the navigation bar.
2. Select the Deployments link in the sub-navigation bar.
3. Click the Edit Deployment icon on the row of the deployment you wish to edit.
4. Modify information as needed
5. Click the Save Changes button to save.

2.11.7 Delete Deployment

1. Select the Provisioning link in the navigation bar.
2. Select the Deployments link in the sub-navigation bar.
3. Click the Delete Deployment icon on the row of the deployment you wish to delete.
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.

### 3.1 Groups

#### 3.1.1 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

**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

**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"
3.1.2 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

Minimal values: `groups add CLITest`. There would be prompt to provide optional values for code and location.
3.1.3 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.

3.1.4 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.

3.1.5 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

3.1.6 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.

3.2 Clouds

3.2.1 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)
- Bluemix
- Bluemix Platform
- Cloud Foundry
- Dell (Cloud type for PXE and manually added Dell EMC Hosts)
- DigitalOcean
3.2 Clouds

- Google Cloud
- HPE (Cloud type for PXE and manually added HPE Hosts)
- HPE OneView
- Huawei
- Hyper-V
- Kubernetes
- MacStadium
- Metacloud
- Morpheus (Generic Cloud type for PXE 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 vCenter
- VMware vCloud Air
- VMware vCloud Director
- VirtualBox
- Virtustream
- XenServer

Information on each cloud type can be found in the Integration Guides section.

3.2.2 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 Integration Guides section.
3.2.3 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.
**Hosts**  The hosts tab panel displays available hosts in the cloud and displays power, os, name, type, cloud, ip address, nodes, disc space, memory, and status. You can add a container host from this by clicking the Container Hosts button, add a hypervisor host by clicking the HyperVisor button, or perform actions by click the Actions button.

**Virtual Machine**  Displays an Inventory of Existing Instances in your cloud configuration and provides details such as power, os, name, type, cloud, ip address, nodes, disc space, memory, and status.

**Bare Metal**  Setup PXE Boot in the Boot section to add bare metal servers. Once setup you can view information such as power, os, name, type, cloud, ip address, nodes, disc space, memory, and status.

**Security Groups**  The Security Groups tab panel displays a list of existing Security groups in the cloud. You can add a security group to this cloud by clicking the Edit Security Groups button.

**Load Balancers**  The load balancers tab panel displays available load balancers in the cloud and displays the name, description, type, cloud and host. You can add a load balancer from this tab by clicking the Add Load Balancer button.

**Networks**  Displays Networks synced or added to the Cloud.

**DataStores**  Displays Datastores synced or added to the Cloud.


**Policies**  Manages Policies enforced on the Cloud.

* + Container Host Provisions a Docker host into the Cloud, or adds an existing Docker Host (manual) to the Cloud. KVM hosts are also available for Morpheus and Bare Metal cloud types.

* + Hypervisor Add an existing Hypervisor to the Cloud. Not available for all Cloud types.

### 3.2.4 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 and managed Hosts and VM’s must be removed prior to deleting a cloud. To remove Instances, Hosts and VM’s from Morpheus without deleting them in the actual Cloud, select Delete on the Host or VM, unselect “Remove Infrastructure” and select “Remove Associated Instances” if Instance are associated with the Hosts or VMs.

### 3.3 Hosts

#### 3.3.1 Overview

The *Infrastructure -> Hosts* section provides a universal stage for viewing and managing Hosts and Virtual Machines from all of your Clouds.

In this section you can:

- View & Manage all Hosts, Virtual Machines & Bare Metal
- Provision Docker & KVM Hosts
• Convert existing hosts to Docker & KVM Hosts
• Add Hypervisors
• Convert Hosts, Virtual Machines and Bare Metal to Managed

**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.

### 3.3.2 Hosts

Hosts in Morpheus are Hypervisors and Docker Hosts that your VM’s and Container are hosted on, such as ESXi, Hyper-V and Docker Hosts. These Hosts are populated from integrated clouds, hosts provisioned from Morpheus, or manually added Hosts.

### 3.3.3 Virtual Machines

The Virtual Machines tab lists all Managed and Unmanaged VM’s across Morpheus. Managed VM’s are either provisioned by Morpheus, or inventoried VM’s that were converted to managed. Unmanaged VM’s are from Cloud integrations with “Inventory Existing Instances” enabled in the Cloud settings.

### 3.3.4 Bare Metal

Bare Metal hosts are from PXE Boot or manually added in this section. Bare Metal hosts that are also Hypervisors will be listed in both the Bare Metal and Hypervisor sections.

### 3.3.5 Docker Hosts

**Overview**

Morpheus can provision Docker Hosts into any cloud, convert existing Hosts to Docker Hosts, or even make itself a Docker Host.

**To add a Docker Host to any cloud:**

1. Navigate to Infrastructure -> Hosts
2. Click the `+CONTAINER HOST` button
3. Select a container host type
4. Select a Group

3.3. Hosts
5. Enter the following:
   • Name
   • Description
   • Visibility
   • Select a Cloud
   • Enter tags (optional)

Then click NEXT.

6. Configure the host options

Select a Service Plan (Volume, Memory and CPU count fields may not be shown if selected service plan does not have custom options enabled).

   • Add and set size the volumes
   • Set memory size
   • Set the CPU count
   • Select a network

Optionally configure the following:

   • OS username
   • OS password
   • Domain name
   • Hostname (default is the name previously provided for the container host)
Then click the NEXT button

7. Optionally add any Automation Workflows and configure for Backups.

8. Review and click Complete to save
Your new container host will begin provisioning, and soon be running and ready for containers.

**Add an existing Docker Host**

Morpheus can manage and inventory existing/brownfield Docker Hosts by using the Manual Docker Host option.

**Note:** Adding a Docker Host that was previously managed by another Morpheus Appliance will disable management of the host on that Appliance as the Morpheus Agent settings will be reconfigured.

**Note:** *Container Mode* on the Cloud settings where the Host is being added must be set to Morpheus for non-Kubernetes/Swarm hosts.

1. Navigate to Infrastructure -> Hosts
2. Select +CONTAINER HOST button
3. Select Manual Docker Host
4. In the CREATE HOST Wizard, enter the following:
   
   GROUP
   
   **GROUP** Select the Group this Host will be available for
   
   Select NEXT
   
   NAME
**CLOUD**  Select the Cloud the Host will be assigned to

**NAME**  Enter name for the Docker Host in Morpheus

**DESCRIPTION**  Enter optional description for the Docker Host

**VISIBILITY**  Select Tenant Visibility

**TAGS**  Add optional Morpheus tags (these are not meta-data tags)

Select *NEXT*

**CONFIGURE**

**SSH HOST**  Enter IP or resolvable hostname of the target host

**SSH USER**  Enter existing username on the target host

**SSH PASSWORD**  Enter password for SSH User

**PUBLIC KEY**  For key auth (recommended), copy and add the displayed Public Key to the *authorized_keys* file on the target host.

**PLAN**  Default Manual

**LVM ENABLED?**  Deselect if target host is not LVM enabled (required when using Morpheus provided docker images)

**DATA VOLUME**  Enter path of the target data volume on the target host

**SOFTWARE RAID?**  Enable for software RAID (disabled by default)

**NET INTERFACE**  Enter network interface name of target host’s target network

Select *NEXT*

**AUTOMATION**

**POST PROVISION**  Select a workflow to execute after Host is added (optional).

Select *NEXT*

**REVIEW**  Review settings and select *COMPLETE* to add the Manual Docker Host.

Your new container host will begin provisioning, and soon be running and ready for containers.

---

**Note:** Existing containers will be inventoried after the Hosts is successfully added.

### 3.4 Network

#### 3.4.1 Networks

*Infrastructure -> Network -> Networks*

**Overview**

The Networks section is for configuring networks across all clouds in Morpheus. Existing networks from the 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. Networks can also be set as inactive and unavailable for provisioning use.

**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

### 3.4.2 Services

#### Overview

The Network Services 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

3.4. Network
• phpIPAM

DNS
• Microsoft DNS
• Power DNS
• Route 53

Service Registry
• Consul

Security
• Cisco ACI

Add a Service

To configure any of the services, select *ADD SERVICE*, and fill out the required fields.

Infoblox
• Name
• URL (wapi url + version)
  – example https://x.x.x.x/wapi/v2.2.1
• Username
• Password

Bluecat
• Name
• URL
• Username
• Password

Microsoft DNS
• Name
• DNS Server
• Username
• Password
• Zone

PowerDNS
• Name
• API Host
• Token

Route 53
• Region
• Access Key
• Secret Key

After Saving, your Network Service integrations will be available for use. These integrations must be scoped to the appropriate sections in Morpheus:

**Scoping Services**

**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.

**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.

### 3.4.3 IP Pools

*Infrastructure -> Network -> IP Pools*

**Overview**

The Networks IP Pools sections allows you to create Morpheus IP Pools, which is an IP Range Morpheus can use to assign available static IP addresses to instances. The IP Pool section also displays pools from IPAM integrations like Infoblox and Bluecat.

**To add a Morpheus Network Pool**

1. Select + ADD in the Infrastructure -> Network -> IP Pools section
2. Enter the following:
   - **Name**  Name of the IP Pool in Morpheus. The name is presented when selecting an IP Pool for a Network, so use a name that easily identifies the IP Pool.
   - **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 to the right of the first 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.

### 3.4.4 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 Windows Instances to Domains, and creating A Records with DNS Integrations. The Domains section is also a multi-tenant endpoint for managing domain settings across multiple accounts

- Added and synced 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 Provisioning -> Virtual Images 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** Example demo.example.com
   - **Description** Descriptive meta-data for use in Morpheus
   - **Public Zone** Check for Public Zones, leave uncheck for Private Zones.
   - **Join Domain Controller** Enable to have Windows instances join a Domain Controller
   - **Username** Admin user for Domain Controller
   - **Password** Password for DC Username
   - **DC Server** (optional) Specify the URL or Path of the DC Server
   - **OU Path** (optional) Enter the OU Path for the connection string.
   - **Permissions** Configure Tenant permissions in Morpheus for the Domain (only applicable in Multi-tenant Morpheus setups)
   - **Tenant** Select the Tenant to set permissions to for the Domain.
   - **Visibility**
     - Private: Only Accessible by the select Tenant
     - Public: Available for use by all Tenants.
4. Save Changes

The Domain has been added and will be selectable in Domain dropdown during provisioning, and in Cloud and Network settings.

**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.
Editing and Removing Domains

- Domains can be edited by selecting the Actions dropdown for the Domain and selecting Edit.
- Added Domains can be removed from Morpheus by selecting the Actions dropdown for the Domain and selecting Remove.

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.

3.4.5 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 Admin -> 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 hosts 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.

3.4.6 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 -> 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 cloud to add an ACL.
3. Click the Security Groups tab.
4. Click the *Edit Security Groups* button.
5. Click the + (Add) button next to the Security Group(s) in the Available Security Groups list to add to Added Security groups list.
6. Save Changes

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

3.5 Load Balancers

*Infrastructure -> Load Balancers*

3.5.1 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.

Note:  HaProxy VM Load Balancer option, Load Balancer detail pages, Balance Mode, Sticky Mode and Shared VIP address option are available in Morpheus 2.11.3+.

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.
3.5.2 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

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.

### 3.5.3 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

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 Provisioning -> 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.

### 3.6 F5 Load Balancers

#### 3.6.1 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

**F5 Details Page**

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 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 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.

3.7 Storage

Note: In v3.5.2 STORAGE PROVIDERS has been split out into BUCKETS and FILE SHARES sections.

3.7.1 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/`. It 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.

3.7.2 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
- 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.

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 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 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.

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.

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.

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.
     **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.

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 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.

### 3.7.3 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 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.

---

**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.
  - **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 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 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.

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.

**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.
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.

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**
       - **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**
       - **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.

### 3.7.4 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
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

### 3.7.5 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.

3.8 Key Pairs & Certificates

3.8.1 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.

To navigate to the Key Pairs section:
1. Select the Infrastructure link in the navigation bar.
2. Select the Key Pairs link in the sub navigation bar.

3.8.2 Add Key Pair

To Add Key Pair:
1. Select the Infrastructure link in the navigation bar.
2. Select the Key Pairs link in the sub navigation bar.
3. Click the Add Key Pair button.
4. From the Add Key Pair Wizard input the following:
   - Name
   - Public Key
   - Private Key

Note: Certain features do not require storage of the private key.

3.8.3 Delete Key Pair

To Delete Key Pair:
1. Select the Infrastructure link in the navigation bar.
2. Select the Key Pairs link in the sub navigation bar.
3. Click the Delete icon on the row of the Key Pair to delete.

3.9 PXE Boot

3.9.1 Overview

Morpheus includes a built in PXE Server to enable easy and rapid bare metal provisioning.
3.9.2 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`.

3.9.3 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.

**3.9.4 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 Version**: Version 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.

**3.9.5 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.
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.

4.1 Tenants

4.1.1 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 besides the Master Tenants are Sub Tenants.

- The Master Tenant is the default Tenant created during the installation of Morpheus.
- All Tenants created after installation are Sub Tenants. Only one Master Tenant can exist.
- The Master Tenant creates and controls all Sub Tenants.
- Tenants are isolated environments.
  - Tenants have unique users
  - Tenants have unique workloads
- The Master Tenant can share or assign Master Tenants resources with/to Sub Tenants
- Sub Tenants cannot share their resources with other tenants
- Sub Tenants cannot see resources from other Sub Tenants
- Sub Tenants can only access Master Tenant resources that have been set to Public visibility or assigned to the Sub Tenant.
Roles

It is important to understand Role types and permission when creating and managing Tenants.

Tenant Roles

Tenant Roles are for capping Sub Tenant permissions by setting the maximum permissions for a Tenant. User Roles in a Tenant cannot exceed the permissions of the Tenant Role assigned to the Tenant.

- Tenant Roles set the maximum permissions for a Tenant
- User Roles in a Tenant cannot exceed the permissions of the Tenant Role assigned to the Tenant.
- Tenants Roles can be set on one or multiple tenants

- **Tenant Roles determine Public Cloud access for the tenant.**
  - All Clouds in the Master Tenants the have Visibility set to Public will show as options in the Tenant Role Cloud Access.
  - Only Master Tenant Clouds given access in a Tenants assigned Tenants role will be accessible in the Sub Tenant.

  IMPORTANT: Tenant Roles cap permissions on all Sub Tenant user roles. Sub Tenant user roles can be created in the sub Tenant will lesser permissions than the Tenant Role allows.

Tenants Roles are designed for a Master Tenant Admin to set max permissions for a Tenant, and a Sub Tenant Admin to configure User Roles inside the Sub Tenant.

User Roles

User Roles determine Feature, Group and Instance Type access for all Users. For multi-tenancy, there are two types of User Roles:

- **Single Tenant User Roles** Single Tenant User Roles only exist in the Tenant they exist in. All Roles created in a Sub Tenant are Single Tenant User Roles.

- **Multi Tenant User Roles** The Master Tenant and only the Master Tenant can create Multi Tenant User Roles. These Roles are for automating the creation of base User Roles in Sub Tenants.

  - Multi Tenant User Roles will automatically create matching User Roles in all Tenants

**Note:** Multi Tenant User Roles are intended to make Sub Tenant User Role creation easier, so Master Tenant users do not have to re-created the same base Sub Tenant Users Roles for every Sub Tenant. Multi Tenant User Roles are not a single role across Tenants, but more of a template that creates new Sub Tenant User Roles that can then be managed in the Sub Tenant.

  - Multi Tenant User Role changes will propagate to all Sub Tenants unless edited by a Sub Tenant
  - Once a Multi Tenant User Role is edited inside a Sub Tenant, it is no longer connected to the Multi Tenant User Role and is its own unique Role.
  - At least one Multi Tenant User Role is required before any Sub Tenants can be created

**Important:** Deleting a Multi Tenant User Role from the Master tenant will not remove that Role from Sub Tenants.
4.1.2 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, Delete, 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)
   - Base Role Primary role of the Tenant. All User roles within the Tenant cannot exceed the permission of this Role.
   - Limits Restricts the amount of Storage and Memory allocated to the Tenant
5. Click the Save Changes button.

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

**4.1.3 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 create prior to adding sub-tenant users or the user will not save. In previous versions a default multi-tenant role was seeded, but due to customer requests the seeded role was removed and a multi-tenant role must be created by the master tenant for sub-tenant 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 the Create User button.
5. From the New User wizard input the fields below
   
   - First Name of the user being created
   - Last Name of the user being created
   - Username used to login
   - Email address of the new user
   - Role to be inherited by the user
   - Password
   - Limits
     - Restricts the amount of Storage and Memory the user can provision.
   - Save Changes.
**Important:** In versions 3.1.1 and 2.12.5 and later, a multi-tenant user role must be create prior to adding sub-tenant users or the user will not save. In previous versions a default multi-tenant role was seeded, but due to customer requests the seeded role was removed and a multi-tenant role must be created by the master tenant for sub-tenant 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 Tenant Name on the row of the Tenant containing the user to be edited.
4. Click the Edit pencil icon of the row of the to edit.
5. Edit User information

*Note:* Name, Username, Passwords and e-mail addresses cannot be edited on Users created from Identity Source Integrations.

6. 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 on the row of the Tenant containing the user.
4. Click the Delete trashcan icon of the row of the user to delete.
5. Confirm

**Subtenant User Login**

Subusers can have the same username as the user on the master tenant or any other tenant. Subusers 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`
4.1.4 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, and the Created Date. Click the Tenant Name to drill into the Tenant View where you can again Edit, Delete, as well as Create Users, Edit Users, and Delete Users 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 * Description(optional) * Base Role- Primary role of the Tenant. All roles created within the Tenant must inherit this role as the base role. * Currency (for pricing) * Limits- These restrict the amount of Storage, Memory, and CPUs that can be collectively provisioned by all users in the Tenant. The default is 0 for these limits, which means no limits will be applied.
5. Click the Save Changes button.
Viewing Tenants

To View an individual Tenant page, select the Tenant name from the main Tenants section.
From inside this Tenant view, the Tenant settings can be edited, existing users can be viewed or edited, and new users for this Tenant can be created.

**Tenant Users**

To create a new user for a Tenant (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.)

1. Click the **CREATE USER** button. From the New User wizard input the fields below.
   - * First Name of the user being created
   - * Last Name of the user being created
   - * Username used to login
   - * Email address of the new user
   - * Role to be inherited by the user
   - * Password
   - Storage, Memory and CPU limits for this specific user, if any (0 is no limit)
2. Click **Save Changes**.

**Impersonate Tenant User**

“Impersonate User” enables administrators to login as sub-Tenant users directly from the master Tenant.

To impersonate a user, you must be logged in as a user with the “Impersonate User” feature enabled in assigned role.

Navigate to Tenants, select an Tenant, and in the specific user 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 top right, 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 (master Tenant only): Available across all Tenants

Resources in the Master Tenant can also be assigned directly to sub-Tenants. When a resource is assigned to a sub-Tenant, it is only available for that sub-Tenant, and its visibility is automatically set to private. Public Visibility is not an option for any resource assigned to or created in a sub-Tenant.

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
Cloud Visibility & Assignment

Edit Visibility of a Cloud

To set the Visibility of 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 far right of the cloud row, or click the name of the cloud and select “Edit” in the top right of the cloud page.
3. From the “Visibility” drop down, select either “Public” or “Private”
4. Select Save Changes in the lower right of the Edit Cloud modal.
When a cloud is set to Public visibility, it is available to be added to sub Tenants. All sub-Tenants 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 sub Tenant(s).

For Tenants created prior to a Master Tenant cloud being set to public visibility, the sub Tenant will have the option to add that cloud but it will not automatically be added.

While the cloud will be available for Sub-Tenants, the resources available in that cloud to the sub-Tenant(s) depends on the visibility or assignment of the individual resources.

**Note:** A sub-Tenant user must have sufficient role permissions/cloud access to add publicly available clouds. Master Tenant clouds settings cannot be edited from sub Tenants.

---

**Assign a Cloud to an Tenant**

**Important:** When assigning a Cloud to an 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 far right of the cloud row, or click the name of the cloud and select “Edit” in the top right of 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 lower right 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 a 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 top right of the resource page to bring up the config modal.
5. From the “Visibility” drop down, select either “Public” or “Private”

6. Select **Save Changes** in the lower right of the modal

---

Assigning a Host, Virtual Machine, or Bare Metal server to a 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 top right of 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 lower right of 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 on the far right of the network row, or click the name of the network and select “Edit” in the top right of the network page.
3. From the “Visibility” drop down, select either “Public” or “Private”
4. Select Save Changes in the lower right of the modal
Assignable Network to an Tenant

1. From the Master Tenant, navigate to Infrastructure, Network
2. Select either the pencil/edit icon on the far right of the network row, or click the name of the network and select “Edit” in the top right of the network page.
3. From the “Tenant” drop down, select an Tenant to assign the network to.
4. Select Save Changes in the lower right of 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 on the far right of 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 lower right of 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 on the far right of 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 lower right of the modal
The Virtual Image will now be available for use by the assigned Tenants.

4.2 Identity Sources

Administration -> Tenants -> Select Tenant -> Identity Sources

4.2.1 Overview

There are several built in single sign-on integrations included with Morpheus. These can be configured via the Identity Sources button in Admin -> Accounts. These integrations include linking capabilities with LDAP, Active Directory, Okta, and Jump Cloud. One can even map these sign on tools to equivalent roles in Morpheus so at first log in users are assigned the appropriate role.

4.2.2 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.

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.
7. 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.

### 4.2.3 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

4.2. Identity Sources
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.

6. 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.

4.3 Plans & Pricing

4.3.1 Overview

The Plans & Pricing page displays a list of all of your available service plans. From the service plans page you will be able to Create, Edit, and Delete service plans, as well as review basic plan details. The list of plans displayed on this page displays planName, Description, Instances Layout, Memory, Storage, and Cost, as well as an action column to edit and delete. A default set of Service Plans are created in Morpheus. 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.

4.3.2 Service Plans

Create Service Plan

To create service plan
1. Select the Administration link in the navigation bar.
2. Select the Plans & Pricing link in the sub navigation bar.
3. Click the Create Service Plan button.
4. From the New Service Plan wizard, input:
   - Name
   - Code used as a unique identifier in the API and CLI.
   - Storage size in megabytes.
   - Memory size in megabytes.
   - Cost is internal cost of plan.
   - Price is what the service offering will be priced at.
   - Instance Types that will be associated with this plan.
   - Click the Save Changes button to save.

**Edit Service Plan**

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. These all can be easily managed from the Admin -> Service Plans section.

To edit service plan:
1. Select the Administration link in the navigation bar.
2. Select the Plans & Pricing link in the sub navigation bar.
3. Click the Edit pencil icon on the row of the plan to edit.
4. Edit the following Edit Service Plan.
5. Click the Save Changes button to save.

**Delete Service Plan**

To delete service plan
1. Select the Administration link in the navigation bar.
2. Select the Plans & Pricing link in the sub navigation bar.
3. Click the Delete trashcan icon on the row of the plan to delete.
4. Confirm

**4.3.3 Pricing**

**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.

Note: Month is equivalent to 30 days by default. For AWS, month is 30.5 days. For Azure, month is 30.4 days.

Types
Price Set Types determine what prices the Set is composed of.

Note: Make note of the Price set options below before creating Prices.

Everything ‘Everything’ price sets require 1 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.

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.

Price Types

• Everything
  – One price for all resources Memory, CPU, RAM, and Disks

• Memory + CPU

• Memory Only

• Cores Only

• Disk Only

• Platform

• Software
Price Units

- Minute
- Hour
- Day
- Month
- Year
- Two Year
- Three Year
- Four Year
- Five Year

Currency

- AUD
- CHF
- DKK
- EUR
- GBP
- IDR
- ILS
- MAD
- NOK
- NZD
- ROL
- SEK
- TRL
- USD
- 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 + (Cost x Markup %)

Custom Price  Sets a Price independent from the Cost. If the Cost changes, a Custom Price will not.

4.4 Roles

4.4.1 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 users feature access level to be respected.

4.4.2 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.

4.4.3 Roles and Identity Sources

It is very common for large enterprises to have an existing identity source that they would like to plugin 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 found in Admin -> Tenants, and has to be configured on a per tenant basis.

4.4.4 Resource Limits

While it is possible to restrict usages by roles assigned to a tenant or role with max memory utilizations and max storage utilizations, it is preferred to now control this at the Policy level within a group or cloud. Morpheus provides a large swatch of policy types that can be assigned globally or to specific tenants both globally, and per cloud/group entity.

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.

FEATURE ACCESS Controls Tenant and User access level for sections and features in Morpheus.

GROUP ACCESS Controls User access level for Groups. (Groups are not Multi-Tenant.)

CLOUD ACCESS Controls Sub-Tenant access level for Master Tenant publicly visible Clouds.

INSTANCE TYPE ACCESS Controls Tenant and User access level for Instance Types.
Feature Access Permissions

Feature Access settings control permissions for sections and features in Morpheus. Permission options include:

- **None**  Hidden or inaccessible for user
- **Read**  User can access the section, but cannot edit or create
- **Full**  User has full access
- **User**  User only has access to data from the Instances they have created/own.

**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.

- Admin: Appliance Settings (None, Full)
- Admin: Backup Settings (None, Full)
- Admin: Environment Settings (None, Full)
- Admin: Identity Source (None, Full)
- Admin: Integrations (None, Read, Full)
- Admin: License Settings (None, Full)
- Admin: Log Settings (None, Full)
- Admin: Monitoring Settings (None, Full)
- Admin: Provisioning Settings (None, Full)
- Admin: Roles (None, Read, Full)
- Admin: Service Plans (None, Read, Full)
- Admin: Tenant (None, Full)
- Admin: Tenant - Impersonate Users (None, Full)
- Admin: Users (None, Read, Full)
- Admin: Whitelabel Settings (None, Full)
- Administration: Manage Policies (None, Read, Full)
- Backups (None, View, Read, User, Full)
- Billing (None, Read, Full)
- Infrastructure: Boot (None, Read, Full)
- Infrastructure: Certificates (None, Read, Full)
- Infrastructure: Clouds (None, Read, Full)
- Infrastructure: Groups (None, Read, Full)
- Infrastructure: Hosts (None, Read, Full)
- Infrastructure: KeyPairs (None, Read, Full)
- Infrastructure: Load Balancers (None, Read, Full)
- Infrastructure: Networks (None, Read, Full)
- Infrastructure: Security Groups (None, Read, Full)
4.4.5 Adding Roles

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 Mater Account.
To create a Tenant Role:

1. In the Master Account, navigate to Administration -> Roles
2. Select the + CREATE ROLE button
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. Optionally set Limits for Storage, Memory or CPU Count. These limits will apply for any Tenant the Role is assigned to. 0.0 is default and is equal to no limit.

After saving the Role will be created, and you will be redirected to that Roles Permissions settings.

User Roles

User Roles can be single or multi-tenant. Multi-tenant User Roles will automatically be copied to all current and future Tenants.

Important: Multi-tenant User Roles are copied to Tenants, but each copied Role becomes its own unique role per tenant and needs to be edited in the Tenant. Changes to a Multi-Tenant User Role at the Master Tenant level will not change existing user roles in Tenants created from the Multi-Tenant Role due to unique Role permissions in each Tenant, such as changes from the overriding Tenant Role and unique Group and Instance Type permissions.

Create a Single Tenant User Role

1. In the Master Account, navigate to Administration -> Roles
2. Select the + CREATE ROLE button
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. Optionally set Limits for Storage, Memory or CPU Count. These limits will apply for any User the Role is assigned to. 0.0 is default and is equal to no limit.

After saving the Role will be created, and you will be redirected to the Roles Permissions settings.

Create a Multi Tenant Role

1. In the Master Account, navigate to Administration -> Roles
2. Select the + CREATE ROLE button
3. Enter a name for the Role and optional Description
4. For TYPE, select “User Role”

5. Select the “Multi-tenant Role” checkbox.

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. Optionally set Limits for Storage, Memory or CPU Count. These limits will apply for any User the Role is assigned to. 0.0 is default and is equal to no limit.

After saving the Role will be created, and you will be redirected to that Roles Permissions settings.

---

**Important:** While a Multi-tenant role is automatically copied into all existing subtenants as well as placed into any new Tenants, the generated roles inside each Tenant should be treated and managed as their own role. The Group Access configuration of a multi-tenant role only applies to the Tenant the role is being edited in, as Groups are unique to each tenant and not shared across Tenants. The purpose of a multi-tenant role is to facilitate an easy method of generating multiple pre-defined user roles for Tenants, NOT manage Tenant User Roles from the master tenant. When editing the permissions for a sub-tenant user, be sure to edit their user role(s) from inside the sub-tenant, not from the Master account, by impersonating a sub-tenant admin with full Role permissions.

---

**4.5 Users & User Groups**

**4.5.1 Users**

**Overview**

The Users page displays a list of all users. From the users page: Create, Edit, and Delete users. The list of users displayed on this page displays Account, Name, Username, Email, and Role.

**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.

---

**Create User**

Users can be created from Administration -> Users or Administration -> Tenants -> Select a 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:

   **User Name & 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.

**Limits** Combined Instance Resource Limits for the User. When a limit is reached, the User will not be able to provision more Instances

- **STORAGE**
  - Total amount of Storage the user can Provision, set in GiB. 0.0 is unlimited.

- **MEMORY**
  - Total amount of RAM the user can Provision, set in MiB. 0.0 is unlimited.

- **CPU COUNT**
  - Total combined Cores the user can Provision. 0 is unlimited.

4. 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 very top right of the browser window.
2. Select User Settings

To edit the User you are currently logged in as from User Settings:
1. Select your name in the very top right of the window
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 very top right of the window.
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

### 4.5.2 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.
   - **SUDDO 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).

4.6 Integrations

Administration -> Integrations

To add an integration select + ADD and choose your integration. For more information on each integration, please see the Integration Guides.

4.7 Policies

4.7.1 Overview

Policies add governance, ease of use, cost-savings, and auditing features to Morpheus. Morpheus enables end users to create user, group, cloud, and global policies to give users full control and governance over their environments! Policies can apply towards any instance provisioned by a specific user, globally or into a group or cloud with active policies. Policy generation is a role permission.

4.7.2 Creating Policies

Policies can be created in three different locations.
   • Administration -> Policies
   • Infrastructure -> Groups -> Group -> Policies
   • Infrastructure -> Clouds -> Cloud -> Policies

Policies can be edited and set to active or inactive.

**Important:** Cloud policies will override matching or conflicting group policies during provisioning.
Available Policy Types

**Backup Creation**  Disable or enable the ability to create a backup when provisioning an instance.

**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.

**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.

**Host Name**  Pre-populates a fixed or editable name for Hosts and Virtual Machines using ${variable} naming patterns and/or text.

**Hostname**  Pre-populates a fixed or editable name for hostnames/machine names using ${variable} naming patterns and/or text.

**Instance Name**  Pre-populates a fixed or editable name for Instance Names using ${variable} naming patterns and/or text.

**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.

**Power Scheduling**  Adds a Power Schedule for the Instances in a Group or Cloud. Power Schedules can be created in Operations -> Scheduling

**Provision Approval**  Sets an Approval requirement for Provisioning into a Group or Cloud using Morpheus Approvals or an Approval Integration such a Service Now.

**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.

**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.

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 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 -> 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 Types sections below for Configuration options.
6. Select SAVE CHANGES

4.7.3 Policy Types

Expiration Policies

Expiration policies set an expiration timeframe for any instance provisioned into the cloud or group 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?.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 moved into a Group with an Active Policy or Instances created when converting an unmanaged 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 `${variable}` string interpolation.

Commonly used variables for naming patterns include:

```
${groupName}
${groupCode}
${cloudName}
${cloudCode}
$type
$accountId
$account
$accountType
$platform
$userId
$userName
$userInitials
$provisionType
$sequence  #results in 1
$sequence+100  #results in 101
$sequence.toString().padLeft(5,'0')  #results in 00001
```

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. Cloud codes and Group codes are fields found in their respective configuration panes.

**Note:** Static text can also be used in conjunction with ${variable}'s, such as morpheus${cloudCode}${type}${sequence+3000}

**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**

- **User Configurable** Shutdown timeframe is editable during provisioning.
- **Fixed Expiration** User cannot change shutdown timeframe during provisioning.

**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.

**Note:** Expiration and Shutdown Policies will be enforced on Instances moved into a Group with an Active Policy or Instances created when converting an unmanaged host to managed.

**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 Operations -> 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 Operations -> 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 and Groups for maximum amount of Memory, Storage, Cores, Hosts, VM’s, or Containers that can be created in the Cloud or Group the Policy is assigned to.

Configuration options for Max Resources Policies:

- **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.
- **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 do 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.
4.8 Provisioning Settings

Administration -> Provisioning

Settings  Configure Global Provisioning, Cloud-init and PXE Boot settings.
Environments  Create and manage Environment Tags
Licenses  Add License to apply to Windows Instances during Provisioning.

4.8.1 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.
Show Pricing  Displays or hides Pricing in Provisioning wizard and Instance and Host detail pages.
Deployment Archive Store  Default Storage Provider for storing Deployment Archives.

Note:  Storage Providers can be configured and managed in the Infrastructure -> Storage section.

4.8.2 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 -> Key Pairs section.

Windows

•  *Administrator Password*: Enter password to be set for the Windows Administrator User during provisioning.

4.8.3 PXE Boot Settings

Default Root Password  Enter the default password to be set for Root during PXE Boots.

Environments

Administration -> Provisioning -> Environments
4.8.4 Overview

The Environments section is where you create and manage Environment Tags, which are available in the Environment dropdown during Provisioning to attach to Instances. An instances Environment Tag can be changed by editing the instance.

4.8.5 Creating Environments

1. Select + Create Environment
2. Populate the following for the New Environment:
   - **Name** Name of the Environment
   - **Code** Shortcode used for API and CLI
   - **Description** Environment description displayed in Environments list page.
   - **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: Existing Environments can be edited or removed using the Actions dropdown in the Environments list.

4.8.6 Overview

The License section is for automating the application of Licensee 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.

4.8.7 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** License Version
   - **Copies** The Number of copies available on the License
   - **Description** License description displayed in the Licenses list in Morpheus. Helpful for identifying 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 *Provisioning -> 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

### 4.8.8 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.

### 4.8.9 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.

### 4.9 Monitoring Settings

#### 4.9.1 Overview

The Administration -> Monitoring section is for configuring Morpheus Monitoring and Monitoring Integrations.

#### 4.9.2 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.

### 4.9.3 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.

### 4.9.4 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>
4.9.5 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.

4.10 Backup Settings

Administration -> Backups

4.10.1 Overview

The Backups Settings page allows you enable or disable Scheduled Backups, and select a Default Backup Storage Provider. Backups within Morpheus can always be run manually. However the scheduled backups toggle must be enabled to run jobs automatically. Configure the default storage provider to select the target location for all new backups. (This does not affect existing backups.)

4.10.2 Morpheus Backup Settings

Options:

**Scheduled Backups** Enable automatic scheduled backups for provisioned instances.

**Create Backups** When enabled, Morpheus will automatically configure instances for manual or scheduled backups.

**Copy Snapshots to Store** Copy VMware snapshots to selected Backup Storage Provider

**Default Backups Storage Provider** Default Backups Storage Provider

**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 Provider** Enable/Disable Morpheus as the default backup provider.

**Default Backup Storage Provider** Storage Providers can be configured and managed in the infrastructure Storage section.

**Backup Retention Count** Default maximum number of successful backups to retain.

4.10.3 Veeam Settings

**Enabled** Enable the Veeam integration

**Default Backup Provider** Sets Veeam as the Default Backup Provider in Morpheus. Backup Providers can also be configured per Backup.

**Visibility** Sets visibility in multi-tenant Morpheus environments:
• Public: Accessible by all Tenants
• Private: Accessible only to the Tenant the Veeam integration is added.

**Host** Host name or the IP address of the Veeam Backup Enterprise Manager. This is the same host that you use to access the Veeam Backup Enterprise Manager browser-based user interface.

**Port** The HTTP(S) port of the Veeam Backup Enterprise Manager API. The default is 9399.

**Username** The username used to authenticate with the Veeam Backup Enterprise Manager.

**Password** The password used to authenticate with the Veeam Backup Enterprise Manager.

**Backup Repositories** Once credentials are authenticated, search will populate available Veeam Repositories to select from.

**Backup Job Templates** The backup jobs configured in the Veeam Backup and Replication Console that can be cloned when creating new backup jobs.

**Refresh Available Jobs** Use to sync newly created Jobs in Veeam.

---

**Important:** Once a Veeam Integration has been enabled, a **VEEAM SERVER** setting will be available in VMware and Hyper-V cloud settings (Infrastructure -> Clouds -> Edit a Cloud). To enabled backups on a Cloud, a Veeam Server must be selected in the **VEEAM SERVER** dropdown in the Cloud settings and saved. Failure to do so will result in blank **Backup Repositories** and **Backup Job Templates** options when configuring Veeam Backups during provisioning.”

---

### 4.10.4 Commvault Settings

**Enabled** Enable the Commvault integration

**Default Backup Provider** Sets Commvault as the Default Backup Provider in Morpheus. Backup Providers can be configured per Instance backup settings.

**Host** IP or Hostname of the Commvault server.

**Port** Port configured to access the Commvault server

**Commvault server Username** Admin Username for Commvault

**Password** Password for Username provided (encrypted in Morpheus)

---

### 4.11 Logging Settings

#### 4.11.1 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 VM’s 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 3.5.2+ in Operations - Health.

Logs are stored in ElasticSearch and retention can be set by adjusting the Availability Time Frame in the Administration -> Logs section.

Morpheus also has built in Integrations with 3rd Party solutions. When configured, the Morpheus agent will forward logs to the integrated platforms automatically.

Logging Settings for the build-in Logging, Syslog forwards, and 3rd Party Integrations are configurable in the Administration -> Logs section.

4.11.2 Morpheus Logging

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.

4.11.3 Splunk

To configure Splunk create a syslog listener configuration in Splunk. Then it is simply a matter of expanding the section in Logging settings pertaining to Splunk and filling out the host and port of the appender. Once saved, all hosts managed by Morpheus will be configured to forward logs to the target Splunk listener.

4.11.4 LogRhythm

Configuring LogRhythm is much like configuring Splunk. Simply toggle the enabled flag in the LogRhythm section to enabled and fill in the Host, and Port information for the LogRhythm listener.

4.12 Appliance Settings

The Administration -> Settings section sets global configuration parameters for the Appliance, Tenant Registration, Email, Proxy and sets which Cloud types are enabled.

4.12.1 Appliance Settings

Host Level Firewall Enabled Enables or Disables the host level firewall. This must be Enabled to use Morpheus Security Groups.

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.

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.

Email Settings

A default installation of Morpheus uses an online service called postmarkapp. Morpheus api requests to the postmarkapp service to send notification e-mails.

To add your own SMTP server you will need to go to the Administration and Settings of your Morpheus appliance. You will then need to provide Morpheus the following information, your mail server systems administrator should provide you with the below information and the preferred encryption method.

- From Address
- SMTP Server
- SMTP Port
- SSL Enabled
- TLS Encryption
- SMTP User
- SMTP Password

We recommend that you add your Morpheus server to your SMTP white list as well as using user authentication as an additional security measure.

Once you have added your SMTP server information into Morpheus scroll down the Administration and Settings page and press the blue save button which can be found under enabled clouds.

When you have saved your SMTP server settings in the Morpheus appliance you will then need to restart the Morpheus-ui. To restart the Morpheus-ui connection to your Morpheus server via ssh and run the below command.

```
sudo morpheus-ctl restart morpheus-ui
```

**Important:** If you do not restart the Morpheus-ui the notifications will be sent by the original notification service postmarkapp. Please note it can take up to 3 minutes for the ui to become reachable again. has a built in SMTP server for email notifications and alerts. An alternate SMTP server can be specified below:

Add an alternate SMTP Server:

- From Address
- SMTP Server
- SMTP Port
- SSL Enabled
- TLS Encryption
- SMTP User
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

Enabled Clouds

Cloud types can be Enabled or Disabled in this section. When a Cloud type is disabled, it will be removed from the available options when adding new clouds in the Infrastructure section.

Available Cloud types:

- Morpheus
- OpenStack
- Amazon
- Metacloud
- VMware vCenter
- VMware vCloud Air
- SoftLayer
- Google Cloud
- Azure (Public)
- Azure Stack (Private)
- DigitalOcean
- VirtualBox
- VMware Fusion
- VMWare ESXi
- Nutanix
- UCS
- XenServer
4.12.2 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. Preferred Image Size (500x76)

Disable Support Menu  Enable this flag to hide the support dropdown menu in the header.

Footer Logo  Footer Logo in bottom left. Preferred Image Size (264x54)

Login Logo  Logo shown on Login screen. Preferred Image Size (228x280)

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
Override CSS

Override CSS settings by entering CSS in Override CSS field.

Example: (this will add one continues background image to the Header)

```css
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 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.

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.

```lua
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 * 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'
```

(continues on next page)
4.12.3 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.

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](https://morpheushub.com), or by contacting support@ or sales@ morpheusdata.com.

4.12.4 Advanced morpheus.rb Settings

Overview

Morpheus allows for additional advanced customizations to the morpheus.rb file located in `/etc/morpheus/morpheus.rb`. Below is a list of the supported items available in the morpheus.rb file.
ui['vm_images_cdn_url'] = 'https://morpheus-images.morpheusdata.com'
ui['kerberos_config'] = nil
ui['kerberos_login_config'] = nil
ui['max_memory_mb'] = nil
ui['memory_map_threshold'] = 131072
ui['memory_trim_threshold'] = 131072
ui['memory_top_pad'] = 131072
ui['memory_map_max'] = 65536
ui['memory_alloc_arena_max'] = 2
ui['http_client_connect_timeout'] = 10000
ui['http_client_connect_timeout'] = 600000

mysql['enable'] = true
mysql['morpheus_db'] = 'morpheus'
mysql['morpheus_db_user'] = 'morpheus'
mysql['max_active'] = 100
mysql['host'] = '127.0.0.1'
mysql['port'] = 3306
mysql['tmp_dir'] = '/tmp/mysql'

logging['svlogd_size'] = 209715200 # 200 MB in bytes
logging['svlogd_num'] = 30 # keep 30 rotated log files
logging['svlogd_timeout'] = 86400 # rotate after 24 hours in seconds

rabbitmq['enable'] = true
rabbitmq['vhost'] = 'morpheus'
rabbitmq['queue_user'] = 'queue_user'
rabbitmq['host'] = '127.0.0.1'
rabbitmq['port'] = '5672'
rabbitmq['nodename'] = 'rabbit@localhost'
rabbitmq['stomp_port'] = 61613
rabbitmq['heartbeat'] = nil

elasticsearch['enable'] = true
elasticsearch['host'] = "127.0.0.1"
elasticsearch['es_hosts'] = {'127.0.0.1' => 9200}
elasticsearch['open_files'] = 204800
elasticsearch['memory_map_threshold'] = 131072
elasticsearch['memory_trim_threshold'] = 131072
elasticsearch['memory_top_pad'] = 131072
elasticsearch['memory_map_max'] = 65536
elasticsearch['memory_alloc_arena_max'] = 2
elasticsearch['replica_count'] = 1

nginx['enable'] = true
nginx['workers'] = integer calculated from number of cpus
nginx['worker_connections'] = 10240
nginx['cache_max_size'] = '5000m'
nginx['ssl_country_name'] = "US"
nginx['ssl_state_name'] = "CA"
nginx['ssl_locality_name'] = "San Mateo"
nginx['ssl_company_name'] = "Morpheus, LLC"
nginx['ssl_organizational_unit_name'] = "DevOps"
nginx['ssl_email_address'] = "personal@email.com"
nginx['ssl_ciphers'] = "ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:

4.12. Appliance Settings 213
nginx['ssl_protocols'] = "TLSv1 TLSv1.1 TLSv1.2"
nginx['ssl_session_cache'] = "builtin:1000 shared:SSL:10m"
nginx['ssl_session_timeout'] = "5m"
nginx['loading_pages']['max_loops'] = 60 # seconds
nginx['loading_pages']['timeout_page'] = '/timeout.html'
nginx['loading_pages']['iteration_time'] = 10000 # milliseconds
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.'
repo['repo_host_url'] = 'https://downloads.morpheusdata.com'
5.1 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.

5.1.1 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 reattempt 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](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>
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

5.1.2 Groups & Apps

One great feature of the monitoring system is the ability to organize checks by groups and apps. This provides a nice convenient way to determine what a customer facing impact might be for a single failure as well as representing redundancy via groupings.

It is important to note the relationship of apps, groups, and even checks with regards to instances provisioned within Morpheus. For every Instance that is provisioned: A monitoring Group is created and a Check is added to that group for every Container or Virtual Machine within that Instance. This makes sense such that as an Instance is scaled out horizontally (containers/vms added to it) The monitoring system accurately represents the layers of redundancy. An App simply maps to a Provisioning App and should be pretty straightforward to understand.

Groups

It is also possible to organize custom checks in this hierarchical structure by manually adding or editing a Group or App. Groups 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.

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 checks Max Severity setting.

Affects Availability Whether or not a failed group impacts system wide availability calculations.

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.

Apps

Apps are very useful for seeing an aggregation of failures, or impact based on a set of checks and groups. Apps typically correlate to apps created in provisioning 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. There are a few useful options as well with regards to Apps:

Max Severity The maximum severity incident a failed app may create. This setting overrides check and group Max Severity settings.

Affects Availability Whether or not a failed app impacts system wide availability calculations.
5.1.3 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.

5.1.4 Alerts

There are several ways to configure alerts and notifications within Morpheus. Users can be notified via Email or SMS as well as several other direct integrations. These integrations include PagerDuty, Alert Ops, Victor Ops, and even Slack chat Channel notifications (or optionally via the ServiceNow integration).

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 https://slack.com/[[]]Slack] channel.
- **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.

Alert Rules

Alert Rules provide a powerful means to configure who gets notified in various scenarios. These scenarios include targetting 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.
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.

Notifications

Configuring Notification Services

By default Morpheus provides email notification services using the morpheusdata.com email address. It may be advisable to customize these services to use another mail delivery service.

5.1.5 Monitoring Integrations

While Morpheus provides a fantastic means for determining uptime and availability of both services and VMs sometimes more is needed. A good example of this is performance application monitoring. To solve this several external integrations are provided out of the box. Even some external integrations with regards to incident management are provided.

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 AppDyanmics there are more required settings to integrate it with Morpheus. To get started expand the section in Admin -> Monitoring related to AppDynamics and toggle it to Enabled. There are several fields here that need filled out. Once completed hit save and all hosts will automatically be configured to install the AppDynamics agent.

AppDynamics is capable of begin 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.

NewRelic

New Relic is a very popular service based performance monitoring tool. It supports a wide variety of application platforms and is a breeze to configure with Morpheus. Another great feature of new relic is its ability to monitor the server applications run on and provide additional stats. To do this an agent needs to be installed and configured on each server. Fortunately, this is performed automatically for every vm and docker host provisioned within Morpheus. To turn on the integration simply go to Admin -> Monitoring and expand the section titled “New Relic”. There it is simply a matter of toggling the Enabled setting to on and entering the New Relic account API Key.

Service Now

Service now integration is provided out of the box with Morpheus. To add a service now integration simply visit the ‘Monitoring Settings’ section in Admin -> Monitoring. This allows one to map incident severity levels to equivalent severities in ServiceNow.

To enable service now simply expand the section labelled “ServiceNow” in Admin -> Monitoring. Toggle the enabled flag and enter the Host, User, and Password information required to connect to ServiceNow. The other options below include behaviors upon new incidents being opened and old incidents closing. It also includes a table for mapping Morpheus incident severity levels to their ServiceNow counterparts.
6.1 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.

6.1.1 Configuration

Logging configuration can be setup in the Admin -> Logs section. There are a couple useful settings here including customizing the retainment policy (by default 7 days). This could be expanded to years for PCI Compliance purposes or other potential requirements an organization might have.

Note: When increasing the retainment 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.

This area of administration 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/ documentation.

6.1.2 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. Simple 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](https://lucene.apache.org/core/2_9_4/queryparsersyntax.html)

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.

### 6.2 Integrations

While the built in logging solution provided by Morpheus is sufficient for most, there are some scenarios in which a more advanced logging system may be desired or already in place. To facilitate this Morpheus makes it easy to add custom syslog rules as well as built in direct integrations with Splunk and LogRhythm. All integrations pertaining to logging can be configured in the Administration -> Logging section.

#### 6.2.1 Splunk

To configure Splunk simply create a syslog listener configuration in Splunk. Then it is simply a matter of expanding the section in Logging settings pertaining to Splunk and filling out the host and port of the appender. Once saved, all hosts managed by Morpheus will be configured to forward logs to the target Splunk listener.

#### 6.2.2 LogRhythm

Configuring LogRhythm is much like configuring Splunk. Simply toggle the enabled flag in the LogRhythm section to enabled and fill in the Host, and Port information for the LogRhythm listener.

### 6.3 Exporting Logs

#### 6.3.1 Log Settings

There are three main log areas in Morpheus
- Agent Logs
- Morpheus Server Logs
- Activity / Audit Logs
6.4 Agent Logs

When instances are deployed through Morpheus, the agent that is installed, captures Application logs and sends them back to the Morpheus Server.

While the built-in logging solution provided by Morpheus is sufficient for most, there are some scenarios in which a more advanced logging system may be desired or already in place. To facilitate this Morpheus makes it easy to add custom syslog rules as well as built in direct integrations with Splunk and LogRhythm. All integrations pertaining to logging can be configured in the Administration -> Logging section.

6.4.1 Splunk

To configure Splunk simply create a syslog listener configuration in Splunk. Then it is simply a matter of expanding the section in Logging settings pertaining to Splunk and filling out the host and port of the appender. Once saved, all hosts managed by Morpheus will be configured to forward logs to the target Splunk listener.

6.4.2 LogRhythm

Configuring LogRhythm is much like configuring Splunk. Simply toggle the enabled flag in the LogRhythm section to enabled and fill in the Host, and Port information for the LogRhythm listener.

6.5 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

   ```
   module(load="imfile" PollingInterval="50")
   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")
   input(type="imfile" File="/var/log/morpheus/guacd/current" Tag="guacd" ReadMode="2" Severity="info")
   input(type="imfile" File="/var/log/morpheus/elasticsearch/current" Tag="elasticsearch ReadMode="2")
   input(type="imfile" File="/var/log/morpheus/mysql/current" Tag="mysql" ReadMode="2" Severity="info")
   input(type="imfile" File="/var/log/morpheus/nginx/current" Tag="nginx" ReadMode="2" Severity="info")
   input(type="imfile" File="/var/log/morpheus/rabbitmq/current" Tag="rabbitmq" ReadMode="2" Severity="info")
   input(type="imfile" File="/var/log/morpheus/redis/current" Tag="redis" ReadMode="2" Severity="info")
   ```

2. Restart rsyslog
The logfiles will now be 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.

### 6.6 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:

   ```bash
   morpheus-ctl stop morpheus-ui
   ```

   **Note:** Please be aware this will restart 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)

   ```bash
   morpheus-ctl start morpheus-ui
   ```

5. To know when the UI is up and running you can run the following command

   ```bash
   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 logile, you could create an Appender definition for your SIEM audit database product.

### 6.7 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
}
```
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.

### 7.1 Initial Backups Setup

Global Backup settings, Storage Providers and Execution Schedules should be configured prior to creating backups.

#### 7.1.1 Global Backups Settings

Morpheus Backups can be enabled under *Administration -> Backups*.

- **Scheduled Backups** When enabled, configured Backups will automatically run on the set Schedule. If disabled, backups need to be manually ran.
- **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 *Operations -> Scheduling -> Execution Schedules*
- **Backup Retention Count** Default maximum number of successful backups to retain.
7.1.2 Backup Schedules

Backup Execution Schedules can be configured and managed in the Operations -> Scheduling -> Execution Schedules. The Default Backup Schedule set in Administration -> Backups will be selected when configuring Backups but other Schedules can be selected during configuration.

7.2 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
- Veeam Hyper-V VM Backup
• Google VM Snapshot
• Commvault File/Directory Backup
• Azure VM Snapshot
• Morpheus Appliance
• Openstack VM Snapshot
• DigitalOcean VM Snapshot
• Nutanix VM Snapshot
• Softlayer VM Snapshot
• Hyper-V VM Snapshot
• VMWare VM Snapshot
• SCVMM VM Snapshot
• UpCloud VM Snapshot
• Bluemix VM Snapshot
• Alibaba VM Snapshot
• Oracle Cloud VM Snapshot
• KVM VM Snapshot
• Container Backup
• VM Backup
• Object Storage Backup

7.3 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.

7.4 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.
7.4.1 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.

7.4.2 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.

7.4.3 Create Server Backup

To create a server backup:

1. Select the Backups link in the navigation bar.
2. Select the Backups link in the sub navigation bar.
3. Click Add Backup.
4. From the Create Backup Wizard select the radio button Server, then click Next.
5. Input the following:
   - Name of the backup job being created
   - Server
   - Type of backup you wish to create.
6. Click Next. Different options are presented based upon the type of backup being created.
   - File/Directory - input path for the backup.

7. Click Next.

8. Schedule the backup Days, Time, Storage Provider & Retention Count.

9. Click Complete to save.

7.5 Managing Backups

7.5.1 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.

7.5.2 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
   - Container
   - etc..
8. Click the Next button.
10. Click Complete to save.

7.5.3 Create Server Backup

To create a server backup:

1. Select the Backups link in the navigation bar.
2. Select the Backups link in the sub navigation bar.
3. Click Add Backup.
4. From the Create Backup Wizard select the radio button Server, then click Next.
5. Input the following:
   - Name of the backup job being created
   - Server
   - Type of backup you wish to create.
     - File
     - Directory
     - Mongo
     - MySQL
     - Postgres
6. Click Next. Different options are presented based upon the type of backup being created.
   • File/Directory - input path for the backup.

7. Click Next.

8. Schedule the backup Days, Time, Storage Provider & Retention Count.

9. Click Complete to save.
8.1 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.

8.2 Reports

8.2.1 Overview

Customizable Cloud, App and Instance usage reports can be generate in the *Operations -> Reports* section.
8.2.2 Report Types

INVENTORY REPORTS

Account
- Tenant Inventory Summary

Infrastructure
- Cloud Inventory Summary
- Container Host Inventory Summary
- Group Inventory Summary
- Hypervisor Inventory Summary
- Tenant Resource Allocation

Provisioning
- Instance Inventory Summary
- Virtual Machine Inventory Summary

CLOUD REPORTS

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

COST REPORTS

Cost
- Application Cost
- Cloud Cost
- Group Cost
- Instance Cost
- Tenant Cost

8.2.3 Reports History

The landing page of the reports section gives a selection of report types to generate and a history view of generated reports.

8.2.4 Generating Reports

To generate a new Report
1. Select a Report type
2. Set Start and End dates for the report
3. Select Cloud(s)
4. Select other options depending on report type
5. Select run and the report will be generated

### 8.2.5 Viewing Reports

To view a report, select the Name of the report after the status changes to ready. Generated Reports are available from the Reports History page or in their respective Section.

---

**Note:** All reports are saved and accessible until deleted.

---

### 8.3 Analytics

#### 8.3.1 Overview

The Morpheus Analytics engine analyzes resource utilization and costs across clouds. This functionality helps users make decisions on where instances and workloads should be provisioned.
8.3.2 Analytics Report Types

Cost

By Application
- Month to Date

By Cloud
- Month to Date

By Group
- Month to Date

By Instance
- Month to Date

By Tenant
• Month to Date

Instances Types

By Cloud
• Count
• Total Memory
• Total Storage
• Total CPUs/Cores

By Group
• Count
• Total Memory
• Total Storage
• Total CPUs/Cores

Instances

By Cloud
• Count
• Total Memory
• Total Storage
• Total CPUs/Cores

By Group
• Count
• Total Memory
• Total Storage
• Total CPUs/Cores

Utilization

CPU vs Price
• Hosts
• Virtual Machines
• Bare Metal

Overall vs Price
• Hosts
• Virtual Machines
• Bare Metal

RAM vs Price
• Hosts
• Virtual Machines
• Bare Metal
8.4 Guidance

8.4.1 Overview

The Operations -> Guidance section show recommendations for Resource and Costs Utilization optimization. By analyzing the CPU, RAM, and Storage activity of Instances and Hosts, Morpheus can recommend actions for Sizing and Power State.

Configuration

Guidance is configured per Cloud and is set to off by default.

To turn on Guidance for a Cloud:
1. Navigate to Infrastructure -> Clouds.
2. Select the Edit icon of the Cloud to configure Guidance for.
3. Expand the Advanced Options section in the Edit Cloud modal.
5. Select Save Changes.

Guidance recommendations will begin to appear in the guidance section when generated.

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.
8.5 Scheduling

8.5.1 Overview

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.

8.5.2 Power Schedules

Create Power Schedule

1. Navigate to Operations -> 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 -> Hosts -> 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 to a Cloud

Note: Power Schedule Policies apply to Instances created in the Cloud 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
5. Select TYPE Power Schedule
6. Configure the Power Schedule 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 Operations -> Scheduling
   Permissions- TENANTS Leave blank to apply to all Tenants, or search for and select Tenants to enforce the Policy on specific Tenants.
7. Select SAVE CHANGES

Add Power Schedule to a Group

Note: Power Schedule Policies apply to Instances created or moved into the Group 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
5. Select TYPE Power Schedule
6. Configure the Power Schedule 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 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 Operations -> Scheduling
   - Permissions- TENANTS Leave blank to apply to all Tenants, or search for and select Tenants to enforce the Policy on specific Tenants.

8.5.3 Execution Schedules

Create Execution Schedule

- NAME
- DESCRIPTION
- TIME ZONE
- Enabled
- SCHEDULE
  - 0 0 * * *
  - Every day at 00:00

8.6 Approvals

Morpheus and Service Now Approvals

8.6.1 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.
8.6.2 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.

8.6.3 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 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:

• Request: What is being requested
• Type: The type of the approval request
- Request For: Name and link to Instance
- Status
- Date Created
- Requested By
- Actions dropdown * For Internal Approval Requests
  - Approve
  - Deny
  - Cancel
  - For ServiceNow Approval Requests * Cancel

**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.

### 8.7 Usage

#### 8.7.1 Overview

The Operations -> Usage section shows Billing information for Instances and Hosts that have pricing configured on their Service Plan.
**Important:** Pricing must be enabled in Administration -> Provisioning and Service Plans configured with Price sets in Administration -> Plans & Pricing for Pricing to show in the Usage section.

### 8.7.2 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.

### 8.7.3 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.

### 8.8 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.

#### 8.8.1 Activity Reports

There are 5 types of activities that are displayed in the Activity Reports:

- Provisioning
- Monitoring
- Alert
- Backups
- Logs

**To View a Recent Activity report:**

1. Select the Reports link in the navigation bar.
2. Click the tab Recent Activity.

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.

**To Filter:**

1. Click the filter drop down of type of filter you want to apply.
2. Select the appropriate filter.

### 8.9 Health

#### 8.9.1 Morpheus Health

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

**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
8.9.2 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.

8.9.3 Morpheus Logs

The Logs displayed in 'Operations - 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 Operations - Health - Morpheus Logs are filtered for Morpheus services. Complete stack traces can be found in /var/log/morpheus/morpheus-ui/current.
CHAPTER 9

Services

9.1 Cypher

9.1.1 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.

9.1.2 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 milliseconds and default to 32 days (2764800000 ms).
  - Quick MS Time Reference:
    - Day: 86400000
    - Week: 604800000
9.1.3 Creating Cypher Keys

1. Navigate to Services - Cypher and select “+ ADD KEY”
2. Configure one of the following types of Keys:

9.1.4 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 milliseconds (ex. 604800000 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.

9.1.5 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 milliseconds (ex. 604800000 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.

9.1.6 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 milliseconds (ex. 604800000 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.

### 9.1.7 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 milliseconds (ex. 604800000 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.

### 9.1.8 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.

### 9.2 Archives

#### 9.2.1 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.
9.2.2 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.

9.2.3 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.

9.2.4 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.

9.2.5 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.

9.2.6 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).
10.1 Automation

10.1.1 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 the 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
Add Ansible Integration

1. Navigate to **Provisioning -> Automation -> 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.
   - **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 ran 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 Provisioning -> 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.
---
- 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 Option type that provides a text box to enter a username. The fieldName of the option type in this case would be `username`. Below is the playbook.

---
- 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.

- 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:
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.

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 it’s 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.

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 but certain os’s or network conditions can prevent automated install. You can run `ansible --version` in the Morpheus Appliance, or in the Ansible integration details page (Administration -> Integrations -> Select Ansible Integration, or 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:

```bash
sudo apt-get install software-properties-common
sudo apt-add-repository ppa:ansible/ansible
sudo apt-get update
sudo apt-get install ansible
```

CentOS:

```bash
sudo yum install epel-release
sudo yum install ansible
```

Then create the working Ansible directory for Morpheus:

```bash
sudo mkdir /opt/morpheus/.ansible
sudo chown morpheus-local.morpheus-local /opt/morpheus/.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 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.

- 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.

### 10.1.2 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: It will not import data of the jobs which are not executed from Morpheus.

### Add Ansible Tower Integration

1. Navigate to Administration -> Integrations 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: Enabled by default it is enabled. To disable the integration, uncheck this option and save.
   - Ansible Tower URL: This would be 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.

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.

### 10.1.3 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 Actions->Run Workflow. 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 \url{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.

**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

### 10.1.4 Puppet

**Overview**

**Add Puppet Integration**

1. Navigate to Administration -> Integrations and select + New Integration
2. Select Integration type “Puppet”
3. Populate the following fields
   - Name: Name of the Puppet Integration in Morpheus
   - Puppet Master: Hostname
   - Allow Immediate Execution: Yes or No
4. Save Changes

### 10.1.5 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 dropdown.
After a page refresh you should see your Saltstack tab in your group page.

Clicking on it will reveal a page that includes:
1. An interface to run Salt Master commands
2. Parsed Top File
3. Available States

The classic example of running

```bash
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.
In our example the Apache State from a git backend was applied successfully to our newly created vm.
10.1.6 Terraform

Requirements

Role Access

- In order to see the Terraform Blueprint type option and create Terraform App Blueprints in Provisioning -> 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
- AWS
- 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.

2. Create a working directory for Terraform, and change owner to morpheus-app.

   ```bash
   sudo mkdir /var/opt/morpheus/morpheus-ui/terraform
   sudo chown morpheus-app.morpheus-app /var/opt/morpheus/morpheus-ui/terraform
   ```

   The default location is `/var/opt/morpheus/morpheus-ui/terraform` but can be changed.

3. Add the Terraform working path to `/opt/morpheus/conf/application.yml`

   ```bash
   sudo vi /opt/morpheus/conf/application.yml
   ```

   Add the following to the application.yml config below and in-line with the repo section:

   ```yaml
   terraform:
     location: '/var/opt/morpheus/morpheus-ui/terraform'
   ```

   Example application.yml config with Terraform location added:

   ```yaml
   repo:
     git:
       location: '/var/opt/morpheus/morpheus-ui/repo/git'
     local:
       location: '/var/opt/morpheus/morpheus-ui/repo/local'
   terraform:
     location: '/var/opt/morpheus/morpheus-ui/terraform'
   bitcan:
     backup:
       destination:
         root: '/var/opt/morpheus/bitcan/backup'
         working: '/var/opt/morpheus/bitcan/working'
   ```

   **Important:** Uses spaces not tabs to indent or ui startup will fail. If you used a different path than the default location, enter that path instead.
4. Restart the morpheus-ui to apply the application.yml config.

```
sudo morpheus-ctl restart morpheus-ui
```

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 versions 3.3.0 and 3.3.1 VMware cloud types are supported for Terraform App provisioning targets. Additional clouds will be available in later releases.

1. Navigate to Provisioning -> 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 TFVAR 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 TFVAR 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 Provisioning -> Apps.

**Provisioning Terraform Apps**

**Note:** An existing Terraform App Blueprints must be added to Provisioning -> Blueprints before it can be provisioned.

**Note:** 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.

1. Navigate to Provisioning -> Apps
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 (Provisioning -> Apps -> select the App). This section contains State and Plan output:
10.2 Backups

10.2.1 Commvault

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**

### 10.2.2 Veeam

**Adding Veeam Integration**

1. Navigate to *Backups -> Services*
2. Select + ADD
3. Select Veeam
4. Fill in the following:
   - **Name** Name of the Integration in Morpheus
   - **Enabled** Enable the Veeam integration
   - **Host** IP or Hostname of the Veeam server.
   - **Port** Port number configured to access the Veeam server
   - **Username** Admin Username for Veeam
   - **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**

**Important:** Once a Veeam Integration has been enabled, a VEEAM SERVER setting will be available in VMware and Hyper-V cloud settings (Infrastructure -> Clouds -> Edit a Cloud). To enabled backups on a Cloud, a Veeam Server must be selected in the VEEAM SERVER dropdown in the Cloud settings and saved. Failure
to do so will result in blank Backup Repositories and Backup Job Templates options when configuring Veeam Backups during provisioning”.

10.2.3 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

10.2.4 Zerto

Adding Zerto Integration

1. Navigate to Backups -> Services
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 or Zerto Replication Manager
   - **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

10.3 Clouds

10.3.1 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

- Virtual Machine Provisioning
- Containers
- Backups / Snapshots
- Resources Groups
- Migrations
- Auto Scaling
- Load Balancing
- AWS Marketplace Search and Provisioning
- Remote Console
- Periodic Synchronization
- Lifecycle Management and Resize
- Restore from Snapshots
- EC2
- RDS
- S3
- ELBs
- ALBs
- Route53
- IAM Profile sync and assignment
- Network Sync
- Security Group Sync (selectable when provisioning, will not appear in Security Groups section)
• Pricing Sync
• Assign Elastic IP’s
• Network Pools
• MetaData Tag creation

Morpheus can provide a single pane of glass and self-service portal for managing instances scattered across both AWS and private cloud offerings like VMWare and Hyper-V.

Requirements

AWS IAM Security Credentials  Access Key Secret Key Sufficient User Privileges (see MinimumIAMPolicies section for more info)


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.

Note: Each AWS Cloud in Morpheus is scoped to an AWS Region and VPC Multiple AWS Clouds can be added and even Grouped. Verify Security groups are properly configured in all Regions Morpheus will scope to.

Adding an AWS Cloud

1. Navigate to Infrastructure -> Clouds
2. Select + Create Cloud
3. Select AWS
4. Enter 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.
   Region  Select AWS Region for the Cloud
   Access Key  Access Key ID from AWS IAM User Security Credentials.
   Secret Key  Secret Access Key associate with the Access Key ID.
   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.

---

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.

**Advanced Options**

**DOMAIN** Specify a default domain for instances provisioned to this Cloud.

**SCALE PRIORITY** 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 Managed

**SECURITY MODE** Defines if Morpheus will control local firewall of provisioned servers and hosts.

---

**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.

---

**STORAGE MODE** Single Disk, LVM or Clustered

**GUIDANCE** Enable Guidance recommendations on cloud resources.

**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.

**AGENT INSTALL MODE**

- **SSH / WINRM:** Morpheus will use SSH or WINRM for Agent install.
- **Cloud-Init (when available):** 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.

---

10.3. **Clouds**
API PROXY Required when a Proxy Server blocks communication between the Morpheus Appliance and the Cloud. Proxies can be added in the Infrastructure -> Networks -> Proxies tab.

Provisioning Options

PROXY Required when a Proxy Server blocks communication between an Instance and 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 Instance Agent communication to the Appliance URL.

USER DATA (LINUX) Add cloud-init user data or scripts. Assumes bash syntax.

Note: All fields and options can be edited after the Cloud is created.

Minimum AWS IAM Policies

Below are the AWS IAM Policies for EC2, RDS, and S3 covering the minimum access for Morpheus applying to all resources.


EC2

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AttachVolume",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CancelExportTask",
        "ec2:CancelImportTask",
        "ec2:CopyImage",
        "ec2:CreateImage",
        "ec2:CopySnapshot",
        "ec2:CreateInstanceExportTask",
        "ec2:CreateKeyPair",
        "ec2:CreateNetworkAcl",
        "ec2:CreateNetworkAclEntry",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSnapshot",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DeleteKeyPair",
        "ec2:DeleteNetworkAcl",
        "ec2:DeleteNetworkAclEntry",
```

(continues on next page)
"ec2:DeleteNetworkInterface",
"ec2:DeleteSecurityGroup",
"ec2:DeleteSnapshot",
"ec2:DeleteTags",
"ec2:DeleteVolume",
"ec2:DeregisterImage",
"ec2:DescribeAccountAttributes",
"ec2:DescribeAddresses",
"ec2:DescribeAvailabilityZones",
"ec2:DescribeClassicLinkInstances",
"ec2:DescribeConversionTasks",
"ec2:DescribeExportTasks",
"ec2:DescribeImageAttribute",
"ec2:DescribeImages",
"ec2:DescribeImportImageTasks",
"ec2:DescribeImportSnapshotTasks",
"ec2:DescribeInstances",
"ec2:DescribeInstanceStatus",
"ec2:DescribeKeyPairs",
"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:DescribeVpcs",
"ec2:DetachNetworkInterface",
"ec2:DetachVolume",
"ec2:DisassociateAddress",
"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",
"Resource": "*"
}
}

RDS:

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "rds:AddRoleToDBCluster",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:AuthorizeDBSecurityGroupIngress",
        "rds:CopyDBParameterGroup",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBSnapshot",
        "rds:CreateDBCluster",
        "rds:CreateDBClusterSnapshot",
        "rds:CreateDBInstance",
        "rds:CreateDBInstanceRead Replica",
        "rds:CreateDBSecurityGroup",
        "rds:CreateDBSnapshot",
        "rds:DeleteDBCluster",
        "rds:DeleteDBInstance",
        "rds:DeleteDBSecurityGroup",
        "rds:DeleteDBSnapshot",
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
      ]
    }
  ]
}
"rds:DescribeDBSecurityGroups",
"rds:DescribeDBSnapshotAttributes",
"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"
],
"Resource": "*"
}]

S3

{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
"s3:AbortMultipartUpload",
"s3:DeleteObject",
"s3:DeleteObjectVersion",
"s3:GetBucketLocation",
"s3:GetObject",
"s3:GetObjectVersion",
"s3:ListBucket",
"s3:ListBucketMultipartUploads",
"s3:ListBucketVersions",
"s3:ListMultipartUploadParts",
"s3:PutObject"
],
"Resource": [
"arn:aws:s3:::bucketname",
]}

(continues on next page)
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"
        }
    }
}
```

Amazon Cost and Reservation Sync

If you are enabling costing or costing and reservations sync on an amazon cloud then you will need to enable the following policy.

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ce:*",
            "Resource": *,
        }
    ]
}
```
10.3.2 Azure

Overview

Azure is Microsoft’s public cloud offering. Offering a full range of services and features across the globe in various datacenters. It is the equivalent of AWS for Microsoft running primarily on the Hyper-V based hypervisor. While it is a great public cloud offering, it can be somewhat difficult to get integrated with which is what this guide aims to cover.

Features

- Virtual Machine Provisioning
- Azure SQL Database
- Backups / Snapshots
- Resource Group Sync & Selection
- Network Sync & Selection
- Security Group Sync & Selection
- Storage Account Sync & Selection
- Marketplace Search and Provisioning
- Azure Marketplace Custom Library Item Support
- Remote Console
- Periodic Synchronization
- Lifecycle Management and Resize
- Availability Set Support
- Azure Load Balancers
- Azure Storage
- Docker Host Provisioning & Management
- Service Plan Sync
- Pricing Sync with markup options
- Cost Estimator

Combine these features with on premise solutions like Azure-Stack and Morpheus can provide a single pane of glass and self service portal for managing instances scattered across both public Azure and private Azure Stack offerings.

Note: Morpheus even supports integrating with CSP based accounts in Azure (typically used by managed service providers).

Requirements

- Azure Active Directory Application & Credentials
  - Client ID (old portal) / Application ID (new portal)
  - Client Secret (old portal) / Key Value (new portal)
– Tenant ID (old Portal) / Directory ID (new portal)
– Azure Subscription ID

• Above Active Directory App added as owner of this Azure Subscription

• Existing Azure Resources
  – Network Security Group(s) * Typical Inbound ports open from Morpheus Appliance: 22, 5985, 3389
    * Typical Outbound to Morpheus Appliance: 80, 443
    · 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.
  – Virtual Network(s)
    * Public IP assignment required for instances if Morpheus Appliance is not able to communicate with Azure instances private ip’s.
  – Resource Group(s)
  – Storage Account(s)

Note: Morpheus v2.10.3 added support for multiple Resource Groups and Storage Accounts per cloud, making our Azure integration more capable and easier to configure. Prior versions of Morpheus supported one resource group and one storage account per cloud, with the security group and network selection limited to the scoped Resource Group. If you are on an earlier version of Morpheus, please note you will need to add an Azure cloud integration for each Resource Group and Storage Account you would like to use.

Azure Active Directory Credentials

If you do not already have the Azure Active Directory credentials required to add an Azure cloud to Morpheus, use the steps below to obtain them.

Important: Microsoft recently added support for Active Directory application configuration in the new Azure portal. Previously, users had to use the old portal to get the required credentials to integrate Azure with Morpheus. The instructions below are updated for the new portal. Microsoft also changed the naming conventions of the credentials:

<table>
<thead>
<tr>
<th>Old Azure Portal Name</th>
<th>New Azure Portal Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenant ID</td>
<td>Directory ID</td>
</tr>
<tr>
<td>Client ID</td>
<td>Application ID</td>
</tr>
</tbody>
</table>

Creating an Azure Active Directory Application

If you do not have an existing Azure Active Directory application for Morpheus, you will need to create a new one by:

1. Log into the Azure portal
2. Select “Azure Active Directory”
3. Select “App Registrations”
4. Select “New Application Registration”

5. Next, give your new AD 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 Azure Active Directory Application will be created.
Now that we have (or already had) our AD app, we will gather the credentials required for the Morpheus Azure integration.

**Tenant ID/Directory ID**

While still in the Active Directory Section:

1. Select Properties
2. Copy the Directory ID
3. Store/Paste for use as the Tenant ID when Adding your Azure cloud in Morpheus
Client ID/Application ID

1. Select App Registrations
2. Select your Active Directory Application
3. Copy the Application ID
4. Store/Paste for use as the Client ID when Adding your Azure cloud in Morpheus
Client Secret/Key Value

While still in your Active Directory Application:
1. Select Keys in the Settings pane
2. Enter a name for the key
3. Select a duration
4. Select save
5. Copy the Key Value
6. Store/Paste for use as the Client Secret when Adding your Azure cloud in Morpheus

Important: Copy the key value. You won’t be able to retrieve after you leave this blade.

You now have the 3 Active directory credentials required for Morpheus Azure cloud integration.

Subscription ID

The last credential required for the Morpheus Azure cloud integration is the Azure Subscription ID
1. Select Resource Groups
2. Select a Resource Group (instruction below if you do not have an existing resource group)
3. Copy the Subscription ID
4. Store/Paste for use as the Subscription ID when Adding your Azure cloud in Morpheus
Make Azure Active Directory Application owner of Subscription

The Active Directory Application used needs to be an owner of the subscription used for the Azure Morpheus cloud integration.

1. In the Subscription pane, select “Access Control (IAM)”
2. Click “+ Add”, in the pane to the right, select “1 Select a role” and then select “Owner”
3. Select “2. Add Users” and in the search box begin to type the name of the AD Application created earlier.

**Note:** the AD Application will not display by default and must be searched for.

4. Select the Application, then click “Select” at the bottom of the Add Users pane, and the select “OK” at the bottom of the Add Access pane.

**Important:** Be sure to select “OK” at the bottom of the Add Access pane or the user addition will not save.
You now have the required Credentials to add an Azure cloud integration into Morpheus.

**Important:** You will also need to have existing Network Security Group(s), Virtual Networks(s) and Storage Accounts(s). Instructions for creating these can be found later in this article.

### Add Azure cloud in Morpheus

Azure is now ready to be added into Morpheus. Ensure you have the noted Subscription ID, Tenant ID, Client ID, and Client Secret accessible.

1. In Infrastructure - Clouds, select **CREATE CLOUD** and select Azure from the cloud widget.

   OR

2. In Infrastructure, Groups- you can select the Clouds tab of a Group and click **ADD** next to Azure in the Public Cloud section

3. Enter the following:
   - Name
   - Location (optional)
   - Domain (if not localdomain)
   - Scale Priority
   - Subscription ID (from step 18)
   - Tenant ID (from step 16)
• Client ID (from step 13)
• Client Secret (from step 13)

If everything is entered correctly, the Location dropdown will populate.

4. Select the Location/Region to scope the cloud to (additional Clouds can be added for multiple regions)
5. Select All or specify a Resource Group to scope this cloud to
6. Optionally select “Inventory Existing Instances” (This will inventory your existing vm’s in Azure and list them in Morpheus as unmanaged instances.)
7. Click + Save Changes

Your Azure Cloud will be created.
Creating Resources in Azure

If you do not have existing Network Security Groups, Virtual Networks, or Storage Accounts, you can create them by following the steps below:

Create a Network Security Group

1. In the main Azure toolbar, select the right arrow at the bottom of the toolbar (if collapsed) and search for and select Network Security Groups.
2. Click “+ Add” at the top of the Network security groups pane
3. Enter a unique name for the security group, select the correct subscription, and either select the resource group being used, or create a new one as shown below. Also verify the Location is the same, and then click “Create” at the bottom of the pane.

![Security Group Configuration](image)

4. Configure inbound and outbound rules for the security group. Ports 80 (http), 443 (https) 22 (ssh) and 5985 (winrm) need to be open to and from the Morpheus appliance.

**Create a Virtual Network**

1. In the main Azure toolbar, select the right arrow at the bottom of the toolbar (if collapsed) and search for and select Virtual Networks.
2. Click “+ Add” at the top of the Virtual Networks pane
3. Enter a unique name for the virtual network, the correct subscription, select “Use existing” and select the same resource group as the Network Security Group. Also verify the Location is the same, and then click “Create” at the bottom of the pane.

Create a Storage Account

1. In the main Azure toolbar, select the right arrow at the bottom of the toolbar (if collapsed) and search for and select Storage Accounts.
2. Click “+ Add” at the top of the Storage accounts pane
3. Enter a unique name for the storage account, select “Locally-redundant storage (LRS) for Replication, select the correct subscription, select “Use existing” and select the same resource group as the Network Security Group and Virtual Network. Also verify the Location is the same, and finally click “Create” at the bottom of the pane.

Docker

So far this document has covered how to add the Azure 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 Azure (multiple are needed when dealing with horizontal scaling scenarios).

To provision a Docker Host simply navigate to the Cloud detail page or Infrastructure?Hosts section. From there click the + Container Host button to add a Azure Docker Host. This host will show up in the 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 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.

**Multi-tenancy**

A very common scenario for Managed Service Providers is the need to provide access to Azure resources on a customer by customer basis. With Azure several administrative features have been added to ensure customer resources are properly scoped and isolated. For Azure it is possible to assign specific Networks, and Resource Groups to customer accounts or even set the public visibility of certain resources, therefore allowing all sub accounts access to the resource.

**Azure Scale Sets**

Auto-scaling Azure instances can be done with the native Morpheus scaling service or Azure Scale Sets. When using Azure Scale Sets, Morpheus will configure the scale sets and thresholds, but Azure will be responsible for scaling the instances. The Instances nodes that are added and removed by Azure will be synced in by Morpheus as the instance scales up and down.

**Note:** Instances can only be added to Azure Scale Sets at provision time.

**Adding an Instance to a Scale Set**

1. In **Provisioning - Instances** select + **ADD**
2. Select an Instance Type that has scaling enabled (Advanced section when editing an Instance Type in **Provisioning - Library**)
3. Configure the Instance as desired
4. In the **AUTOMATION** section under **Scale - Scale Type** select **Azure Scale Set**
5. Select a default Threshold. Threshold pre-sets can be added in **Provisioning - Automation- Scale Thresholds** (requires Instances - Thresholds permission)
6. Complete the instance configuration and provision the instance.
A Virtual Machine scale set will be created in Azure with the selected threshold and min/max node settings.

**Create Threshold Presets**

1. In Provisioning - Automation select the *SCALE THRESHOLDS* tab

*Note:* Access to the SCALE THRESHOLDS section requires *Instances - Thresholds* Role permissions.
2. Select + ADD
3. Configure Threshold settings.
4. Select **SAVE CHANGES**

The new Threshold will be available for selection in the SCALE section during provisioning or when configuring an App Blueprint.

**Edit Thresholds on an Instance**

1. In **Provisioning - Instances** select the target Instance.
2. Select the **SCALE** tab below the VM’s section
3. In the **THRESHOLDS** section of the SCALE tab, click **EDIT**
4. Update the threshold settings.
5. Select **APPLY**

**Note:** Morpheus will sync in changes to a scale sets threshold settings if the settings are edited in Azure.
10.3.3 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
- 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](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:
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:

   - **NAME** Internal name for the Cloud in Morpheus
   - **LOCATION** (Optional) Can be used to specify the location of the Cloud or add a description.
   - **VISIBILITY** Determines Tenant visibility for the Cloud.
     - Private: Access to the Cloud is limited to the assigned Tenant (Master Tenant by default)
     - Public: Access to the Cloud can be configured for Tenants in their Tenant Role permissions.
   - **IDENTITY 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/
   - **IDENTITY RESOURCE URL** Azure AD Azure Stack Administrator App ID URI Example: https://adminmanagement.xxxxxxx.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 your 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

4. 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.

5. 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  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.

HYPER-CONVERGED ENABLED  Not applicable for Azure Stack

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.

AGENT INSTALL MODE

• SSH / WINRM: Morpheus will use SSH or WINRM for Agent install.

• Cloud-Init (when available): 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.

API PROXY  Required when a Proxy Server blocks communication between the Morpheus Appliance and the Cloud. Proxies can be added in the Infrastructure -> Networks -> Proxies tab.

Provisioning Options

API PROXY  Required when a Proxy Server blocks communication between an Instance and 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 Instance Agent communication to the Appliance URL.

USER DATA (LINUX)  Add cloud-init user data using bash syntax.
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.

**Review**

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.

### 10.3.4 Cloud Foundry

**Configuration**

**Adding PCF Cloud From Infrastructure -> Clouds**

1. Navigate to *Infrastructure -> Clouds*
2. Select *ADD*
3. Select *CLOUD FOUNDARY* from the Clouds list
4. Select *NEXT*
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.
   - **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.

6. Select `NEXT` .. include:: /integration_guides/Clouds/advanced_options.rst

7. Select `NEXT`

8. 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.

9. Select `NEXT`

10. 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.
   - **DOMAIN** Specify a default domain for instances provisioned to this Cloud.
   - **SCALE PRIORITY** 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 Managed

SECURITY MODE  Defines if Morpheus will control local firewall of provisioned servers and hosts.

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.

STORAGE MODE  Single Disk, LVM or Clustered

GUIDANCE  Enable Guidance recommendations on cloud resources.

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.

AGENT INSTALL MODE

• SSH / WINRM: Morpheus will use SSH or WINRM for Agent install.

• Cloud-Init (when available): 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.

API PROXY  Required when a Proxy Server blocks communication between the Morpheus Appliance and the Cloud. Proxies can be added in the Infrastructure -> Networks -> Proxies tab.

PROXY  Required when a Proxy Server blocks communication between an Instance and 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 Instance Agent communication to the Appliance URL.

USER DATA (LINUX)  Add cloud-init user data or scripts. Assumes bash syntax.

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.

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 Provisioning -> Library section and the layout will be automatically added to the Instance Type selected when adding the Marketplace Item.

Provisioning Instances

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.

Important: Add Deployments in Provisioning -> 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 -> 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.

### 10.3.5 Digital Ocean

**Add a Digital Ocean Cloud**

DigitalOcean Cloud Integration Detail fields:

**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.
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  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 Managed

SECURITY MODE  Defines if Morpheus will control local firewall of provisioned servers and hosts.

| 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. |

STORAGE MODE  Single Disk, LVM or Clustered

GUIDANCE  Enable Guidance recommendations on cloud resources.

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.

AGENT INSTALL MODE

- SSH / WINRM: Morpheus will use SSH or WINRM for Agent install.
- Cloud-Init (when available): 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.

API PROXY  Required when a Proxy Server blocks communication between the Morpheus Appliance and the Cloud. Proxies can be added in the Infrastructure -> Networks -> Proxies tab.

Provisioning Options

PROXY  Required when a Proxy Server blocks communication between an Instance and 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 Instance Agent communication to the Appliance URL.

USER DATA (LINUX)  Add cloud-init user data or scripts. Assumes bash syntax.

**10.3.6 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 Name
   - 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**  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 Managed

**SECURITY MODE**  Defines if Morpheus will control local firewall of provisioned servers and hosts.

**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.
STORAGE MODE  Single Disk, LVM or Clustered

GUIDANCE  Enable Guidance recommendations on cloud resources.

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.

AGENT INSTALL MODE

• SSH / WINRM: Morpheus will use SSH or WINRM for Agent install.
• Cloud-Init (when available): 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.

API PROXY  Required when a Proxy Server blocks communication between the Morpheus Appliance and the Cloud.
Proxies can be added in the Infrastructure -> Networks -> Proxies tab.

Provisioning Options

PROXY  Required when a Proxy Server blocks communication between an Instance and 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 Instance Agent communication to the Appliance URL.

USER DATA (LINUX)  Add cloud-init user data or scripts. Assumes bash syntax.

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.

10.3.7 Google

Requirements

• IAM Service Account with Owner or Compute Admin Role permissions
• project_id, private_key and client_email for the Service Account
• Compute Engine API enabled in GCP API’s and Services

Features

• Provisioning Virtual Machines
• Network tagging
• Private and Local Images
Morpheus Documentation, Release 3.6.1

- Google VM Snapshots
- Brownfield Inventory
- Costing
- Right sizing

**Add a Google Cloud**

**Tip:** All of the required Google Cloud credentials can be found in the .json file created when generating a key for a Google Cloud service account.

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:
   - **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.
   - **Project ID** Google Cloud Project ID
   - **Private Key** Service Account Private key, beginning with ——BEGIN PRIVATE KEY——' and ending with ‘—–END PRIVATE KEY—–
   - **Client Email** Service Account Client Email. ex: morpheus@morpheus.iam.gserviceaccount.com
   - **Region** Regions will auto-populate upon successful authentication with the above credentials. Select appropriate region for this Cloud.
   - **Inventory Existing Instances** If enabled, existing Google Instances will be inventoried and appear as unmanaged Virtual Machines in Morpheus.

**Note:** Morpheus scopes clouds to single regions. Multiple clouds can be added for multi-region support, and then optionally added to the same group.

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** 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 Managed
SECURITY MODE  Defines if Morpheus will control local firewall of provisioned servers and hosts.

**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.

STORAGE MODE  Single Disk, LVM or Clustered
GUIDANCE  Enable Guidance recommendations on cloud resources.
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.

AGENT INSTALL MODE
- SSH / WINRM: Morpheus will use SSH or WINRM for Agent install.
- Cloud-Init (when available): 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.

API PROXY  Required when a Proxy Server blocks communication between the Morpheus Appliance and the Cloud. Proxies can be added in the Infrastructure -> Networks -> Proxies tab.

Provisioning Options

PROXY  Required when a Proxy Server blocks communication between an Instance and 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 Instance Agent communication to the Appliance URL.
USER DATA (LINUX)  Add cloud-init user data or scripts. Assumes bash syntax.

Finally, add Google Cloud to an existing Group or create a new Group, and you have now integrated Morpheus with Google Cloud!

**Important:** If you experience difficulties adding a GCP Cloud, ensure you have met all the Requirements above, and have logged into Google Cloud and navigated to the Compute Engine sections as it will not be initialized until navigated to upon Google Cloud account creation.

### 10.3.8 Huawei Cloud

<table>
<thead>
<tr>
<th>NAME</th>
<th>CODE</th>
<th>LOCATION</th>
<th>VISIBILITY</th>
<th>TENANT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Details IDENTITTY API URL DOMAIN ID This pertains to the Openstack V3 API and should be ignored when using V2. This is the Domain ID (Not to be confused with Domain Name). The Domain ID can be found via the CLI by typing openstack domain list. PROJECT USERNAME PASSWORD OS VERSION IMAGE FORMAT LB TYPE
Inventory Existing Instances Enable Hypervisor Console

Hypervisor console support for openstack currently only supports novnc. Be sure the novnc proxy is configured properly in your openstack environment. Advanced Options Provisioning Command

10.3.9 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 and 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
- Containers
- Backups / Snapshots
- Resources Groups
- Migrations
- Auto Scaling
- Load Balancing
- Remote Console
- Periodic Synchronization
- Veeam Integration
- Lifecycle Management and Resize
- Unique Kerberos Authentication

Morpheus can provide a single pane of glass and self-service portal for managing instances scattered across both Hyper-V and public cloud offerings like Azure.

Getting Started

To get started this 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. This document covers Hyper-V 2008 and Hyper-V 2012.

A user account that is part of the local administrators group on the Hyper-V host is also required.

Understand 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 below Microsoft link:

**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:
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:

```
$ sudo yum install krb5-workstation pam_krb5 -y
```

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.

```
[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 on instructions on how to create a keytab file.

**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.
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 all can be easily managed from the Admin | Service Plans & Pricing section.
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 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 Hyper-V (multiple are needed when dealing with horizontal scaling scenarios).

To provision a Docker Host simply navigate to the Cloud detail page or Infrastructure | Hosts section. From there click the + Container Host button to add a Hyper-V 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.

10.3. Clouds

Docker
10.3.10 KVM

Adding VLANs to Morpheus KVM Hosts (CentOS)

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 interfacing.

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.

### 10.3.11 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 must be scoped to a specific data center and cluster. If the drop downs do not populate, please verify the api url and provided credentials have access to Vcenter.

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.

**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 -> Hosts -> 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 Provisioning -> 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.

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 Cloud detail page or Infrastructure->Hosts section. From there click the + Container Host button 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 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.

**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 *Use VNC*. 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.

10.3.12 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
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.

API URL  example: https://10.30.21.220:9440
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.

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 Hosts section. From there click the + Container Host button 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.

10.3.13 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 ranging from HP’s Helion Cloud to Cisco’s Metapod / Metacloud offering. Morpheus supports integration with all the various platform offerings and ranges in support all the way back to Openstack Icehouse. It leverages the APIs and provides full functionality as a self service portal in front of Openstack.

Features

• Virtual Machine Provisioning
• Backups / 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 / configuration

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

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

Adding an Openstack cloud to Morpheus is one of the simpler cloud integrations to get started with. First go to the Infrastructure -> Clouds section and click add cloud. From here there are several options including Metapod, Helion, and general Openstack. Any of these options will actually work and for the most part the branded Openstack options are represented to make it clearer to the user as to the capabilities of Morpheus.

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 scopable to domains and projects as needed. The remaining options help Morpheus determine what 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 2 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 -> Hosts -> 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.

**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. They include OS Volume Type (Local or Volume). This basically 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 instances 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 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 Openstack (multiple are needed when dealing with horizontal scaling scenarios).

To provision a Docker Host simply navigate to the Cloud detail page or **Infrastructure->Hosts** section. From there click the + **Container Host** button to add a Openstack Docker Host. This host will show up in the 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 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.

10.3.14 Oracle VM

Add an Oracle VM Cloud

**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.

**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.

10.3.15 Open Telekom Cloud

Add an Open Telekom Cloud

**NAME**  Name of the Cloud in Morpheus

**CODE**

**LOCATION**  Description field for adding notes on the cloud, such as location.

**VISIBILITY**  Description field for adding notes on the cloud, such as location.

**TENANT**  Enabled Details

**IDENTITY API URL**

**DOMAIN ID**  This pertains to the Openstack V3 API and should be ignored when using V2. This is the Domain ID (Not to be confused with Domain Name). The Domain ID can be found via the CLI by typing openstack domain list.

**PROJECT**

**USERNAME**

**PASSWORD**

**OS VERSION**
IMAGE FORMAT

**LB TYPE**  Inventory Existing Instances Enable Hypervisor Console

**Note:** Hypervisor console support for openstack currently only supports novnc. Be sure the novnc proxy is configured properly in your openstack environment.

Advanced Options
Provisioning Command

**10.3.16 SCVMM**

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 is 5985 in order for Morpheus to communicate to SCVMM. You will also want to make sure SCVMM has WinRM enabled.

- **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.
- **SCVMM HOST**  IP or url of SCVMM host
- **USERNAME**  SCVMM Username. ex: svc.scvmm
- **PASSWORD**  SCVMM User Password
- **CLOUD**  Select a Cloud from the available Clouds in SCVMM.
- **WORKING PATH**  Path for Morpheus to write to. ex: c:\Cloud
- **DISK PATH**  Path for Virtual Disks. ex: c:\VirtualDisks

1. The Cloud can now be added to a Group or configured with additional Advanced options.

**10.3.17 Softlayer**

Add a Softlayer Cloud

- **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.
- **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.

10.3.18 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:
   - Name  Name of the Cloud in Morpheus
   - Code  Cloud Code for variables
   - 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 which Tenant to scope visibility to when Visibility is set to Private.
   - Enabled  Unchecking will disable the scheduled cloud-sync job
   - 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
     - 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

10.3.19 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:
   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.
   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.
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 `Provisioning -> 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 **Provisioning -> 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**
10.3.20 vCloud Director

Configuration

Add vCD Cloud From Infrastructure -> Clouds

1. Navigate to Infrastructure -> Clouds
2. Select + ADD
3. Select VCDIRECTOR from the Clouds list
4. Select NEXT
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.
   - **API URL**: vCloud Director API URL. Example: https://org.vcd.company.com
   - **USERNAME**: vCD Organization Administrator User
     NOTE:: User must have an Organizational Administrator Role in the selected Origination for successful provisioning
   - **PASSWORD**: vCD Organization Administrator User password
   - **ORGANIZATION**: Select Organization. Dropdown populates upon successful authorization.
   - **VDC**: Select VDC. Dropdown populates upon successful authorization.
   - **Inventory Existing Instances**: If enabled, existing Virtual Machines will be inventoried and appear as unmanaged Virtual Machines in Morpheus.
     NOTE: Multiple Organizations/VDC’s can be added by creating additional Clouds in Morpheus.
DOMAIN Specify a default domain for instances provisioned to this Cloud.

SCALE PRIORITY 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 Managed

SECURITY MODE Defines if Morpheus will control local firewall of provisioned servers and hosts.

**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.

STORAGE MODE Single Disk, LVM or Clustered

GUIDANCE Enable Guidance recommendations on cloud resources.

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.

AGENT INSTALL MODE

- SSH / WINRM: Morpheus will use SSH or WINRM for Agent install.
- Cloud-Init (when available): 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.

API PROXY Required when a Proxy Server blocks communication between the Morpheus Appliance and the Cloud. Proxies can be added in the Infrastructure -> Networks -> Proxies tab.

PROXY Required when a Proxy Server blocks communication between an Instance and 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 Instance Agent communication to the Appliance URL.

USER DATA (LINUX) Add cloud-init user data or scripts. Assumes bash syntax.

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
Add vCD Cloud From Infrastructure -> Groups

1. Navigate to Infrastructure -> Groups
2. Select a Group
3. Select the CLOUDS tab
4. Scroll down to VCD DIRECTOR 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.
   - API URL
     - vCloud Director API Url: Example: https://org.vcd.company.com
   - USERNAME: vCD Organization Administrator User
     - NOTE: User must have an Organizational Administrator Role in the selected Origination for successful provisioning
   - PASSWORD: vCD Organization Administrator User password
   - ORGANIZATION: Select Organization. Dropdown populates upon successful authorization.
   - VDC: Select VDC. Dropdown populates upon successful authorization.
   - Inventory Existing Instances: If enabled, existing Virtual Machines will be inventoried and appear as unmanaged Virtual Machines in Morpheus.
     - NOTE: Multiple Organizations/VDC’s can be added by creating additional Clouds in Morpheus.
   - DOMAIN: Specify a default domain for instances provisioned to this Cloud.
   - SCALE PRIORITY: 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 Managed
   - SECURITY MODE: Defines if Morpheus will control local firewall of provisioned servers and hosts.

   **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.

   - STORAGE MODE: Single Disk, LVM or Clustered
   - GUIDANCE: Enable Guidance recommendations on cloud resources.
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.

AGENT INSTALL MODE
- SSH / WINRM: Morpheus will use SSH or WINRM for Agent install.
- Cloud-Init (when available): 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.

API PROXY  Required when a Proxy Server blocks communication between the Morpheus Appliance and the Cloud. Proxies can be added in the Infrastructure -> Networks -> Proxies tab.

PROXY  Required when a Proxy Server blocks communication between an Instance and 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 Instance Agent communication to the Appliance URL.

USER DATA (LINUX)  Add cloud-init user data or scripts. Assumes bash syntax.

6. Select NEXT
7. Review and then Select COMPLETE

How to create vCloud Director templates for Morpheus

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.
   ```powershell
   Get-NetConnectionProfile | Set-NetConnectionProfile -NetworkCategory private
   ```
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.
   ```powershell
   Enable-PSremoting
   ```
7. Shutdown the virtual machine and convert to a template.

Note: Do not run sysprep

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)

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](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 admin-
istrator.

Once logged into vCloud director you will then need select Manage Organizations and then select your organ-
ization.

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 Provisioning > Virtual Images

10.3. Clouds
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.

10.3.21 Virtualbox

Add a VirtualBox Cloud

1. Navigate to Infrastructure -> Clouds
2. Select + CREATE CLOUD, select Virtual Box, and then click Next.
3. Enter the following into the Create Cloud modal:
   - **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.
   - **VIRTUALBOX HOST**: IP or URL of the VirtualBox Host
   - **WORKING PATH**: Path Morpheus will write to. ex: ~/virtualbox
   - **USERNAME**: Host Username
   - **PASSWORD**: Host Password
   - **BRIDGE NAME**: Will auto-populate upon successful authentication with the VirtualBox Host (E.X. ‘EN0: ETHERNET’)
   - **VBOXMANAGE EXECUTABLE**: Defaults to /usr/local/bin/vboxmanage if left blank
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**: 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 Managed
- **SECURITY MODE**: Defines if Morpheus will control local firewall of provisioned servers and hosts.

**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.
STORAGE MODE  Single Disk, LVM or Clustered

GUIDANCE  Enable Guidance recommendations on cloud resources.

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.

AGENT INSTALL MODE

• SSH / WINRM: Morpheus will use SSH or WINRM for Agent install.
• Cloud-Init (when available): 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.

API PROXY  Required when a Proxy Server blocks communication between the Morpheus Appliance and the Cloud. Proxies can be added in the Infrastructure -> Networks -> Proxies tab.

Provisioning Options

PROXY  Required when a Proxy Server blocks communication between an Instance and 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 Instance Agent communication to the Appliance URL.

USER DATA (LINUX)  Add cloud-init user data or scripts. Assumes bash syntax.

10.3.22 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/OFV 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 must be scoped to a specific data center and cluster. If the drop downs do not populate, please verify the api url and provided credentials have access to Vcenter.

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.

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 -> Hosts -> 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 Provisioning -> 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.
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 Cloud detail page or Infrastructure->Hosts section. From there click the + Container Host button 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 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.

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.
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 Use VNC. 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**

**Usage**

**VCenter**
• Non-Propagating

**Datacenter**
• Non-Propagating

**Cluster**
• Non-Propagating

**Host**
• Non-Propagating

**Datastore**
• Propagating

**Privileges**

**Datastore**
• 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

10.3.23 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:
   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.
   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’)

Chapter 10. Integration Guides
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**  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 Managed

**SECURITY MODE**  Defines if Morpheus will control local firewall of provisioned servers and hosts.

---

**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.

**STORAGE MODE**  Single Disk, LVM or Clustered

**GUIDANCE**  Enable Guidance recommendations on cloud resources.

**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.

**AGENT INSTALL MODE**

- **SSH / WINRM:** Morpheus will use SSH or WINRM for Agent install.
- **Cloud-Init (when available):** 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.

**API PROXY**  Required when a Proxy Server blocks communication between the Morpheus Appliance and the Cloud. Proxies can be added in the *Infrastructure -> Networks -> Proxies* tab.

**Provisioning Options**

**PROXY**  Required when a Proxy Server blocks communication between an Instance and 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 Instance Agent communication to the Appliance URL.

**USER DATA (LINUX)**  Add cloud-init user data or scripts. Assumes bash syntax.
10.3.24 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:
   - **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.
   - **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** 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 Managed
- **SECURITY MODE** Defines if Morpheus will control local firewall of provisioned servers and hosts.

<table>
<thead>
<tr>
<th>Important:</th>
<th>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.</th>
</tr>
</thead>
</table>

- **STORAGE MODE** Single Disk, LVM or Clustered
- **GUIDANCE** Enable Guidance recommendations on cloud resources.
- **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.

AGENT INSTALL MODE

- SSH / WINRM: Morpheus will use SSH or WINRM for Agent install.
- Cloud-Init (when available): 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.

API PROXY  Required when a Proxy Server blocks communication between the Morpheus Appliance and the Cloud. Proxies can be added in the Infrastructure -> Networks -> Proxies tab.

Provisioning Options

PROXY  Required when a Proxy Server blocks communication between an Instance and 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 Instance Agent communication to the Appliance URL.

USER DATA (LINUX)  Add cloud-init user data or scripts. Assumes bash syntax.

10.3.25 Windows Image with Cloudbase-Init

Morpheus supports provisioning Windows images with Cloudbase-init to set user data, network setting and other data at boot time. The following is an example of how to prepare a Windows image with cloudbase-init and optionally sysprep it.

Setup

1. On your Windows VM download and install Cloudbase-init from https://cloudbase.it/cloudbase-init/
2. Use the default settings, and do not run sysprep at the end of the install.
3. Under C:Program Files\Cloudbase Solutions\Cloudbase-Initconf, edit the cloudbase-init.conf file, referring to the sample configuration below. If the image will be sysprepped, edit cloudbase-init-unattend.conf and unattend.xml as well.

Note: Sample configurations only, user configurations may vary.

coucloudbase-init.conf

```
[DEFAULT]
# username=Admin
# groups=Administrators
# inject_user_password=true
inject_user_password=false
first_logon_behaviour=no
config_drive_raw_hhd=true
config_drive_cdrom=true
config_drive_vfat=true
bsdtar_path=C:\Program Files\Cloudbase Solutions\Cloudbase-Init\bin\bsdtar.exe
```
mtools_path=C:\Program Files\Cloudbase Solutions\Cloudbase-Init\bin\nverbose=true
default_log_levels=comtypes=INFO,suds=INFO,iso8601=WARN,requests=WARN
logging_serial_port_settings=
mtu_use_dhcp_config=true
local_script_path=C:\Program Files\Cloudbase Solutions\Cloudbase-Init\LocalScripts\n
# servers - tried in order until success
metadata_services=cloudbaseinit.metadata.services.configdrive.ConfigDriveService,
    cloudbaseinit.metadata.services.httpservice.HttpService,
    cloudbaseinit.metadata.services.ec2service.EC2Service,
    cloudbaseinit.metadata.services.maasservice.MaaSHttpService

# What plugins to execute.
plugins=cloudbaseinit.plugins.common.mtu.MTUPlugin,
    cloudbaseinit.plugins.windows.extendvolumes.ExtendVolumesPlugin,
    cloudbaseinit.plugins.common.userdata.UserDataPlugin,
    cloudbaseinit.plugins.common.networkconfig.NetworkConfigPlugin

# disabled plugins
# cloudbaseinit.plugins.common.sethostname.SetHostNamePlugin
# cloudbaseinit.plugins.windows.createuser.CreateUserPlugin
# cloudbaseinit.plugins.windows.setuserpassword.SetUserPasswordPlugin
# cloudbaseinit.plugins.common.networkconfig.NetworkConfigPlugin
# cloudbaseinit.plugins.common.sshpublickeys.SetUserSSHPublicKeysPlugin
# cloudbaseinit.plugins.windows.winrmlistener.ConfigWinRMListenerPlugin
# cloudbaseinit.plugins.windows.licensing.WindowsLicensingPlugin
# cloudbaseinit.plugins.windows.ntpclient.NTPClientPlugin
# cloudbaseinit.plugins.common.userdata.UserDataPlugin

# Miscellaneous.
allow_reboot=false  # allow the service to reboot the system
# stop_service_on_exit=false

### cloudbase-init-unattend.conf

```ini
[DEFAULT]
username=Admin
groups=Administrators
inject_user_password=true
config_drive_raw_hhd=true
config_drive_cdrom=true
config_drive_vfat=true
bsdtar_path=C:\Program Files\Cloudbase Solutions\Cloudbase-Init\bin\bsdtar.exe
mtools_path=C:\Program Files\Cloudbase Solutions\Cloudbase-Init\bin\nverbose=true
default_log_levels=comtypes=INFO,suds=INFO,iso8601=WARN,requests=WARN
logging_serial_port_settings=
mtu_use_dhcp_config=true
```

(continues on next page)
ntp_use_dhcp_config=true
local_scripts_path=C:\Program Files\Cloudbase Solutions\Cloudbase-Init\LocalScripts\
metadata_services=cloudbaseinit.metadata.services.configdrive.ConfigDriveService,
cloudbaseinit.metadata.services.httpservice.HttpService,cloudbaseinit.metadata.services.ec2service.EC2Service,cloudbaseinit.metadata.services.maasservice.
MaasHttpService
plugins=cloudbaseinit.plugins.common.mtu.MTUPlugin,cloudbaseinit.plugins.common.usethostname.SetHostNamePlugin,cloudbaseinit.plugins.windows.extendvolumes.
allow_reboot=false
stop_service_on_exit=false
check_latest_version=false

unattend.xml

<?xml version="1.0" encoding="utf-8"?>
<unattend xmlns="urn:schemas-microsoft-com:unattend">
  <settings pass="generalize">
      <SkipRearm>1</SkipRearm></component>
      <PersistAllDeviceInstalls>false</PersistAllDeviceInstalls>
      <DoNotCleanUpNonPresentDevices>false</DoNotCleanUpNonPresentDevices>
    </component>
  </settings>
  <settings pass="oobeSystem">
      <InputLocale>en-US</InputLocale>
      <SystemLocale>en-US</SystemLocale>
      <UILanguage>en-US</UILanguage>
      <UserLocale>en-US</UserLocale>
    </component>
  </settings>
    <OOBE>
      <HideEULAPage>true</HideEULAPage>
      <ProtectYourPC>1</ProtectYourPC>
      <NetworkLocation>Home</NetworkLocation>
      <HideWirelessSetupInOOBE>true</HideWirelessSetupInOOBE>
    </OOBE>
    <TimeZone>UTC</TimeZone>
    <UserAccounts>
      <AdministratorPassword>
        <Value>administratorPassword</Value>
      </AdministratorPassword>
    </UserAccounts>
  </component>
</unattend>
4. Save and changes to cloudbase-init.conf, cloudbase-init-unattend.conf, and unattend.xml files.

**Note:** The Administrator password is being set in the unattend.xml file to be set upon boot after sysprep. This is not required if sysprep is not being used, and may not be preferred. Other mechanisms such as requiring the Administrator password to be reset or randomly generated can be used. Morpheus can also securely via the user_data file at provision time.

5. To run a sysprep using the cloudbase-init configuration, run the following in a command prompt:

```bash
cd C:\Program Files\Cloudbase Solutions\Cloudbase-Init\conf
C:\Windows\System32\sysprep\sysprep.exe /generalize /oobe /unattend:Unattend.xml
```

6. Sysprep will run and Windows will be powered down. The VM can now be converted to an Image/Blueprint and synced or uploaded to Morpheus and used for Provisioning.

**Important:** Upon upload or sync of the Virtual Image, ensure cloudbase enable is checked in the Virtual Image config, and the existing or unattend.xml credentials when using sysprep are populated.

### 10.3.26 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 Administration -> Provisioning -> 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.

```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 $iface_name
sudo mv /etc/sysconfig/network-scripts/$iface_file /etc/sysconfig/network-scripts/
     $iface_name
sudo sed -i -e "s/$iface_name/eth0/" /etc/sysconfig/network-scripts/ifcfg-eth0
echo NM_CONTROLLED="no" >> /etc/sysconfig/network-scripts/ifcfg-eth0
```

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.
Morpheus Documentation, Release 3.6.1

```bash
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).

```bash
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.
## 10.3.27 Morpheus Cloud Capability Coverage

Table 2: 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>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>

## 10.4 Containers

### 10.4.1 Docker

**Overview**

Morpheus can provision Docker Hosts into any cloud, convert existing Hosts to Docker Hosts, or even make itself a Docker Host.

**Add a Docker Host to any cloud:**

1. Navigate to Infrastructure -> Hosts
2. Click the `+CONTAINER HOST` button
3. Select a container host type
4. Select a Group
5. Enter the following:
   • Name
   • Description
   • Visibility
   • Select a Cloud
   • Enter tags (optional)

Then click NEXT.

6. Configure the host options

Select a Service Plan (Volume, Memory and CPU count fields may not be shown if selected service plan does not have custom options enabled).

   • Add and set size the volumes
   • Set memory size
   • Set the CPU count
   • Select a network

Optionally configure the following:

   • OS username
   • OS password
   • Domain name
   • Hostname (default is the name previously provided for the container host)
Then click the NEXT button

7. Optionally add any Automation Workflows and configure for Backups.

8. Review and click Complete to save
Your new container host will begin provisioning, and soon be running and ready for containers.

**Add an existing Docker Host**

Morpheus can manage and inventory existing/brownfield Docker Hosts by using the *Manual Docker Host* option.

**Note:** Adding a Docker Host that was previously managed by another Morpheus Appliance will disable management of the host on that Appliance as the Morpheus Agent settings will be reconfigured.

**Note:** *Container Mode* on the Cloud settings where the Host is being added must be set to Morpheus for non-Kubernetes/Swarm hosts.

1. Navigate to Infrastructure -> Hosts
2. Select +*CONTAINER HOST* button
3. Select *Manual Docker Host*
4. In the CREATE HOST Wizard, enter the following:
   
   **GROUP**
   
   **GROUP** Select the Group this Host will be available for
   
   Select *NEXT*
   
   NAME
CLOUD  Select the Cloud the Host will be assigned to
NAME  Enter name for the Docker Host in Morpheus
DESCRIPTION  Enter optional description for the Docker Host
VISIBILITY  Select Tenant Visibility
TAGS  Add optional Morpheus tags (these are not meta-data tags)
Select NEXT

CONFIGURE

SSH HOST  Enter IP or resolvable hostname of the target host
SSH USER  Enter existing username on the target host
SSH PASSWORD  Enter password for SSH User
PUBLIC KEY  For key auth (recommended), copy and add the displayed Public Key to the authorized_keys file on the target host.

PLAN  Default Manual
LVM ENABLED?  Deselect if target host is not LVM enabled (required when using Morpheus provided docker images)
DATA VOLUME  Enter path of the target data volume on the target host
SOFTWARE RAID?  Enable for software RAID (disabled by default)
NET INTERFACE  Enter network interface name of target host’s target network
Select NEXT

AUTOMATION

POST PROVISION  Select a workflow to execute after Host is added (optional).
Select NEXT

REVIEW  Review settings and select COMPLETE to add the Manual Docker Host.

Your new container host will begin provisioning, and soon be running and ready for containers.

Note:  Existing containers will be inventoried after the Hosts is successfully added.

10.4.2 Kubernetes

Overview

The Kubernetes Cloud type allow users to inventory and provision to existing Kubernetes clusters. New Kubernetes clusters can also be provisioning using Docker mode setting in clouds and provisioning new Docker hosts.

Add Kubernetes Cloud

1. Navigate to Infrastructure -> Clouds
2. Select + CREATE CLOUD, select Kubernetes Cloud, and then click Next.
3. Enter the following into the Create Cloud modal:
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.
API URL  Kubernetes API URL
API TOKEN  Kubernetes User API Token
Inventory Existing Instances  If enabled, existing Containers will be inventoried and appear in the Containers tab for the Kubernetes Cloud.

4. Save Changes

Create Kubernetes Cluster

Kubernetes Clusters can be provisioned into any Cloud Type by setting the CONTAINER MODE to Kubernetes in the Advanced Settings of a Cloud.

Important: The CONTAINER MODE must be set prior to provisioning any Docker Hosts. Once Docker Hosts exist in a Cloud, the CONTAINER MODE setting cannot be changed.

Once the CONTAINER MODE is set on a Cloud, a Kubernetes Cluster can be created by selecting + CONTAINER HOST -> Kubernetes Master and then Kubernetes Worker from Infrastructure -> Hosts or Infrastructure -> Clouds -> select Cloud -> Hosts.

Important: For the Kubernetes Cluster to be successfully created, the Kubernetes Master must finish provisioning before the worker(s) are created. Do not start provisioning a worker in the cluster until the Master is completed.

10.4.3 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
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.

10.5 Deployment

10.5.1 Git

Authentication

Add a private Github or Git Repository, an SSH Key pair must be added to Morpheus and the public key added to Github or the Git Repository for authentication.

To add a Key Pair to Morpheus:

1. Generate an SSH Key Pair, or use an existing SSH Key Pair.
2. Navigate to Infrastructure -> Key Pairs

#. Select + ADD # Enter both the Public and Private Private

10.6 DNS

10.6.1 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.
10.6.2 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

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
   - USERNAME DNS provider username
   - PASSWORD DNS provider user password
   - ZONE (Optional) Enter a dns zone to limit scope
   - 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.
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.

10.6.3 Power DNS

Overview

Morpheus integrates directly with Power DNS to automatically create DNS entries for Instances provisioned to a configured Cloud or Group. Morpheus also syncs in Power DNS Domains for easy selection while provisioning, or setting as the default Domain on a Cloud or Network.

Add Power DNS Integration

Power 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  Power DNS
   - NAME  Name for the Integration in Morpheus
   - API HOST  URL of Power DNS API. Example: http://10.30.20.10:8081
   - Token  Power DNS API Token
   - Version  Power DNS API Version
4. Once saved the Integration will be added and visible in both Administration -> Integrations and Infrastructure -> Networks -> Services
Domains

Once the integration is added, Power 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 Power 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.

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.

10.7 Identity Management

10.7.1 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.

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.
7. 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.
10.7.2 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.

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>Type</th>
<th>SAML [Beta]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Yes</td>
</tr>
<tr>
<td>Name</td>
<td>SAML</td>
</tr>
<tr>
<td>Description</td>
<td>onelogin SAML</td>
</tr>
</tbody>
</table>

### SAML Configuration

- **Login Redirect URL**: https://morpheusdata-dev.onelogin.com/trust/saml2/http-post
- **Logout POST URL**: https://morpheusdata-dev.onelogin.com/trust/saml2/http-post
- **Signing Public Key**: MIIEFzCCAv+gAwIBAgIuayYdMuoXBTGcalAARanxhrJwytQwDQYJKoZIhvcNAQEF

### 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
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
10.7.3 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 inputing the Identifier (Entity ID) and Reply URL (Assertion Consumer Service URL) in the Azure SSO configuration before it provides the Endpoints and Certificate neccessary 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 (external login) 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 in the Apps left hand nav, 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 SSO config step 3, select user.userprincipalname as the User Identifier.
4. Also in step 3, select “View and edit all other user attributes” the copy the NAMESPACE url for the following:

Name givenname Value: user.givenname Namespace: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
5. In Azure SSO config step 4, 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 at (not related to Morpheus).

7. In Azure SSO config step 5, 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 POST 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> This will be used for the SIGNING PUBLIC KEY in the Morpheus Identity Source Integration settings

   Example Key (the key has been altered and is not valid):

   MIICBECCAdigAwIBAgIQEOZXlNx5wY9Dc60wlsKEMzANBgkqhkiG9w0BAQsFADA0MTIwMAYDVQQDEyNaWNyb3NvZnQgQXp1cmUgRmVkZXJhdGVkIFNTTyBDZX...TlaMDQxMjAwBgNVBAMTTU1pY3Jvc29mdCBBenVyZSBGZWRlcmF0ZWQgU1NPIENlcnRpZmljYXRlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2k/V6GcBpRkoxJd0DLbhubwd0kp651D9Ii5PUY2ohBHvrFAy3SZ204mxoH7LWv3oNrqxaNAksbYF6p9OkKNF/…pqp3qw+nYfTXzSxY6f1Sp64jfs2Ds1jSVjD7upMItKPeOCRmeBUcnebzwKqFB0714VF5qoEJvftT7Wpr4VVoM0L…pH6xzQVRz0GZ7po19V1QJJbJqhLm4uLjWT9VU21Yqdi0NdtK7Qthzo4J0ZFdUG6qFFTFKpVnOAMBx1M4JWxf1gzd…y56+kSRSR87X0cVvTftbHymQnD0f0qKrgpMK7LtmseWqce7rKX7nTCenZ2nBE0CFLDBVH4QEzMrAznEqDjns9nJZBN

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 above and populate the following:

   - **LOGIN REDIRECT URL** Add the SAML Single Sign-On Service URL copied from Azure SSO config.
   - **LOGOUT POST URL** Add the Sign-Out URL copied from Azure SSO config.
   - **SIGNING PUBLIC KEY** (uncheck “Do not validate SAMLResponse signatures” if desired) Add the SAML XML Metadata key copied from Azure SSO config.
   - **GIVEN NAME ATTRIBUTE NAME** Enter the givenname 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
   - **SURNAME ATTRIBUTE NAME** Enter the emailaddress 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 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.

**ROLE ATTRIBUTE NAME** Enter http://schemas.microsoft.com/ws/2008/06/identity/claims/groups for Azure AD SSO

**REQUIRED ROLE ATTRIBUTE VALUE** 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.

**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

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.

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 below LOGIN WITH with the name of the Identity Source Integration as the button title. Example: AZURE AD. Another button titled “USERNAME AND PASSWORD” is also added in place of the standard Username and Password fields.

- **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.** If no local users other than the System Admin have been created, “USERNAME AND PASSWORD” option will not be displayed, only the SAML option.

10.7.4 OneLogin

Adding OneLogin Identity Source Integration

1. Navigate to Administration -> Tenants

10.7. Identity Management
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.
   
   6. 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.

### 10.8 ITSM

#### 10.8.1 ServiceNow

**Add Service Now Integration**

1. Navigate to Administration -> Integrations
2. Select + NEW INTEGRATION
3. Select ServiceNow from the TYPE dropdown.

4. Add the following:
   - **NAME** Name of the Integration in Morpheus.
   - **ENABLED** Leave checked to enable the Integration.
   - **HOST** Url of the ServiceNow Instance ex: https://your.instance.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** Above ServiceNow user’s password

5. Save Changes

**Important:** When using ServiceNow version London, the following steps must also be performed. An administrator needs to modify the access permissions on the ‘catalog_script_client’ and ‘io_set_item’ tables. This is performed by ensuring the ‘Can create’, ‘Can update’, and ‘Can Delete’ are checked under Application Access for ‘All application scopes’ for these tables.

**ServiceNow Approval Policies**

**Add ServiceNow Provision Approval Policy to a Cloud**

**Note:** Any Instance provisioned into a Cloud with an Approval Policy enabled will require approval.

To add a ServiceNow Approval policy to a Cloud:

1. Navigate to Infrastructure -> Clouds
2. Select a Cloud by clicking on the Cloud Name link
3. Select the POLICIES tab
4. Select + 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 workflow in ServiceNow. Note 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 sub-tenant, type the name of the tenant(s) and select the Tenant(s) from the 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 require 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 link
3. Select the POLICIES tab
4. Select + 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 workflow in ServiceNow. Note 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 sub-tenant, type the name of the tenant(s) and select the Tenant(s) from the 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 in 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 Internal Approvals.

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 5 minutes of being approved in ServiceNow.

**ServiceNow Service Catalog Integration**

The following is a guide to installing the Morpheus ServiceNow application.

**Important:** A valid SSL Certificate is required on the Morpheus Appliance for the ServiceNow plugin to be able to communicate with the appliance.
ServiceNow Configuration

1. Install the Morpheus Application from the ServiceNow store
2. Navigate to Morpheus Catalog -> Properties
3. Set the following properties:
   Morpheus Appliance Endpoint  The full url to your Morpheus appliance
   Password  Password of the Morpheus Administrator
   Username  Username of the Morpheus Administrator
4. Create a new User
5. Assign the following roles to the user:
   • x_moda_morpheus_ca.integration
   • catalog_admin
   • itil
   • rest_service

Important: When using ServiceNow version London, the following steps must also be performed. An administrator needs to modify the access permissions on the ‘catalog_script_client’ and ‘io_set_item’ tables. This is performed by ensuring the ‘Can create’, ‘Can update’, and ‘Can Delete’ are checked under Application Access for ‘All application scopes’ for these tables.

Morpheus Configuration

1. Navigate to Administration -> Integrations
2. Click + NEW INTEGRATION
3. Select ‘ServiceNow’ in the Type field
4. Fill in the Host, User and Password fields (using the User and Password created in the previous section)

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
### 10.8.2 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 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:

```json
{
    "Description":"Created from Morpheus by ${instance.createdByUsername} in ${zone.name}"
}
```

5. Save Changes

### 10.8.3 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>
<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%20Change</td>
</tr>
<tr>
<td>/api/arsys/v1/entry/CHG:Infrastructure%20Change</td>
<td>PUT</td>
<td>CHG:Infrastructure%20Change</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>DELETE</td>
<td>BMC.CORE:BMC_DiskDrive</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>DELETE</td>
<td>BMC.CORE:BMC_Memory</td>
</tr>
<tr>
<td>/api/cmdb/v1.0/instances/BMC.ASSET/BMC.CORE/BMC_Processor</td>
<td>POST</td>
<td>BMC.CORE:BMC_Processor</td>
</tr>
<tr>
<td>/api/cmdb/v1.0/instances/BMC.ASSET/BMC.CORE/BMC_Processor</td>
<td>PATCH</td>
<td>BMC.CORE:BMC_Processor</td>
</tr>
<tr>
<td>/api/cmdb/v1.0/instances/BMC.ASSET/BMC.CORE/BMC_Processor</td>
<td>DELETE</td>
<td>BMC.CORE:BMC_Processor</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:Processor</td>
<td>POST</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

10.9 Keys and Certificates

10.9.1 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

10.10 Load Balancers

10.10.1 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

10.10.2 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

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 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 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.

10.11 Logs

10.11.1 LogRhythm

Adding LogRhythm Integration

1. Navigate to Administration -> Logs
2. Expand the LogRhythm section
3. Enable the integration
4. Fill in the following:
   - Enabled  Enable the LogRhythm integration
   - Host  IP or Hostname of the LogRhythm server.
   - Port  Port configured to access the LogRhythm server.
5. SAVE
10.11.2 Splunk

Overview

The Morpheus Splunk Integration allows forwarding logs from managed Linux hosts and vm’s to a target Splunk listener by changing the rsyslogd config on linux vm’s to point to Splunk forwarders. The logs will be forwarded from the clients, not from the Morpheus Appliance.

Adding Splunk Integration

1. Add a syslog listener configuration in Splunk.
2. Navigate to Administration -> Logs
3. Expand the Splunk section
4. Enable the integration
5. Fill in the following:
   - **Enabled** Enable the Splunk integration
   - **Host** IP or Hostname of the Splunk server.
   - **Port** Port configured to access the Splunk server.
6. SAVE

Once added, syslogs from managed Linux hosts and vm’s will be forwards from the clients to the target Splunk listener.

10.11.3 Syslog

Adding Syslog Integration

1. Navigate to Administration -> Logs
2. Expand the Morpheus logging section
3. Add the Syslog forwarding rules
4. Select **QUICK ADD**

10.12 Monitoring

10.12.1 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

<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>

### 10.12.2 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 > 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.

### 10.12.3 NewRelic

**Configuring The NewRelic Integration**

1. Navigate to Administration > 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.

### 10.13 Networking

#### 10.13.1 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

1. Navigate to Infrastructure - Network - Services
2. Select + ADD -> IPAM -> Infoblox
3. Enter the following:
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
USERNAME  Infoblox user username
PASSWORD  Infoblox user password
Disable SSL SNI Verification  Leave selected to disable SSL SNI Verification

NETWORK FILTER  Filter which networks are synced into Morpheus. Example: Network Filter: [ network_view=default&Building=work ]

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
4. Select **SAVE IPAM INTEGRATION**

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)

![Network Pool Screenshot]

- 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 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

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
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
NAME  Name for the record, such as Hostname
Type  A, AAAA, CNAME, MX, NS, PTR, SOA, or TXT
CONTENT  Content of the record, such as IP or A Record
TTL  Time To Live value

4. Select SAVE CHANGES

10.13.2 phpIPAM

Configuration

Configure phpIPAM API

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 - Services
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

10.13.3 NSX

Add NSX Integration

1. Navigate to INFRASTRUCTURE -> NETWORK
2. Select the SERVICES tab
3. Select Select + ADD -> VMWare NSX
4. 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.
5. 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.

Create NSX Transport Zone

1. Navigate to INFRASTRUCTURE -> NETWORK
2. Select the SERVICES tab
3. Select the name of NSX 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
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  d
   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
10.13.4 Bluecat

Overview

Morpheus integrates with Bluecat IPAM to scope pools to networks for Static IP assignment from Infoblox to your Morpheus instances.

Adding Bluecat to Morpheus

1. Navigate to Infrastructure > Network > Services
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

10.13. Networking
• 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

10.14 Service Discovery

10.14.1 Consul

Morpheus can integrate with Consul to automatically install the Consul Agent in Client Mode on Instances and configure communication with the Consul host.

Add Consul Integration

1. Navigate to Administration -> Integrations and select + New Integration
2. Select Integration Type Consul Service Registry
3. Populate the following fields:
   Name Name of the Consul Integration in Morpheus
   Enabled Enabled by default
   Consul Host IP or Url of the Consul Host
   Consul Http Port Http port of the Consul Host
   Username Consul Host User
   Password Consul Host User Password
   Datacenter ID Validator key for the organization
4. Save Changes

The added Consul Integration is now available for use in Morpheus, but must be scoped to a Cloud or Group to automatically install the Consul Agent while provisioning.

Scope Consul Integration to a Cloud

1. Navigate to Infrastructure -> Clouds
2. Edit the target Cloud
3. Expand the Advanced Options section
4. In the Service Registry dropdown, select the Consul Integration.
5. Save Changes

Scope Consul Integration to a Group

1. Navigate to Infrastructure -> Groups
2. Edit the target Group
3. Expand the Advanced Options section
4. In the Service Registry dropdown, select the Consul Integration.

5. Save Changes

And that’s it. After your integration is set up, all containers deployed within the Group or Cloud integrated will provision with the Consul Agent in Client Mode, gossiping to your Consul Server!

### 10.15 Storage

#### 10.15.1 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.

#### 10.15.2 AzureStorage

**To Add Azure Storage**

1. Navigate to Infrastructure -> Storage Hola
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
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 times 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, Files Shares and Storage Groups will be synced in.

**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** 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.

**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.
10.15.4 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*
   - **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.

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.

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.
10.16 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:

<table>
<thead>
<tr>
<th>Technology</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Private Cloud</strong></td>
<td></td>
</tr>
<tr>
<td>Azure Stack</td>
<td>GA</td>
</tr>
<tr>
<td>Microsoft Hyper-V</td>
<td>2012R2, 2016</td>
</tr>
<tr>
<td>Nutanix Acropolis</td>
<td>5.0 - 5.10&lt;br&gt;Note: In 5.5 - 5.7 if Prism Central is enabled, no actions that create images in Prism will function due to Prism Central Image Management.</td>
</tr>
<tr>
<td>Openstack</td>
<td>Juno, Kilo, Liberty, Mitaka, Newton, Ocata, Pike, Queens</td>
</tr>
<tr>
<td>vCloud Director</td>
<td>8.20, 9.1</td>
</tr>
<tr>
<td>VMware vCenter</td>
<td>5.5, 6.0, 6.5, 6.7</td>
</tr>
<tr>
<td>VMware ESXi</td>
<td>5.5, 6.0, 6.5, 6.7</td>
</tr>
<tr>
<td>VMware Fusion</td>
<td>8, 9, 10+</td>
</tr>
<tr>
<td>XenServer</td>
<td>7.0</td>
</tr>
<tr>
<td><strong>Monitoring</strong></td>
<td></td>
</tr>
<tr>
<td>App Dynamics</td>
<td>4.5.1</td>
</tr>
<tr>
<td><strong>Networking</strong></td>
<td></td>
</tr>
<tr>
<td>Cisco ACI</td>
<td>3.10</td>
</tr>
<tr>
<td>VMware NSX</td>
<td>-V</td>
</tr>
<tr>
<td><strong>Backups</strong></td>
<td></td>
</tr>
<tr>
<td>Veeam</td>
<td>9.5</td>
</tr>
<tr>
<td>Commvault</td>
<td>v11 sp 12</td>
</tr>
<tr>
<td>Rubrik</td>
<td>4.2</td>
</tr>
<tr>
<td><strong>Containers</strong></td>
<td></td>
</tr>
<tr>
<td>Docker</td>
<td>1.12.6</td>
</tr>
<tr>
<td>Kubernetes</td>
<td>1.11</td>
</tr>
<tr>
<td>Jenkins</td>
<td>1.64</td>
</tr>
<tr>
<td><strong>ITSM</strong></td>
<td></td>
</tr>
<tr>
<td>ServiceNow</td>
<td>Istanbul, Jakarta, Kingston, London</td>
</tr>
<tr>
<td><strong>Logging</strong></td>
<td></td>
</tr>
<tr>
<td>Splunk</td>
<td>7.10</td>
</tr>
</tbody>
</table>

If you have any specific requirements please contact support@morpheusdata.com
11.1 Common Ports & Requirements

The following chart is useful for troubleshooting Agent install, Static IP assignment, Remote Console connectivity, and Image transfers.
Table 1: Common Ports & Requirements

<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></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></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></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>WinRM</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Windows</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Appliance</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Node</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></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 (<strong>winrm quickconfig</strong>)</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 <strong>Admin -&gt; Provisioning</strong></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></td>
<td></td>
<td></td>
<td>5985</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 <strong>Admin -&gt; Provisioning</strong></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 <strong>Administration -&gt; Provisioning</strong> 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 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 <strong>Administration -&gt; Provisioning</strong></td>
</tr>
<tr>
<td>VMware Tools</td>
<td>All</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Chapter 11. Troubleshooting</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Network configured in Morpheus (Gateway, Primary and Secondary DNS, CIDR populated, DHCP disabled)</td>
</tr>
</tbody>
</table>
11.2 Morpheus Agent Install Troubleshooting

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 Admin -> Settings over 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 Admin -> 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.

11.2.1 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 (Admin -> 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.
• 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 Provisioning - 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 configure, 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 Provisioning -> 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 Provisioning -> 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 custom or synced image. Credentials can be entered on images in the Provisioning -> Virtual Images section.

**Cloud-Init agent install mode**

• Cloud-Init is configured in Admin -> Provisioning section

• Provisioned image/blueprint has Cloud-Init (linux) or Cloudbase-Init (windows) installed
11.2.2 Manually Installing a Morpheus Agent

While it should not be necessary to manually install an agent if the requirements are met, it is possible to manually install an agent on an instance. This can also be handy when troubleshooting an agent install.

**Linux**

1. In Morpheus, go to the VM’s host detail page in Infrastructure->Hosts->Virtual Machines you will see an API Key that is unique to that host.
2. As root user, run: (replacing ${} with the relevant information)
   ```bash
   curl -k -s "${opts.applianceUrl}api/server-script/agentInstall?apiKey=${opts.apiKey}" | bash
   ```
3. This will pull the Morpheus Agent install script from the Morpheus appliance and run it.
4. Once the agent is installed, run `morpheus-node-ctl reconfigure` to complete the manual process.

**Windows**

- The windows agent setup can be downloaded at [https://[morpheus-appliance-url]/msi/morpheus-agent/MorpheusAgentSetup.msi](https://[morpheus-appliance-url]/msi/morpheus-agent/MorpheusAgentSetup.msi)
- On the Morpheus appliance package the windows agent is located at `/var/opt/morpheus/package-repos/msi/morpheus-agent`
- WinRM, VMware Tools, or Cloudbase-Init can be used to install the agent from the Morpheus appliance
- The initial windows installer is `MorpheusAgentSetup.msi`
- Once the Windows agent is downloaded and installed with `MorpheusAgentSetup.msi` the agent is located and runs from `/Program Files x86/morpheus/morpheus Windows Agent`
- Logs can be viewed in the Event Viewer under Applications and Services Logs -> Morpheus Windows Agent

1. Replace the values for `$apiKey` and `$applianceUrl` in the script below.
2. Execute this script on the Windows box in Powershell.

```powershell
$apiKey = "add VM apiKey here"
$applianceUrl = "https://your_appliance_url.com/
$client.DownloadFile($applianceUrl + "msi/morpheus-agent/MorpheusAgentSetup.msi", "C:\Program Files (x86)\Common Files\MorpheusAgentSetup.msi")
Start-Sleep -Seconds 10
cd ${env:commonprogramfiles(x86)}
$serviceName = "Morpheus Windows Agent"
if{(Get-Service $serviceName -ErrorAction SilentlyContinue) { } Stop-Service -displayName $serviceName -ErrorAction SilentlyContinue
Stop-Process -Force -processname Morpheus* -ErrorAction SilentlyContinue
Start-Sleep -s 5
$serviceId = (get-wmiobject Win32_Product -Filter "Name = 'Morpheus Windows Agent'" | Format-Wide -Property IdentifyingNumber | Out-String).Trim()
cmd.exe /c "msiexec /x $serviceId /q"
}[Console]::Out.Flush()
[gc]::collect()
```

(continues on next page)
try {
Write-VolumeCache C
}
Catch {
}$MSIArguments = @{
"/i"
"MorpheusAgentSetup.msi"
"/qn"
"/norestart"
"/i-v"
"morpheus_install.log"
"apiKey=$apiKey"
"host=$applianceUrl"
"username='.".\LocalSystem'"
"vmMode=\"true\"
"logLevel=\"1\"
}$installResults = Start-Process msiexec.exe -Verb runAs -Wait -ArgumentList $MSIArguments
[Console]::Out.Flush()
[gc]::collect()
try {
Write-VolumeCache C
}
Catch {
start-sleep -s 10
$attempts = 0
Do {
try {
Get-Service $serviceName -ea silentlycontinue -ErrorVariable err
if ([$string]::isNullOrEmpty($err)) {
    Break
} else {
    start-sleep -s 10
    $attempts++
}
} Catch {
    start-sleep -s 10
    $attempts++
}
}
While ($attempts -ne 6)
Set-Service $serviceName -startuptype "automatic"
$service = Get-WmiObject -Class Win32_Service -Filter "Name='$serviceName'"
if ($service -And $service.State -ne "Running") {Restart-Service -displayname $serviceName}
exit $installResults.ExitCode

3. If the agent doesn’t install, logs can be found in the morpheus_install.log file located at C:\Program Files (x86)\Common Files\
11.2.3 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

You can use the following to uninstall the linux agent:

```
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 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 pkill runsv
sudo pkill runsvdir
sudo pkill morphd
sudo usermod -l morpheus-old morpheus-node
```

### 11.2.4 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.

---

### 11.3 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.
11.3.1 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.

11.3.2 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.

### 11.3.3 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.

### 11.3.4 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 restart 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 connection will resemble:

```
guacd[24725]: INFO: Creating new client for protocol "ssh"
guacd[24725]: INFO: Connection ID is "$24f67856-f050-4a17-83eb-9101g0cd8869"
guacd[24743]: INFO: Current locale does not use UTF-8. Some characters may not render correctly.
guacd[24743]: INFO: User "@63102f19-eff4-412e-b1f9-718405f55782" joined connection "$24f67856-f050-4a17-83eb-9101g0cd8869" (1 users now present)
guacd[24743]: INFO: Auth key successfully imported.
guacd[24743]: INFO: SSH connection successfully established.
```

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`

11.4 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.

Instances are managed resources that may have one or multiple Virtual Machines associated. Since the vm’s in the Instance are managed by `morpheus`, deleting an Instance a with 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 records in Morpheus need to be removed.

11.4.1 Deleting an Instance without deleting Infrastructure

It is not possible to delete and Instance from the Provisioning section without removing the associated Infrastructure/VM’s. 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’s name in the Virtual Machines section in the Instances details section, or by navigating to `Infrastructure - Hosts - 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 s

11.4.2 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 - Hosts - 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.

### 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 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
   ```
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:

   ```bash
   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:

   ```bash
   mysql -u morpheus -p -h 127.0.0.1 morpheus
   ```

   At the prompt, enter the `mysql` password from the `application.yml`

   Then run:

   ```bash
   DELETE FROM DATABASECHANGELOGLOCK;
   ```

   Then restart `morpheus-ui`:

   ```bash
   sudo morpheus-ctl restart morpheus-ui
   ```

   If the restart times out, run:

   ```bash
   sudo morpheus-ctl kill morpheus-ui
   sudo morpheus-ctl start morpheus-ui
   ```

11.7 Unable to Provision a Custom Image

Prior to provisioning an custom image, the image must be configured in the Provisioning -> 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

### 11.8 Restart a Morpheus Installation

If the initial reconfigure is stopped or your installation is damaged beyond reconfiguring again, it may be necessary to start over.

On the Morpheus appliance:

1. Run `morpheus-ctl cleanse`
2. Remove the Morpheus package
   - deb: `dpkg --purge morpheus-appliance...` using the appropriate package name.
   - rpm: `rpm -e (morpheus-appliance...)` using the appropriate package name.
3. Then Run
   ```
   rm -rf /etc/morpheus
   rm -rf /var/opt/morpheus
   rm -rf /var/run/morpheus
   rm -rf /var/log/morpheus
   rm -rf /opt/morpheus
   ```
4. Re-install Morpheus
   
   If the elasticsearch cluster is unhealthy and needs purged, run:
   ```
   sudo morpheus-ctl stop elasticsearch
   sudo rm -rf /var/opt/morpheus/elasticsearch/data/morpheus
   sudo morpheus-ctl reconfigure
   ```
   If elasticsearch does not restart during reconfigure:
   ```
   sudo morpheus-ctl start elasticsearch
   ```

### 11.9 Variables

The following are the map structures passed to scripts and templates during provisioning inside of a `<%= %>` block. Variables can also be passed in Naming Policies using `$({ } )` block.
Important: Variables are case sensitive

PowerShell Example: $app_id = "<%= instance.metadata.app_id %>">

Bash Example: HOSTNAME="<%= container.server.hostname %>">

Instance Naming Policy example: ${userInitials}-${cloudCode}-${platform == 'windows' ? 'W' : 'L'}-${sequence}

Tip: Variables can be extremely useful when utilized in the environment tab, metadata, and environment variables.

Note: customOptions are user defined as Option Types or Option Lists in custom Library items.

cypher: <%=cypher.read('secret/hello')%>
customOptions: <%=customOptions.fieldName%>
evars: <%=evars%>
instance.metadata: <%=instance.metadata%>
instance.instanceTypeName: <%=instance.instanceTypeName%>
instance.instanceTypeCode: <%=instance.instanceTypeCode%>
instance.provisionType: <%=instance.provisionType%>
instance.instanceVersion: <%=instance.instanceVersion%>
instance.plan: <%=instance.plan%>
instance.name: <%=instance.name%>
instance.displayName: <%=instance.displayName%>
instance.description: <%=instance.description%>
instance.environmentPrefix: <%=instance.environmentPrefix%>
instance.hostname: <%=instance.hostname%>
instance.domainName: <%=instance.domainName%>
instance.firewallEnabled: <%=instance.firewallEnabled%>
instance.status: <%=instance.status%>
instance.userStatus: <%=instance.userStatus%>
instance.networkLevel: <%=instance.networkLevel%>
instance.instanceLevel: <%=instance.instanceLevel%>
instance.deployGroup: <%=instance.deployGroup%>
instance.instanceContext: <%=instance.instanceContext%>
instance.autoScale: <%=instance.autoScale%>
instance.statusMessage: <%=instance.statusMessage%>
instance.expireDate: <%=instance.expireDate%>
instance.tags: <%=instance.tags%>
instance.storage: <%=instance.storage%>
instance.memory: <%=instance.memory%>
instance.cores: <%=instance.cores%>
instance.configId: <%=instance.configId%>
instance.configGroupId: <%=instance.configGroupId%>
instance.configRole: <%=instance.configRole%>
instance.containers[0]: <%=instance.containers[0].containerTypeName%>
instance.createdBYUsername: <%=instance.createdBYUsername%>
instance.createdByEmail: <%=instance.createdByEmail%>
instance.createdBYFirstName: <%=instance.createdBYFirstName%>
instance.createdBYLastName: <%=instance.createdBYLastName%>

(continues on next page)
instance.createdById: <%=instance.createdById%>
container.containerTypeName: <%=container.containerTypeName%>
container.containerTypeCode: <%=container.containerTypeCode%>
container.containerTypeShortName: <%=container.containerTypeShortName%>
container.provisionType: <%=container.provisionType%>
container.dataPath: <%=container.dataPath%>
container.logsPath: <%=container.logsPath%>
container.configPath: <%=container.configPath%>
container.planCode: <%=container.planCode%>
container.dateCreated: <%=container.dateCreated%>
container.status: <%=container.status%>
container.environmentPrefix: <%=container.environmentPrefix%>
container.version: <%=container.version%>
container.image: <%=container.image%>
container.internalHostname: <%=container.internalHostname%>
container.hostname: <%=container.hostname%>
container.domainName: <%=container.domainName%>
container.storage: <%=container.storage%>
container.memory: <%=container.memory%>
container.cores: <%=container.cores%>
container.internalIp: <%=container.internalIp%>
container.externalIp: <%=container.externalIp%>
container.sshHost: <%=container.sshHost%>
container.hostMountPoint: <%=container.hostMountPoint%>
container.configId: <%=container.configId%>
container.configGroup: <%=container.configGroup%>
container.configRole: <%=container.configRole%>
container.serverId: <%=container.serverId%>
container.server: <%=container.server.serverTypeName%>
server.serverTypeName: <%=server.serverTypeName%>
server.serverTypeCode: <%=server.serverTypeCode%>
server.parentServerId: <%=server.parentServerId%>
server.plan: <%=server.plan%>
server.visibility: <%=server.visibility%>
server.osTypeCode: <%=server.osTypeCode%>
server.sourceImageId: <%=server.sourceImageId%>
server.name: <%=server.name%>
server.displayName: <%=server.displayName%>
server.internalName: <%=server.internalName%>
server.category: <%=server.category%>
server.description: <%=server.description%>
server.internalId: <%=server.internalId%>
server.externalId: <%=server.externalId%>
server.platform: <%=server.platform%>
server.platformVersion: <%=server.platformVersion%>
server.agentVersion: <%=server.agentVersion%>
server.nodePackageVersion: <%=server.nodePackageVersion%>
server.sshHost: <%=server.sshHost%>
server.sshPort: <%=server.sshPort%>
server.sshUsername: <%=server.sshUsername%>
server.consoleType: <%=server.consoleType%>
server.consoleHost: <%=server.consoleHost%>
server.consolePort: <%=server.consolePort%>
server.consoleUsername: <%=server.consoleUsername%>
server.internalSshUsername: <%=server.internalSshUsername%>
server.internalIp: <%=server.internalIp%>
server.externalIp: <%=server.externalIp%>
server.osDevice: <%=server.osDevice%>
server.dataDevice: <%=server.dataDevice%>
server.lvmEnabled: <%=server.lvmEnabled%>
server.apiKey: <%=server.apiKey%>
server.softwareRaid: <%=server.softwareRaid%>
server.status: <%=server.status%>
server.powerState: <%=server.powerState%>
server.dateCreated: <%=server.dateCreated%>
server.lastAgentUpdate: <%=server.lastAgentUpdate%>
server.serverType: <%=server.serverType%>
server.osType: <%=server.osType%>
server.commType: <%=server.commType%>
server.managed: <%=server.managed%>
server.agentInstalled: <%=server.agentInstalled%>
server.toolsInstalled: <%=server.toolsInstalled%>
server.hostname: <%=server.hostname%>
server.domainName: <%=server.domainName%>
server.statusMessage: <%=server.statusMessage%>
server.maxStorage: <%=server.maxStorage%>
server.maxMemory: <%=server.maxMemory%>
server.maxCores: <%=server.maxCores%>
server.macAddress: <%=server.macAddress%>
server.serverVendor: <%=server.serverVendor%>
server.serverModel: <%=server.serverModel%>
server.serialNumber: <%=server.serialNumber%>
server.tags: <%=server.tags%>
server.configId: <%=server.configId%>
server.configGroup: <%=server.configGroup%>
server.configRole: <%=server.configRole%>
task.results (using task code): <%=results.taskCode%>
task.results (using task name): <%=results["Task Name"]%>
task.results.value: <%=results.taskCode.key%>
zone.name: <%=zone.name%>
zone.code: <%=zone.code%>
zone.location: <%=zone.location%>
zone.cloudTypeName: <%=zone.cloudTypeName%>
zone.cloudTypeCode: <%=zone.cloudTypeCode%>
zone.domainName: <%=zone.domainName%>
zone.scalePriority: <%=zone.scalePriority%>
zone.firewallEnabled: <%=zone.firewallEnabled%>
zone.regionCode: <%=zone.regionCode%>
zone.agentMode: <%=zone.agentMode%>
zone.datacenterId: <%=zone.datacenterId%>
group.code: <%=group.code%>
group.name: <%=group.name%>
group.location: <%=group.location%>
group.datacenterId: <%=group.datacenterId%

instance {
    instanceTypeName,
    instanceTypeCode,
    provisionType,
    instanceVersion,
    tenantSubdomain,
    plan,
    name,
displayName,
description,
environmentPrefix,
hostname,
domainName,
firewallEnabled,
status,
userStatus,
networkLevel,
instanceLevel,
deployGroup,
instanceContext,
autoScale,
statusMessage,
expireDate,
tags,
storage,
memory,
cores,
configId,
configGroup,
configRole
containers:[],
metadata:[],
evars:[]
}

container {
    containerTypeName,
    containerTypeCode,
    containerTypeShortName,
    provisionType,
    dataPath,
    logsPath,
    configPath,
    planCode,
    dateCreated,
    status,
    environmentPrefix,
    version,
    image,
    internalHostname,
    hostname,
    domainName,
    storage,
    memory,
    cores,
    internalIp,
    externalIp,
    sshHost,
    hostMountPoint,
    configId,
    configGroup,
    configRole,
    serverId,
    server:
}
server {
    serverTypeName,
    serverTypeCode,
    parentServerId,
    plan,
    visibility,
    osTypeCode,
    sourceImageId,
    name,
    displayName,
    internaName,
    category,
    description,
    internaId,
    externaId,
    platform,
    platformVersion,
    agentVersion,
    nodePackageVersion,
    sshHost,
    sshPort,
    sshUsername,
    consoleType,
    consoleHost,
    consolePort,
    consoleUsername,
    internaSshUsername,
    internaIp,
    externaIp,
    osDevice,
    dataDevice,
    lvmEnabled,
    apiKey,
    softwareRaid,
    status,
    powerState,
    dateCreated,
    lastAgentUpdate,
    serverType,
    osType,
    commType,
    managed,
    agentInstalled,
    toolsInstalled,
    hostname,
    domainName,
    statusMessage,
    maxStorage,
    maxMemory,
    maxCores,
    macAddress,
    serverVendor,
    serverModel,
    serialNumber,
    tags,
    configId,
    configGroup,
(continues on next page)
configRole
volumes {
  name
  id
deviceName
maxStorage
unitNumber
displayOrder
rootVolume
}
}
zone {
  name,
code,
location,
cloudTypeName,
cloudTypeCode,
domainName,
scalePriority,
firewallEnabled,
regionCode,
agentMode,
datacenterId
}
group {
  code,
  name,
  location,
datacenterId
}
customOptions {
  customOptions.fieldName
}

11.10 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:

curl -XDELETE http://localhost:9200/*
morpheus-ctl restart elasticsearch
morpheus-ctl restart morpheus-ui
Another option is:

```
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

```
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

### 11.11 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

### 11.12 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
11.13 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 but certain os’s or network conditions can prevent automated install. You can run `ansible --version` in the |morpheus appliance|, or in the Ansible integration details page (Administrati on -> Integrations -> Select Ansible Integration, or 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:**

    ```bash
    sudo apt-get install software-properties-common
    sudo apt-add-repository ppa:ansible/ansible
    sudo apt-get update
    sudo apt-get install ansible
    ```

    **CentOS:**

    ```bash
    sudo yum install epel-release
    sudo yum install ansible
    ```

    Then create the working Ansible directory for Morpheus:

    ```bash
    sudo mkdir /opt/morpheus/.ansible
    sudo chown morpheus-app:morpheus-app /opt/morpheus/.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 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.

- 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.
11.14 How to un-manage an Instance/VM/Host

11.14.1 Description

A managed VM (and associated Instance) needs to be unmanaged and returned to Discovered type.

11.14.2 Solution

Delete the record from the Infrastructure - Hosts (! 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.

11.14.3 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 - Hosts - 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:
Warning! Deleting this Host with "Remove Infrastructure" enabled will permanently delete it from the Cloud. To only delete the record but leave in the Cloud, uncheck "Remove from Infrastructure". If "Inventory Existing Instances" is enabled on the Cloud, the host will be re-synced as discovered.

- 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**

**Important:** If you have to type DELETE that means the Remove Infrastructure flag is selected and you are confirming deletion of the actual VM. Ensure Remove Infrastructure is UNCHECKED when you want to leave the VM intact!

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.
12.1 v3.6.1

Release date: 2/21/2019

12.1.1 New Features

- Ansible: **Built-in Cypher lookup plugin added.** "{{lookup('cypher', 'secret=secret/name')}}" can now be used for Cypher Secrets in Ansible playbooks natively.
- Ansible: Refresh info log added morphues-ui current log
- Ansible: Morpheus Agent Command Bus mode speed enhancements
- API/CLI: createdBy filter added for Instances, Apps and Hosts
- API/CLI: Instances: Improvements to DELETE for Instances and Apps. If an Instance or App delete is called and the instance status is still Provisioning, resizing, restarting or cloning the delete is not attempted and an error message is returned, unless force=true
- AWS: Costing setting added to advanced cloud config options. AWS Costing sync can now be set to “None”, “Costing”, or “Costing and Reservations”.
- Azure: Summary tab added to Azure Cloud detail pages

12.1.2 Built-in Cypher lookup plugin

A great feature with using Ansible and Morpheus together is the built in support for utilizing some of the services that Morpheus exposes for automation. v3.6.1 adds native support for using Cypher secrets in Ansible (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.

### 12.1.3 Fixes

- Ansible: Fix for automated Ansible install when Ansible integration is added to Morpheus.
- Ansible: Fix for execution User when Morpheus agent install is skipped
- Ansible: security fixes for when Morpheus agent is not installed
- Ansible: Updates and fixes for Morpheus Agent Command Bus mode
- Apps: Fix Delete App leaving instances stuck in removing status
- Archives: Fix for downloading large files from Archives service stopping at 1GB. Nginx restart required `sudo morpheus-ctl restart nginx`
- AWS: Cost Explorer Reservation API calls changed to Daily
- AWS: Fix for AWS sync updates for removed vpcs
- AWS: Fix for sync errors caused by missing permissionService
- Azure: Fix for “Daily Syncing” status displayed after changing sync to Full
- Backups: Fix for backup history migration `durationMillis` and `sizeInMb` issue when upgrading from 3.4 to 3.6
- F5: Fix for synced pool member association
- Instances: Fix for flashing Instance Type icon in Instance Detail pages
- Login: Fix for “Forgot Password” subtenant user email notifications
- Nutanix: Fix for provisioning Docker hosts using IP Pools
- Nutanix: Fix for provisioning Docker Hosts using Ubuntu 16 images
- Operations: Nav Dropdown Icon alignment updates
- VMware: Fix for maxStorage Service Plan filter issue
12.2 v3.6.0

Morpheus v3.6 promotes v3.5 to a LTS branch. v3.6.0 contains everything in 3.5.3, please refer to all 3.5 release notes when upgrading from the 3.4 LTS branch to v3.6.

Note: If upgrading from 3.5.2 or earlier, yum and msi agent package requests are now over port 443 instead of 80. 80 is still required for apt packages.

Important: If upgrading from 3.5.2 or earlier, nginx needs to be restarted after 3.5.3 upgrade with `morpheus-ctl restart nginx` to accommodate yum and msi agent installs over 443

Important: Amazon Cost & Reservations sync uses the AWS Cost Explorer API. Please be aware of any additional costs incurred from Amazon.

Note: Update to the latest morpheus-cli with `gem update morpheus-cli`

Release date: 2/9/19

12.2.1 New Features

- Agent: **New Morpheus Windows Agent Install modes**. Morpheus Windows Agent can now install via Guest Customizations or Cloudbase-Init.

- Agent: Morpheus Windows Agent updated to v1.4.4

- Ansible: **Ansible execution over command bus** added. Morpheus has removed the need for ssh or winrm for Ansible!

- Ansible: **Ansible verbose logging mode** added

- API & CLI: Mute and Unmute Monitoring Checks now available from CLI & API

- API & CLI: Billing Data now contains server ID & external ID

- Appliance: Check server agent TLS support for RabbitMQ connection added

- Apps: App Tiered provisioning timeouts raised to accommodate apps that require longer workload times (15+ hours)

- ARM Templates: Added support for conditional ‘if(…)’ statements

- Automation: Added Post Provision phase output to Instance history for Workflows.

- AWS: **Amazon Clouds can now be scoped to all VPCs** in a region instead of a single VPC per cloud.

- AWS: **Amazon Cost & Reservations sync**. Morpheus now syncs in AWS costs and EC2 Reservations from AWS.

- AWS: New Summary Tab added to AWS Cloud detail pages containing cost and EC2 Reservation statistics.

- Azure: Resource Pool creation and removal added

- Backups: Backup archives on failures are now automatically cleaned up
- **Clouds:** *Disable Clouds now filtered* in Instance, App, Host, Migration and Blueprint wizards
- **Clouds:** *Huawei Cloud integration added*
- **DISA Compliance:** sudoers.d via cloud-init no longer adds users with NOPASSWD flag
- **Google Cloud:** Windows support added
- **Google:** Multi-network support added for Google Instances
- **Infrastructure:** VMs & Hosts: Version and Layout selection added to Convert to Managed
- **Instances:** *Run Task Instance Action* added. Allows executing individual tasks on Instances
- **Instances:** *Long Instance and Host names now wrap* in list view
- **Isilon:** *NFS mount path for Isilon volumes* displayed in Isilon tab
- **KVM:** Import Image: Added ability to import a KVM virtual machine image from both a managed and unmanaged KVM cloud. Supports both CEPH and LVM
- **Policies:** *New User Group Creation Policy Type*. Automatically add User Groups via Global, Tenant, Group, Cloud and User Policies
- **Policies:** *New File Share Storage Quotas and Object Storage Quotas* policy types added.
- **Policies:** New Policy Icons
- **Remedy:** Remedy Integrations now support Approval Policies for Provisioning and Lifecycle extension Approvals in Remedy.
- **Remedy:** Tenant and User added to main asset
- **Rubrik:** SLA Domains added to instance detail backup tab and backup details
- **SCVMM:** Do not require cloud selection for SCVMM clouds
- **SCVMM:** Host Agent is now used for SCVMM communication instead of winrm
- **Storage Servers:** Tenancy Visibility setting added for Dell EMC Isilon and ECS Storage Servers
- **TerraForm:** *Apply State Action added to Terraform Apps*
- **TerraForm:** Apply App State wizard added to reapply Terraform App state
- **Terraform:** HCL4j parser updated to handle 100% coverage of terraform syntax formats
- **Usage:** Added usage tracking for changes to Discovered resource sizes for VM’s in VMware vCenter and Nutanix Cloud types
- **VMware:** *Keyboard layout selection added to VMware vCenter Clouds*

### 12.2.2 Highlights

**AWS:** *Amazon Costing & Reservations sync*

Morpheus now syncs in actual costs from AWS, including Month To Date, estimated spend, last months costs, broken down by service, including On-Demand and Reserved hours per EC2 Instance Type.

**Important:** Amazon Cost & Reservations sync uses the AWS Cost Explorer API. Please be aware of any additional costs incurred from Amazon.
Amazon Clouds can now be scoped to all VPCs

Morpheus v3.6.0 added the ability to choose all VPC’s in an AWS region when adding an Amazon cloud. VPS’s are listed in the Resources tab in an Amazon Cloud detail page and similar to other resource pools, a VPC has Group Access, Tenant Access, Service Plan Access, default and active configuration options. This allows users to add a single aws cloud per region and then carve up access across groups and tenants and limit which Service Plans/EC2 Instance Types can be access per VPC. Users with access to multiple VPC’s can choose target VPC at provision time.
Ansible execution over command bus

Morpheus has removed the need for ssh or winrm for Ansible! The new Ansible execution over command bus feature allows running ansible over the Morpheus agent command bus, removing the need for an ssh or winrm connection for Ansible, or any open incoming ports on the target host. The Morpheus Agent (which can be installed with no open incoming ports on the target vm/host as well) will pull and execute Ansible commands locally.
To enable Ansible execution over the Morpheus agent command bus, edit your Ansible integration and select “Use Morpheus Agent Command Bus.”

Ansible verbose logging mode

When using Ansible execution over the Morpheus Agent command bus, verbose debug logging can be enabled by editing an Ansible Integration. Along with the “Use Morpheus Agent Command Bus” flag, “Enable Verbose Logging” is a new setting on Ansible integration settings that will output debug level logs for Ansible execution, visible in the Instance history section by selecting the “i” bubble on an executed Ansible task.
File Share Storage Quotas

The new File Share Storage Quotas Policy type allows, you guessed it, setting Storage Quotas for File Shares.
To add, in Administration -> Policies add a new Policy, and select File Share Storage Quota.

Then set the Name, give it a good description, set the size in GB, and scope it Globally or to a User.

Object Storage Quotas

The new Object Storage Quotas Policy type allows, you guessed it, setting Storage Quotas for Object Stores.
To add, in Administration -> Policies add a new Policy, and select Object Storage Quota.

Then set the Name, give it a good description, set the size in GB, and scope it Globally or to a User.

Disable Clouds now filtered

Previously, deselecting “Enabled” in a Clouds configuration settings only disabled sync and greyed it out in the Clouds list view. Now disabled clouds are filtered out/hidden in Instance, App, Host, Migration and Blueprint wizards.

Note: If you disable a cloud to temporarily pause sync, be sure to re-enable it for provisioning.

Long Instance and Host names now wrap

Instance and Host list pages now wrap long Instance and Host names, allowing for viewing the entirety of a long Instance or Host name without having to select or hover.

Huawei Cloud integration added

Huawei Cloud now available as a Cloud integration in Morpheus v3.6.0.

NFS mount path for Isilon volumes

The path to the file share is now displayed on the Isilon tab to make it easier for users to know how to mount the share in a VM.
Morphus Documentation, Release 3.6.1

Mute and Unmute Monitoring Checks now available from CLI & API

Usage: morpheus monitor-checks mute [name]
Usage: morpheus monitor-groups mute [name]
Usage: morpheus monitor-apps mute [name]

Mute a check, check group, or monitoring app. This prevents it from creating new incidents.
[name] is required. This is the name or id of a check.
--disable can be passed to disable mute state instead, the same as unmute

Usage: morpheus monitor-checks mute-all
Usage: morpheus monitor-groups mute-all
Usage: morpheus monitor-apps mute-all

Mute all checks. This prevents the creation new incidents.
--disable can be passed to disable mute state instead, the same as unmute

Usage: morpheus monitor-incidents mute-all

Mute all incidents.

Usage: morpheus monitor-checks unmute [name]

Unmute a check.
[name] is required. This is the name or id of a check.
Morpheus Windows Agent Install modes

3.6.0 adds the ability to execute Windows Agent install script with vmware guest customizations or cloudbase-Init utilizing unattend.xml. Now, in addition to winrm and vmtools, morpheus can inject the agent install script into the unattend.xml, reducing vmware provision times and removing winrm/5985 requirement for agent install when using images configured with cloudbase-init.

**Note:** Agent Install mode must be set to “Cloud-init when available” on target cloud for cloudbase-init agent install.

New User Group Creation Policy Type

Automatically add User Groups via Global, Tenant, Group, Cloud and User Policies

**Note:** User groups can be configured in Administraiton-> Users- User Groups tab or in the CLI with user-groups add/update

Apply State Action added to Terraform Apps

New Apply State action brings up the new Apply App State wizard to re-apply state to TerraForm Apps.

Keyboard layout selection added to VMware vCenter Clouds

Keyboard layouts for Remote Console connections cannot be set in VMware vCenter cloud in the Cloud configuration.

12.2.3 Fixes & other updates

- Active Directory: Fix for user accounts locking during login because of perceived failed login attempts
- Administration: Fix for tenant delete issue when a master tenant service plan is assigned to the sub-tenant
- API/CLI: Fix for API processes history for appId query
- API/CLI: Fix for API/CLI network creation
- API/CLI: Fix for Create App not handling JSON parameters (description & site ID)
- API/CLI: Fix for creating a restart task on CLI
- API/CLI: Fix for creating a security group rule not persisting instanceTypeId
- API/CLI: Fix for history API query filters not working
- API/CLI: Fix for updating cloud access settings in roles
- API/CLI: Fix for updating user role multitenant flag
- API/CLI: Fix for Morpheus push API checks
- Apps: Fix for instance configuration getting reset when using “previous” in the app wizard
- Archive: Fix for Morpheus user session timeout during large file upload
- Backups: Updated backup message in Admin - Backups when backups are disabled
- Blueprint: Fix for exposed ports not being lockable
- Blueprint: Fix for tier order display in multi tier blueprint
- Blueprint: Fix for volume size field responsiveness
- Clouds: Fix for AWS security group subnetant visibility
- Clouds: Fix for Open Telekom Cloud router & network creation
- Clouds: Fix for Morpheus IP-pool ranges being deleted when a cloud with associated network is deleted
- Custom Library: Fix for instance wizard not allowing a custom library item for oracleVM
- Custom Library: Fix for Sub-Tenants role permissions for custom instance types when tenant role Instance Type Access is set to Global:Custom
- Groups: Fix for User Group deletion when user group is associated with existing instances
- Hosts: Fix for Docker & Kubernetes hosts not deployable on VIO
- Hosts: Fix for Ubuntu Docker hosts DNS name servers being removed on reboot
- Images: Fix for GPS images incorrect labeling
- Images: Fix for images being larger than selected plan
- Images: Fix for seeded CentOS 7.2 & 7.3 Docker system images
- Instances: Fix for Plan/Resource change detected when altered on cloud (not creating new usage records)
- Instances: Fix for multi-select convert to managed not having group selection
- Instances: Fix for not being able to clone Windows instance
- Instances: Fix for reconfiguring VM/Host not adding new usage record
- Instances: Fix for start/stop service on instance list showing when not applicable
- Instances: Fix for sub nav bar not appearing when clicking app link in instance detail page
- Load Balancer: Fix for AVI fields missing in LB provisioning wizard
- Networking: Fix for not being able to create NSX edge gateway
- Nutanix: Fix for Windows hostnames being counted/truncated
- OCI: Fix for regions not working properly
- Openstack: Fix for wrong plan tied being to instance
- Pricing: Fix for changes in machine configuration not being recorded in billing
- Pricing: Fix for cloud not showing in pricing label
- Pricing: Fix for hourly plan inconsistency
- Provisioning: Cloudbase-init: Fix for user creation via Cloudbase-init
- Provisioning: Fix for Windows VM turning status green prematurely
- Reporting: Fix for cost reports currency conversion
- Reporting: Fix Group and Tenant Cost reports both using the Term Zone instead of Cloud
- SAML: Fix for subtenant SAML Logout redirecting to error page
• Scaling: Fix for scale cloud priority settings, additional help text added
• SCVMM: Fix for SCVMM provisioning failing during failover cluster setup
• SCVMM: Fix for SVCMM cloud sync datastore cache
• Storage: Fix for storage showing wrong datastore
• vCD: Fix for cloud-init iso file cleanup
• vCD: Fix for custom vCD instance types not available for selection on convert to managed
• vCD: Fix for discovered & converted VM’s not creating an instance type
• vCD: Fix for hostname truncated with container ID
• vCD: Fix for issue with large number of templates
• vCD: Fix for vCD guest customizations running after instance restart triggered
• vCD: Fix for Windows instances appearing as discovered when provisioned onto vCD
• vCD: Fix for Morpheus triggering a power off instead of graceful shutdown for vApps
• vCD: vmId and vappId sent to their proper homes
• Veeam: Fix for Actions -> Backup on an instance executing the entire job
• Veeam: Fix for removing existing backup job removing other jobs
• VIO: Fix for not being able to delete instance with attached load balancer
• VMware: Fix for 8th additional disk using SCSI 0:7
• VMware: Fix for reconfigure not respecting cloud thick/thin disk setting
• VMware: Fix for record removal when changing Cloud Cluster scope from ALL to a single cluster
• VMware: Reconfigure now warns about requirement to delete snapshots
• VMware: Sync now updates cloud association when a VM is migrated between clusters scoped to multiple clouds.
• VMware: Sync now updates volume info for volumes that no longer exist on discovered vms

12.3 v3.5.3

Release date: 12/13/18

Note: yum and msi agent installs are now over port 443

Important: Nginx needs to be restarted after 3.5.3 upgrade with morpheus-ctl restart nginx

12.3.1 New Features

• API: Added externalId for vm’s
• API: Added user setting endpoints
• API: Blueprint Group & Tenant Access
• API: Customizing Blueprint Access
• API: Instance history added
• API: Provision Instances/Apps using Workflow names
• API: Track usage for Discovered VM’s
• API: Update host ssh password
• Appliance: ElasticSearch: Added support for ElasticSearch TLS connections
• Appliance: Global general performance improvement
• Appliance: Increase timeout for linux tasks
• Appliance: RabbitMQ: STOMP SSL support added
• Apps: Added App execution aborting
• Apps: Added review tab to app wizard
• Automation: Ansible: Morpheus Variables support added. containerScriptConfig map now sent to an extraVars.yml for Ansible use
• Backups: Commvault: Refactored Commvault integration
• Backups: Rubrik integration added with SLA Domain sync, Backup creation and restore.
• Backups: Rubrik Integration added.
• Backups: Zerto improvements
• Blueprints: Permissions section with Group Access and Tenant visibility added
• Clouds: Nutanix: CVM’s now shown as Hosts
• Clouds: Nutanix: V2 & V3 API stats for discovered VMs, Image Sync
• Clouds: Nutanix: Windows: Domain Join added to unattend.xml
• Clouds: Nutanix: Windows: License application added to unattend.xml
• Clouds: OpenStack: Added Network type choices for OpenStack SDN
• Clouds: OpenStack: LBaaSv2 API endpoints for VIO added
• Clouds: Openstack: Specify Floating IP option added
• Clouds: OTC: Added support for availability zones
• Clouds: SCVMM: Static IP’s now injected in unattend.xml
• Clouds: SCVMM: Windows: Domain Join added to unattend.xml
• Clouds: SCVMM: Windows: License application added to unattend.xml
• Clouds: Status in Clouds list view now shown as disabled and greyed out when when a Cloud is not enabled
• Clouds: VMware: Hypervisor Console: WMKS console added, replacing VNC. GDB Server port requirement on ESXi hosts is not required for WMKS.
• Load Balancers: F5: SSL profile creation added
• Infrastructure: Custom Instance Types can now be used on Convert To Managed
• Infrastructure: Renamed “Unmanaged” to “Discovered”
• Infrastructure: Service Plan can now be specified on Convert to Managed
• ITSM: New Cherwell Integration
• ITSM: New Remedy Integration
• ITSM: ServiceNow: CMDB update CI on status change
• Library: “Supports Convert To Managed” flag added to Layouts
• Operations: Activity: New History section added with active processes and process history
• Operations: Health: Added info message for single node Elasticsearch health
• Operations: Usage: Added Type Filter with Container, Host and Discovered options
• Provisioning: Auto-truncation of Windows hostnames if specified hostname is over 15 character limit. If truncated name matches existing hostname sequence added.
• Provisioning: Morpheus Agent msi and yum packages now transferred over 443. 80 still required for deb agents
• Provisioning: Support Deployments enabled on System MySQL Instance Type
• Provisioning: Windows: Agent install optimizations, speed improvements
• Storage: Dell EMC Isilon: Create exports to allow access from ip addresses
• Storage: Dell EMC Isilon: Create new NFS shares
• Storage: Dell EMC Isilon: Create storage providers from an Isilon volume
• Storage: Dell EMC Isilon: Manage existing NFS shares
• Storage: Dell EMC Isilon: Sync NFS volume shares to Morpheus
• Virtual Images: Prevent form autofill for username/password

12.3.2 Fixes

• Administration: Fix for deleting users that have history records in Archives
• Administration: Fix for external smtp settings requiring username
• Administration: Fix for saving white label settings in subtenants
• Administration: Fix for Windows passwords with ampersand
• Analytics: Fix for utilization time filters not returning data
• Ansible Tower: Fix for “Limit to Instance” flag
• Ansible Tower: Fix for Ansible Tower groups not set to mandatory
• Ansible Tower: Fix for Ansible Tower integration details search
• Ansible Tower: Fix for editing an Ansible Tower in Provisioning: Automation: Services
• Ansible: Fix for Ansible workflow execution fails as no hosts are found
• Ansible: Fix for intermittent git lock issue
• Ansible: Security Updates
• Appliance: Installer: Fix for :9200 being appended in elasticsearch.yml unicast hosts array
• Apps: Fix for App export creating extra configs when group is defined
• Apps: Fix for variables in Instance names not evaluated in App Tier view
• Automation: Fix for Automation Tasks search not working beyond first page
• Azure: Scale Sets: Fix for missed deployments when scaling multiple nodes
• Blueprints: Fix for blueprint export including name and templateName
• Blueprints: Fix for incorrect price data displayed for custom plans
• CLI: Fix for sub-tenant user invalid login counter
• Clouds: Fix for display of warning message when attempting to delete a cloud with existing managed vm’s
• Clouds: Fix for Instance usage record creation for Convert to Managed
• Dell ECS: Fix for ECS Bucket Edit unknown error on Bucket Name Update
• ESXI: Fix for ESXI Docker Host not using LVM on 2 disk Hosts
• Git: Fix for auto appending of .git to git url in Git Integrations
• Global Search: Fix for partial Instance Name search
• Groups: Fix for add clouds to group buttons hidden if no public clouds are enabled inAdministration - Settings
• Instances: Fix for instance clone not respecting cloud selection
• Instances: Fix for instance details auto refresh resetting history pagination
• Integrations: Fix for Integration: Edit dialog clearing host, username, & password fields on authentication failure
• Integrations: Fix for issue with display of Group & Cloud Integration scoping
• Load Balancers: F5: Fix for adding F5 Load balancer with SSL configured from instance scale tab
• Load Balancers: F5: Fix for editing F5 Load balancer settings from instance scale tab
• Logs: Fix for date filters
• Logs: Fix for log availability timeframe setting not applying
• Logs: Fix for page size when using log level filter
• Networking: Security Groups: Fix for ICMP rule requiring port
• Nutanix: Fix for plan assignment on Instances and associated VM’s for convert to managed
• Nutanix: Fix for Windows unattend.xml DNS settings
• Nutanix: Windows unattend.xml forced flag corrected to force
• OTC: Fix for OTC provisioning not surfacing failures
• Pricing: Fix for OracleVM plans issue with incorrect cores
• Pricing: Fix for price comparison missing some expected cloud prices
• Provisioning: Fix for tenant Plan visibility
• Provisioning: /morpheus directory perms created by Agent Install now set to drwxrwxr-x
• Provisioning: Fix for Load Balancer not retaining settings in instance wizard
• Provisioning: Fix for overzealous enforcement of min ram setting on custom Plans
• Provisioning: Fix for scaling down not cleaning up environment variables
• SCVMM: Fix for Resource Pool input styling
• SCVMM: Fix for Network Group Validation error
• SCVMM: Fix for VHD/VHDX in node type dropdown
• Storage: Fix for storage bucket/shares input validation
• Tenants: Fix for inability to delete tenants with IP pools in use
• UCS: Fix for UCS cloud credentials not working on add, only edit
• User Settings: Fix for Default Cloud selection displaying clouds in groups not accessible to user
• Users: Fix for Bearer token expiration
• VCD: Fix for provisioning when using a synced Image from non-morpheus generated vCD catalogue.
• VCD: Fix for uploading Images over 1 GB
• VCD: Network DNS settings now updated upon cloud sync
• VCD: Removed Hostname value in discovered vm’s detail view. This was set to machine name previously as Hostname is not available via vcd cloud sync.
• Veeam: Fix for Veeam backup restores not working for existing jobs
• VMware: Fix for VMware Docker Host creation when cloud is scoped to a Resource Pool
• VMware: Fix for VMware reconfigure listing duplicate storage controllers
• Workflows: Fix for executing workflows on Hosts

12.4 v3.4.4

Release date: 11/2018

12.4.1 New Features

• Currencies: Rand currency added
• Administration: Inactive option added for Tenants
• Load Balancers: Allow host selection when creating HAProxy LB
• Hosts: External ID added to Host, VM and Bare Metal detail views
• Nutanix: Hypervisor Hosts sync added, improved statistics for inventoried Hosts and VM’s
• API: externalId added to Hosts
• License: Applying Windows Licenses support added to Amazon, Azure, Alibaba, Nutanix and Openstack Clouds

12.4.2 Fixes

• Hosts: SSH Username corrected to SSH Password when adding Unmanaged Linux Vm
• Forgot Password Email: Email subject more indicative of password reset, not account lock
• Remote Console: Fix for Console issue when instance has multiple nodes
• Global Search: Fix for User results missing from Quick Results
• VMware: Fix for Resize issue with add/remove volumes when disk type selection disabled
• Hosts: Resolved toggle for “Manage Internal Firewall” on Edit Host to reset all acls on save.
• Provisioning: Issue evaluating variables in instance name while using copies
• Provisioning: Fix for not showing error icon for all invalid fields
• Provisioning: Fix for Service Plans not filtered by Min Ram setting for “VMware” Instance Type
• Docker: Fix for intermittent LVM volume creation issue
• User Details: Fix for updating User Settings changing password on save when passwords were not updated.
• Instance List: Fix for Instance Category icons not filtering the Instances List
• Search: Search bar displayed now after 250ms hover
• User Impersonation: Fix for impersonating when duplicate usernames exist across Tenants
• Load Balancers: F5: Fix for issues with edit pool
• Load Balancers: F5: Monitor - parent monitor not working with custom monitors
• Load Balancers: F5: Fix for error when saving with no port number defined when >=2 members
• Load Balancers: F5: Fix for description not being set for pool
• Load Balancers: F5: Fix for editing F5 Load balancer settings from instance scale tab
• Load Balancers: F5: Fix for adding F5 Load balancer with SSL configured from instance scale tab
• Infoblox: Fix for issues with pool and domain records
• Nutanix: Windows Computer Name now set in sysprep unattend.xml
• Instances: /morpheus directory perms created by Agent Install now set to drwxrwxr-x
• Users: Fix for deleting a user with Archives history records
• Instance details: Fix for Price data refreshing to inaccurate value
• Provisioning: Fix for overzealous enforcement of min ram setting on custom Plans
• Whitelabeling: Fix for issue saving sub-tenant Whitelabel setting
• Tenants: Fix for sub-tenant created plans names visible in other Tenants when creating Docker Hosts
• Blueprints: Fix for incorrect price data displayed for custom plans
• OracleVM: Fix for provisioning using deprecated CPU value rather than Cores value
• Instances: Clone: Fix for Cloud selection when cloning
• VCD: Fix for provisioning when using a synced Image from non-morpheus generated vCD catalogue.
• Config Management: Fix for Config Management scoping sometimes not visible when editing a Group or Cloud
• UCS Cloud: Fix for credentials not saving and add cloud
• VMware: Fix for duplicate storage controllers on reconfigure
• Nutanix: Fix for Windows static IP assignment via sysprep unattend.xml
• Nutanix: Fix for Windows DNS settings via sysprep unattend.xml
• Provisioning: Price Comparison: Fix for missing Azure price comparisons
• Scaling: Fix for scaling down not cleaning up environment variables
• Nutanix: Fix for sysprep unattend.xml typo in powershell cmdlets
• VCD: Fix for VCD IP Pools Network DNS Servers changes updating on cloud sync
• Administration: Settings: Fix for external SMTP server username requirement (now not required)
• Automation: Tasks and Workflows: Fix for search scope limited to 1st page
• Git Integration: Fix for .git being appending to git urls
• Provisioning: Apps: Fix for extra definitions in App export json/yaml
• Groups: Fix for Add Cloud to Group options hidden if no Public Clouds are enabled
• Usage: Fix for usage records not being generated upon “Convert to Managed”
• VCD: Fix for uploading images over 1 GB
• VCD: Removed Hostname value in Unmanaged Host detail view. This was set to machine name previously as Hostname not available via sync.
• Administration: Fix for deleting Tenants with existing IP Pools
• ESXi: Docker Host Provisioning: Fix for 2 disk hosts not using LVM
• User settings: Default cloud selection now only lists user accessible clouds
• Reports: Fix for Reports permissions
• Installer: Fix for :9200 being appended in elasticsearch.yml unicast hosts array

12.5 v3.5.2

Release date: 10/22/2018

12.5.1 New Features

• Administration: Inactive option added for Tenants
• Ansible: Run output now always displayed in Instance history
• API/CLI: Storage Providers renamed to Storage Buckets
• API/CLI: Update instance metadata and power schedule added
• Appliance: Tomcat upgraded to v9.0.12, addresses CVE-2018-11784
• Apps: App Loading performance improvements
• Automation: Provisioning Workflow and Script output always added to Instance history
• Automation: Execute Options added to Tasks w/ Retryable Flag, Retry Count and Retry Delay settings
• Automation: Tasks sets set on “Post Provision” phase now run when executing workflows post-provision
• Automation: Workflows will now stop running on a task failure
• Blueprints: AWS CloudFormation support added
• Clouds: Virtustream integration added
• Commvault: Integration expanded including sync, instance support, job management and restores.
• Currencies: Rand currency added
• Hosts: External ID added to Host, VM and Bare Metal detail views
• Infoblox: Sync optimizations
• Instances: Owner assignment added to Instances
• Load Balancers: Allow host selection when creating HAProxy LB
• Logs: Enhanced logs display and formatting
• License: Applying Windows Licenses support added to Amazon, Azure, Alibaba, Nutanix and Openstack Clouds
• Network: External ID added to Network detail view
• Nutanix: Hypervisor Console added
• Openstack: Hypervisor Console added
• Operations: Morpheus Health section added with Health, Alerts and Appliance Logs
• Provisioning: Add timezone option to Provisioning wizard
• Roles: Operations: Health, Provisioning: Blueprints - CloudFormation Feature Access permissions added
• SCVMM: Multi host and datastore support added
• Storage: Dell EMC ECS Integration added
• Storage: Dell EMC Isilon Integration added
• Storage: NFS volume share sync added
• Storage: Providers split to to Storage Buckets and File Shares sections
• Tenants: Message added to Users section when no multi-tenant User Roles exist
• VCD: CentOS Image and Instance type added
• VCD: Debian image and Instance type added
• VCD: IP Pool allocated IPs sync added
• VCD: Ubuntu 16.04 layout
• Xen: Hypervisor Console added

12.5.2 Fixes

• API: Fix for /api/check-types call fails w/ unable to find API endpoint error
• API: Fix for /api/key-pairs call triggering 403 error
• API: Fix for /api/certificates call triggering 403 error
• API: Fix for /api/instances/:id call resulting in http 500 error if the Instance has any backups
• App Wizard: Fix for app validation issue with service plan ranges
• App Wizard: Fix for blueprint search when no config exists in Blueprint
• Clouds: Fix for Cloud Timezone setting not being respected for IBM Cloud, UpCloud and Softlayer
• Docker: Fix for intermittent LVM volume creation issue
• Forgot Password Email: Email subject more indicative of password reset, not account lock
• Global Search: Fix for User results missing from Quick Results
• Hosts: Resolved toggle for “Manage Internal Firewall” on Edit Host to reset all acls on save.
• Hosts: SSH Username corrected to SSH Password when adding Unmanaged Linux Vm
• Infoblox: Fix for issues with pool and domain records
• Instance List: Fix for Instance Category icons not filtering the Instances List
• Load Balancers: F5: Fix for description not being set for pool
• Load Balancers: F5: Fix for error when saving with no port number defined when >=2 members
• Load Balancers: F5: Fix for issues with edit pool
• Load Balancers: F5: Monitor - parent monitor not working with custom monitors
• Load Balancers: Fix for LB’s not getting created when provisioned via app wizard
• Nutanix: Fix for applying Static IP’s via unattend.xml
• OTC: Local Disk provision option removed (not supported)
• Price Policy: Provisioning Instances now counted towards policy
• Pricing: CPU Only price type removed
• Provisioning: Fix for not showing error icon for all invalid fields
• Provisioning: Fix for Service Plans not filtered for “VMware” Instance Type
• Remote Console: Fix for Console issue when instance has multiple nodes
• Search: Search bar displayed now after 250ms hover
• Tenants: Tenant Limits removed, replaced by Tenant Policies
• User Details: Fix for updating User Settings changing password on save when passwords were not updated.
• User Impersonation: not properly handling duplicate usernames
• VCD: Fix for Cloud sync not syncing all VMs
• Veeam: Fix for Veeam Service legacy data (pre 3.5.0) causing backups servers not appearing
• VMware: Fix for Resize issue with add/remove volumes when disk type selection disabled

12.6 v3.4.3

Release date: 9/21/2018

12.6.1 New Features

• Appliance: Reduced memory database query overhead for agent comms
• VMware: API session management improvements
• VMware: Massive cloud sync speed improvements

12.6.2 Fixes

• AWS: Fix for io volume type selection
• Azure: Fix for price plans syncing
• Docker Hosts: Total Storage value fix
• Docker Hosts: Total Storage value fix
• ESXi: Fix for file cleanup on failed provisions
• Guidance: Improved core count recommendations
• Identity Sources: Fix for form resetting back to LDAP on unsuccessful save
• KVM: Fix for Backup Restore for multi-disk VMs
• KVM: Fix for Ubuntu 14 backups
• Load Balancers: AVI: Fix for edit instance lb setup
• Nutanix: Fix for automated Domain joins
• OTC: Fix for Reconfigures
• Policies: Fix for Max VMs Policy enforcement
• Policies: Unable to edit policy assigned to tenant
• Reports: Fix for 500 error when report generated by deleted user exists
• Scaling: Fix for NGINX autoscaling
• Scaling: Fix for Scaling Schedules
• User Settings: Fix for unable to set user settings when connected to AD identity source.
• Venafi: Fix for deleting integration
• Venafi: Fix for deleting integration

12.7 v3.5.1

Release date: 9/21/2018

12.7.1 New Features

• API: Services - Cypher added
• API: User creation passwordConfirmation requirement removed
• Appliance: Reduced memory database query overhead for agent comms
• Backups: Avamar Integration added
• Bluemix renamed to IBM Cloud
• Infoblox: Variable support for ext attributes added
• Instances: Metadata fields added to Edit Instance modal
• Instances: Post-Provision Metadata and Tags editing
• Morpheus Agent: Ubuntu 17.10 support added
• Openstack: Additional support for versioned endpoints added
• Openstack: Octavia Load Balancer Support added
• Openstack: Queens support added
• Option Lists: Authentication added for remote data providers
• Policies - Policies section added to Administration for managing all Policies.
• Policies: Budget Policy type Added
• Policies: Global and User policy levels added
• PXE: webHost in answer files now forced to http
• Reports: Workload Summary Report added
• Softlayer: Washington 6 region added
• Storage: Storage Browser for NFS, Azure & Alibaba provider types added
• Tenants: Disable option added for sub-tenants
• VCD: support for vcd v9
• VCD: Virtual Machine sync now includes undeployed VMs
• vCloud Director: Support for v9.x added
• Veeam: Service detail page added
• VMware: API session management improvements
• VMware: Massive cloud sync speed improvements

12.7.2 Fixes

• Ansible Tower: Fix for Edit Integration
• Ansible Tower: Fix for removing Ansible Tower Integration from Group or Cloud
• Approvals: Fix for VM state updating on Instances list page after request is rejected or cancelled
• Azure: Fix for price plans syncing
• Backup: AWS backup shows in progress when snapshot limit exceeded
• Backups: Default Backup Schedule not applied
• Docker Hosts: Total Storage value fix
• ESXi: Fix for file cleanup on failed provisions
• Guidance: Fix for resize action
• Guidance: Improved core count recommendations
• Identity Sources: Fix for form resetting back to LDAP on unsuccessful save
• Identity Sources: Fix for Required Group still applying after removal
• Instances: Clone: Fix for Cloud selection not being respected
• Instances: Fix for creating Instance with numbers-only names
• KVM: Fix for Backup Restore for multi-disk VMs
• KVM: Fix for Ubuntu 14 backups
• LB: AVI - SSL shows ‘Select’ instead of ‘No SSL’
• Library: Layouts: “Min Ram” not enforced when using custom plans
• Library: Option Lists: Fix for option list with failed validation still creating records
• Library: Scripts: Fix for WindowsFeature "$Feature$Number" causing scripts to be un-editable
• Load Balancers: AVI: Fix for edit instance lb setup
• Load Balancers: AVI: Fix for manually adding Virtual Server
• Localizations - added message for Venafi delete
• Networks: Fix for deleting an ACI Integration
• Nutanix: Fix for automated Domain joins
• OTC - Docker Host setup fails to complete
• OTC: Fix for Reconfigures
• Policies: Fix for issue with Power Schedule Tenant permissions
• Policies: Fix for Max VMs Policy enforcement
• Policies: Unable to edit policy assigned to tenant
• Pricing: Fix for Azure price discrepancy
• Provisioning: Fix for Cores per socket resetting back to 1 when going back in provisioning form
• Provisioning: Fix for Price comparison modal for custom images
• PXE: Fix for deleting kickstart files for subtenants
• Reports: Fix for 500 error when report generated by deleted user exists
• Scaling: Fix for NGINX autoscaling
• Scaling: Fix for Scaling Schedules
• Subtenants: Removed invalid link to Shared Clouds on Instance Details page
• User Settings: Fix for unable to set user settings when connected to AD identity source.
• User Settings: Username uniqueness now scoped to Tenants
• vCloud Director: Fix for sync error when a vm has no disks
• Veeam: Fix for Legacy referenceData causes backupServer dropdown to not load
• Venafi: Fix for deleting integration
• Venafi: Fix for incorrect subject set when applying cert during provisioning
• Virtual Images: Removed “Convert” option for synced images

12.8 v3.4.2

Release date: 8/23/2018

12.8.1 New Features

• Amazon: Additional service plans available
• API & CLI: Instances metadata added
• AWS: China cn-north-1/Beijing and cn-northwest-1/Ningxia regions added
• Infoblox: Extended attributes for A and PTR records added
• Infoblox: Script variable support added for extended attributes
• Instances: Custom exposed ports are now globally available
• KVM: VM Actions, MultiDisk, Reconfigure, Apps & Blueprints. Backups/Restore added
• Morpheus Agent: Ubuntu 17.10 support added
• PXE: Now force webHost to http for answer files

12.8. v3.4.2 475
• Xen: CUSTOM PORT option added to Xen Cloud Config

12.8.2 Fixes

• ACI: Fix for deleting an ACI integration
• Active Directory: Fix for removing Required Group after one is added
• Approvals: VM status now moves from pending to cancelled/rejected on cancelled/rejected action from approval screen
• AVI: multiple fixes and improvements
• Azure: Fix for discrepancy in the prices shown in Morpheus for Azure prices
• Evars: Fix for environment variables/deployment option values longer than 255 result in 500 error
• Guidance: Fix for resize action on recommendations
• Image builder: fix for config issue with plans when custom cpu is enabled
• Instances: Cloning: Fix for cloud selection
• LB: AVI: Create Pool - fix for blank monitors field
• LB: AVI: Nodes: Fix for empty Monitor column
• LB: Edit AVI - avi cloud field not populating
• Load Balancers: Fix for Load Balancer for failing to save when multiple ports are available but only on 1 port is configured
• Monitoring: Fix for updating existing App Checks causing a 500 error
• Oracle Cloud: Fix for Virtual Image Icon missing
• Provisioning: Fix for creating instances with names containing only numbers
• Provisioning: Price comparisons: Fix for custom images not displaying Price comparisons
• PXE: Fix for subtenant kickstart file deletion
• Scale Schedules: Fix for schedule execution
• Seed: Fix for hasNodeMonitors seed error
• Subtenants: Removed hyperlink on Cloud Name for inaccessible clouds that would result in 500 error
• Unmanaged VMs: Fix for cores not updated on refresh
• User Settings: User name uniqueness now scoped to Tenant
• VCD: Fix for Guest Customization for Windows failing to run.
• Venafi: Fix for Add Integration from Administration section
• Venafi: Fix for Details page error
• Venafi: Fix for subject on certs added during provisioning
• Venafi: Fix for viewing Certificates
• Venafi: Instance Settings: Fix for edit cert
• Virtual Images: Convert option removed for synced images
• Virtual Images: Fix for deleting failed conversions
12.9 v3.5.0

Release date: 7/31/2018

12.9.1 New Features

- Administration: Added support link white label
- Analytics: Added Cost by Tenant report
- Analytics: Added Cost by Group report
- Analytics: Added Cost by Application report
- Analytics: Added Cost by Instance report
- Analytics: Added Cost by Cloud report
- Analytics: Added Tenant Instance Usage report
- Analytics: Added metadata filter to reports
- Ansible: Added Ansible Tower integration
- API/CLI: Workflows now support custom option types
- API/CLI: DataStores added
- API/CLI: Subtenant Groups added
- API/CLI: Added “taskPhase” for workflow tasks
- API/CLI: Added CLI login via token
- API/CLI: Added optimization for virtual image upload
- API/CLI: Added metadata for instances
- Backups: Direct Stream to Storage Provider added for VMware, Xen and KVM backups and Image imports.
- Backups refactored with Schedules, Job, Types, and Services
- Backups: Zerto Integration added
- Multicloud object storage backup and archival
- Blueprints: Added ACI fields to Blueprint and App wizards
- Cloud Foundry: Added inventory of applications during cloud sync
- Cloud Foundry: Added support scaling
- Cloud Foundry: Added sync for build packs
- Cloud Foundry: Added custom route
- Plans & Pricing: Prices: Datastore Price Type added
- KVM: Added KVM migration workflow
- KVM: Added CEPH storage support
- KVM: Backup/restore is now possible for local datastores and LVM
- Library: Debian 9.4 qcow2 image added
- Instances: Backup type, provider, job, latest, next, added to instance detail page
- Network: VMware NSX Integration added
- Option Lists: Tenant visibility added to Option Lists
- Option Lists: Added realtime sync option
- Oracle: Added support for different storage types
- Oracle: Added Oracle Cloud library nodes
- Oracle: Added ability to upload a local image and provision to Oracle Cloud
- phpIPAM: Added additional details (description, hostname, owner)
- Variables: Added tenantSubdomain variable
- Policies: Backup Creation policy type added
- Policies: User Creation policy type added
- Infrastructure: Hosts: Added host OS, Type and Status filters
- Plans & Pricing: Added Custom Ranges to Service Plans for min/max storage, memory and cores
- Provisioning: Added ability to toggle between MB and GB for memory settings in provisioning wizard
- Roles: Added Global Access: Custom option to roles
- SAML: Added response validation
- ServiceNow: Added credential validation
- Storage: Renamed “Object Stores” to “Providers”
- Storage Providers: Added details page that allows you to browse, upload and delete files
- Storage Providers: Verify permissions to path on save added
- Storage Providers: Removed option for Tenants to create local storage providers
- Storage Providers: Retention policy added
- Storage Providers: Amazon S3: Added Create Bucket option
- Users: Subtenant users will no longer be able to login from the main login page without specifying their subdomain
- Users: Added API token generation for users via UI
- Virtual Images: Default “force guest customizations” to “on”
- VMware: Added VMware “Clone to Template” Action
- VMware: Direct stream Backups added
- XenServer: Backups don’t offload backup

### 12.9.2 Fixes

- Fix for Chef detail section not displaying in app wizard
- Fix for deployment failure with ARM template copies
- Fix for Blueprints: broken image for library items with no custom icon
- Fix for Analytics: Instance Count by Type and Cloud report: Cloud value
- Fix for Instance Count by Cloud report
• Fix for ServiceNow Plugin and API issue
• Fix for web instance types
• Fix for ServiceNow not listing datastores
• Fix for issue deleting ServiceNow integration
• Fix for OpenStack space issue
• Fix for OpenStack floating IP issue
• Fix for F5 destination port issue
• Fix for VMware ServiceNow Plugin
• Fix for manually deleting F5 pools and nodes
• Fix for Nutanix VM taking multiple IP slots
• Fix for PXE answer file
• Fix for ENI records not being cleaned up in Amazon
• Fix for tenant delete issues
• Fix for Nutanix image endpoint
• Fix for Install Agent flag for Nutanix
• Fix for OTC missing icons
• Fix for HCL parsing not saving
• Fix for CentOS VM conversion issue
• Fix for Blueprints resource pool
• Fix for instance provisioning hanging at configure stage
• Fix for Blueprints not connecting to Azure LB
• Fix for Option List ignoring SSL errors
• Fix for OTC duplicate images
• Fix for changing roles via AD groups
• Fix for user data in Windows Cloud
• Fix for provisioning Windows into vCD
• Fix for Custom Checks
• Fix for local firewall not working for VM’s
• Fix for Cloud Foundry and inventoried apps
• Fix for Cloud Foundry API check type missing logo
• Fix for Cloud Foundry cloud details
• Fix for Cloud Foundry orphaned instances and hosts
• Fix for Instance Inventory Summary
• Fix for deployment versions not sorting
• Fix for Archive Snapshots not saving
• Fix for Alibaba CentOS 6.9 bad layouts
• Fix for security groups
• Fix for Hadoop Ports map error
• Fix for modals not loading
• Fix for price editing
• Fix for multidisk component not using virtual image locations
• Fix for instance name validation
• Fix for instance type search limited to selected category
• Fix for adding disks requiring logs
• Fix for volume addition requiring infrastructure
• Fix for private hosts visible to tenants
• Fix for AD login when user OU changes
• Fix for changing plan not updating volume
• Fix for order of logs display
• Fix for cloud not saving user data
• Fix for network CRUD issues
• Fix for VMware ‘Clone to Image’ not showing failures
• Fix for API task ‘deleting’ failing
• Fix for log parse error
• Fix for creating app from existing template with no blueprint
• Fix for Azure ARM parsing error
• Fix for VMware ‘Clone to Image’ not working for stopped VM’s
• Fix for billing API
• Fix for App wizard naming issue
• Fix for Oracle Cloud Virtual Image icon missing
• Fix for Venafi integration details page
• Fix for AVI LB monitors field being blank
• Fix for Image Builder configuration issue
• Fix for Veeam integration not being checked by default
• Fix for Blueprints missing backup locks
• Fix for error deleting Cloud Foundry service
• Fix for i18n missing label

12.10 v3.4.1

Release date: 7/20/2018
12.10.1 New Features

- API: Run workflow now allows arbitrary `customOptions` to be passed
- API/CLI: Added CLI login via token. `login -T <token>` can be used instead of requiring a username and password.
- API/CLI: Added optimizations for Virtual Image uploads
- API/CLI: Added “taskPhase” for workflow tasks
- Backups: Direct Stream to Storage Provider added for VMware, Xen and KVM backups and Image imports.
- Blueprints: Added ACI fields to Blueprints and Apps wizards
- phpIPAM: Added additional information including description, hostname and owner
- Policies: Added variable `<%= tenantSubdomain %>` for Tenant SubDomain value in scripts and naming policies. The SubDomain is used for creating a direct login url in Identity Sources or as a login prefix to identify the tenant i.e. ‘subdomainusername’
- Puppet: Expanded OS support for Puppet Agent install.
- Users: User Settings: `API Access` section added for API & CLI user token generation
- VMware: Added `Clone to Image` Instance Action to create new VMware Templates from Instances with corresponding Morpheus Virtual Image record.
- VMware: Virtual Images: Switched “Force Guest Customizations” to on by default for Windows Virtual Images

12.10.2 Fixes

- Fix for VMware ovf export timeouts for large images. Impacted offloaded backups, `Import as Image` actions.
- Fix for Deployment versions not sorting
- Fix for disabling ‘Archive Snapshots’ flag on Storage Providers not saving. When executing backups, the ‘Archive Snapshots’ flag enables ovf export of VMware snapshots to default or specified backup Storage Provider and removes the snapshot in VMware. If disabled, backup jobs will only trigger and leave snapshots in VMware.
- Fix for Active Directory user login when users OU has been changed
- Fix for duplicate Alibaba CentOS 6.9 layouts
- Fix for Azure: ARM Templates `copyIndex` parsing errors
- Fix for Security Groups with Source Type set to All
- Fix for Actions: `Reconfigure` modal not loading in Infrastructure -> Hosts Section
- Fix for Instance Name uniqueness validation in provisioning Wizard
- Reverted Provision Wizard: Instance Type search being limited to selected category
- Fix for adding disks requiring `Logs: Read or Full Role permissions`
- Fix for volume addition requiring `Infrastructure - Storage: Read or Full Role permissions`
- Fix for Master Tenant private KVM Host Subtenant visibility
- Fix for changing plan not updating volume size for Nutanix Instance Type until image is selected
- Fix for adding AVI load balancer integration.
- Fix for API: `/groups/:id/update-zones` removal of zone not passed in the `zones` parameter
Morpheus Documentation, Release 3.6.1

- Fix for Apps wizard not loading when User Role permission set to Provisioning: Blueprints: None
- Fix for Logs: Date parsing error when Windows Event logs are localized

### 12.11 v3.4.0

Release Date: 6/19/2018

**Important:** Morpheus v3.4.0 adds support for subtenant users to login via the main tenant url using subtenant id or subdomain prefix, ie subtenantId\username or subdomain\username. Subtenant local users will no longer be able to login from main login url without using subtenant id or subdomain prefix. Tenant subdomain can be defined by editing the Tenant settings and updating the SUBDOMAIN field.

### 12.11.1 New Features

- API/CLI: DataStores added
- API/CLI: Salt command options added
- API/CLI: Subtenant Groups added
- API/CLI: Workflows now support custom option types
- Blueprints: ARM template Git integration added
- Currency: Conversion settings added to Administration -> Settings.
- Datastores: Storage > Datastores capacity column now hidden when “Hide Datastore Stats On Selection” is enabled
- Identity Sources: Subtenant users can now login from the main login url using subtenant name or id prefix, including users created from Identity Source Integrations.
- KVM: Added OnApp migration support
- Library: CentOS 7.5 qcow2 image added
- Library: Ubuntu 16.04, 18.04 qcow2 images added
- Policies: User Creation Policy added
- Provisioning: Added default datastore for additional disks to match first disk
- Provisioning: Additional Network Interface types now default to match first Interface type
- SAML: Validation configuration options added
- Storage Providers: Verify permissions to path on save added

**Note:** In 3.4.0+ currency conversion data users will need to provide an open exchange or fixer.io api key under Administration -> Settings.
12.11.2 Fixes

- Fix for Chef detail section hidden in UI
- Fix for Cost by Cloud error
- Fix for incorrect Instance provisioning status when using copies with ARM Templates
- Fix for broken image issue for library items with no custom icon
- Fix for Instance Type Count - By Clouds Value in Analytics
- Fix for Instance Count by Cloud Group Count Value in Analytics
- Fix for CLI Bad Request issue when creating a cloud
- Fix for Web Instance Types to be scalable
- Fix for Cost Month to Date report
- Fix for ServiceNow listed Datastores
- Fix for Cloud Init enabled in Images
- Fix for KVM provisioning issue
- Fix for i18n missing message
- Fix for App Wizard Amazon validation issue
- Fix for space issue with Openstack
- Fix for postgresQL issue with BluemixCF
- Fix for Clouds stuck in deleting when removing
- Fix for issue with adding/editing local storage objects
- Fix for OpenStack Floating IP's being required
- Fix for F5 destination port issue
- Fix for Storage Object issue with NFS
- Fix for instance Wizard Issues
- Fix for ServiceNow Plugin unable to provision VMWare instance
- Fix for ServiceNow Plugin Datastores duplicate options
- Fix for F5 error deleting Pools and Nodes
- Fix for missing scale tab for VCD Instances
- Fix for KVM SSH fail after stop/start
- Fix for App Wizard form update when changing cloud
- Fix for ESXI Debian 8.8 failing to provision
- Fix for KVM provision failing on self managed host
- Fix for OEL build fail if more than 3 disks are requested during provisioning
- Fix for Open Telekom Cloud provisioning issue
- Fix for Cost by Cloud projected values
- Fix for Nutanix duplicate IP's when using IP Pools
- Fix for PXE answer file not getting generated
• Fix for ENI records not being cleaned up (Amazon)
• Fix for Tenant delete issues
• Fix for Nutanix sysprep unattend.xml passwords
• Fix for “Install Agent” Flag for Nutanix Images
• Fix for missing image icons
• Fix Terraform HCL parsing
• Fix for some converted-to-managed VM’s having docker check type
• Fix for unnecessary resource pool request
• Fix for vmToolsInstalled: no such property

Morpheus v3.4.0 is available in the Downloads section of

12.12 v3.3.2

Release Date 5/24/2018

**Important:** If upgrading from versions earlier than 3.2.0 please follow the 3.2.0+ upgrade instructions below the release notes.

**Important:** Appliance Elasticsearch communication in 3.3.1+ switches from transport protocol 9300 port to http 9200

12.12.1 3.3.2 New Features

• Agent: Support for Ubuntu 18.04 LTS added
• Alibaba: Docker Host support added
• Alibaba: Virtual Image upload added
• API: Virtual Image Upload via url added
• API: Identity Source added
• API: Instance config and volume details added
• Apps: New default Blueprint logos
• Auditing: Now support the ability to export the audit log from user interactions to a SIEM tool
• Auditing: AuditLogService added to morpheus-ui logs
• Azure: Scale Set threshold validation added
• Bluecat: New method added for instant dns record deployments
• Blueprints: Templates have been renamed to Blueprints
• Blueprints: Default Blueprint type option added to Administration - Provisioning
• Blueprints: ARM: Support for “concat” and “copies” added
• Blueprints: Terraform: AWS support added
• Blueprints: Terraform: Support for variable instance names added
• Blueprints: Terraform: Oracle Cloud support added
• Blueprints: Terraform: Failures surface on the app details page
• Blueprints: Terraform: Variables now surface in App wizard
• Global Search: Quick results added to header search
• Infoblox: Support for custom extended attributes added
• Instance Wizard: Code reworked for optimizations
• Infrastructure: Updated delete dialog text
• Keys & Certs: Services section added
• Keys & Certs: Venafi service added
• Keys & Certs: EC type public key support added
• Keys & Certs: Upload keypair option added
• Kubernetes: Ports no longer need to be defined on custom library items
• Kubernetes: Added icon for Kubernetes instance type
• KVM: Caching virtual machines now include metadata on network and storage volumes attached to a KVM VM
• KVM: Re-factored LVM implementation of KVM to allocate a volume per disk instead of nested QCOW2 files
• KVM: VM Inventory added
• Network Services: phpIPAM integration added
• Plans & Pricing: Max disk limit added to plans
• Reports: Tenant filtering added to Usage Reports
• Reports: Cost Reports added with Application, Cloud, Group, Instance and Tenant Cost Reports
• Reports: Usage Reports: Tenant Usage Report Added
• Roles: Trust Services permission added. Controls Infra > Keys & Certs > Services access and Admin > Integrations > Add (trust options)
• ServiceNow: Kingston certification added for Morpheus SNOW Plugin
• Users: Password confirmation fields added for Linux and Windows users
• vCloud Director: Custom Plans support added
• vCloud Director: Docker Host support added
• vCloud Director: Reconfigure added
• VMware: Instance Notes sync added

### 12.12.2 3.3.2 Fixes

• Fix for tenant delete that fails if an app with custom tiers is used to create an app
• Fix for Alibaba Cloud sync delay
• Fix for Alibaba release EIP not respected when deleting VM
• Fix for Alibaba network being recreated on sync
• Fix for Alibaba instance validation not completing
• Fix for Alibaba instance name validation
• Fix for Xen snapshots not being cleaned up
• Fix to show existing VM’s in Alibaba inventory
• Fix for deleting SCVMM cloud
• Fix for style issue with load balancer advanced options
• Fix for Veeam Templates/Jobs not populating
• Fix for Oracle Cloud VM. VM will restart after it is resized
• Fix for VMware storage containers where adding a controller would clear the volume type
• Fix for extra backup that’s created on an Azure Scale Set instance
• Fix for Azure Scale Set instance data issues
• Fix for MacStadium creating a duplicate VM after cloud sync
• Fix for Alibaba cloud not cleaning security groups when deleted
• Fix for Oracle Cloud users not being created for non-cloudinit images
• Fix for Service Now incident level update
• Fix for KVM multidisk provision
• Fix for Bluemix Platform not cleaning up service library items
• Fix for Alibaba not using available EIP
• Fix for missing price component
• Fix for Kubernetes host cert issue
• Fix for Windows Cloudbase-init userdata and DNS client settings missing
• Fix for wrong Ethernet adapter type being set on uploaded Windows images
• Fix for Alibaba backups not getting deleted when instance is deleted
• Fix for KVM provision not respecting host selection
• Fix for Cloud Foundry user permissions
• Fix for manual KVM host deletion error
• Fix for permissions on default storage path
• Fix for Openstack cloud service plans assigned to subtenants
• Fix for default instance deployment
• Fix for Alibaba ‘preserve volume’ not working on delete
• Fix for system instance type: macOS
• Fix for expired backup archived not deleting on S3
• Fix for unintended firewall evaluation when using shared resource in an app
• Fix for KVM App/Template issues
• Fix for Last Deployment: Never Deployment phrasing
Important: If upgrading from versions earlier than 3.2.0 please follow the 3.2.0+ upgrade instructions below

### 12.12.3 3.2.0+ Upgrades

Upgrading from previous versions of Morpheus to 3.2.0 or later requires upgrading ElasticSearch to 5.4.1 or 5.x. We do not support ElasticSearch 6.x at this time. This upgrade requires an export and import of Morpheus ElasticSearch data if you want to retain logs, backup history, statistics, and check history of your instances. If you do not need to retain that data you can skip the ElasticSearch migration. Upgrading to 3.2.0 will create a blank ElasticSearch node with no data. Your Morpheus layout configuration will determine how to migrate your ElasticSearch data: all-in-one or distributed high availability.

This deployment configuration is the default mode for Morpheus and contains a single ElasticSearch instance on the appliance. The migration steps are as follows:

1. Login to your appliance as a user that has sudo privileges and can switch to the root user sudo su -. You can run the following commands under sudo, but you will need to pass the PATH to the Morpheus embedded directory. Export the Morpheus embedded path to your environment by executing: export PATH=/opt/morpheus/sbin:/opt/morpheus/sbin:/opt/morpheus/embedded/sbin:/opt/morpheus/embedded/bin:$PATH

2. Verify that you are using the Morpheus embedded gem by executing the command: which gem. You should see the path /opt/morpheus/embedded/bin/gem

3. Install the elastic-util gem by executing: gem install elastic-util if you don’t want the documentation then execute gem install elastic-util --no-ri --no-rdoc

4. Stop the Morpheus application by executing morpheus-ctl stop morpheus-ui, this will stop creating new documents in ElasticSearch.

5. Create a backup of the ElasticSearch indices by executing: elastic-util backup http://localhost:9200 /root/es_backup, you can change the location of the backup to any file location. You can also pass the --force argument to overwrite the existing location if you are repeating the backup.

6. Upgrade Morpheus as usual by executing the package upgrade command dpkg -i morpheus-appliance_3.2.0-1_amd64.deb or rpm -U morpheus-appliance-3.2.0-1.el7.x86_64.rpm, and run morpheus-ctl reconfigure to complete the upgrade process.

7. You can start Morpheus at this point to bring up the Morpheus application by executing: morpheus-ctl start morpheus-ui.

Note: Make sure that Morpheus is fully started before moving on to the next step.

Once the application has started, a new ElasticSearch node is created with default data, to import your data from the backup execute: morpheus-ctl elastic-util restore http://localhost:9200 /root/es_backup, substitute the path you used during the backup if different from above.

Note: The restore may take several hours depending on the amount of data to restore. You can run this while running Morpheus.

This deployment configuration assumes that you manage an ElasticSearch cluster externally from Morpheus. The steps for upgrading ElasticSearch from 1.x to 5.x are located on the ElasticSearch website. Run the following from a “master” appliance, it has the required Ruby installed in the Morpheus full stack directory. Ensure that the appliance
can reach at least one ElasticSearch node over port 9200 (http). Also, make sure there is enough disk space to hold the exported data on the appliance.

1. Login to the master appliance as a user that has sudo privileges and can switch to the root user `sudo su -`. You can run the following commands under sudo, but you will need to pass the PATH to the Morpheus embedded directory.

2. Export the Morpheus embedded path to your environment by executing: `export PATH=/opt/morpheus/sbin:/opt/morpheus/sbin:/opt/morpheus/embedded/sbin:/opt/morpheus/embedded/bin:$PATH`

3. Verify that you are using the Morpheus embedded gem by executing the command: `which gem`. You should see the path `/opt/morpheus/embedded/bin/gem`

4. Install the elastic-util gem by executing: `gem install elastic-util` if you don’t want the documentation then execute `gem install elastic-util --no-ri --no-rdoc`

5. Stop all the Morpheus application instances by executing `morpheus-ctl stop morpheus-ui` on each appliance node, this will stop creating new documents in ElasticSearch.

6. Create a backup of the ElasticSearch indices by executing: `elastic-util backup http://xxx.xxx.xxx.xxx:9200 /root/es_backup`, you can change the location of the backup to any file location. You can also pass the `--force` argument to overwrite the existing location if you are repeating the backup.

   **Note:** The next steps are done on the ElasticSearch node(s).

7. Stop ElasticSearch on each node.

8. Backup the ElasticSearch config directory for each node, normally located at `/etc/elasticsearch/`.

9. Since the index data between 1.x and 5.x is incompatible, delete the data from the data directory normally located at `/var/lib/elasticsearch`. To prepare for future upgrades make sure that you delete the cluster name directory as well, ie morpheus.

10. Upgrade ElasticSearch, use the method that best fits your situation ie pkg, tar, or zip.

11. Remove unsupported configuration from the existing ElasticSearch configuration

    • `index.number_of_shards`
    • `index.number_of_replicas`
    • `discovery.zen.ping.multicast`

12. Replace or update the package installed configuration with your existing configuration if it was overwritten.

    • Set `network.host` or `network.bind_ip` and `network.publish_ip` accordingly to your network configuration.

13. Start ElasticSearch on each node and form a new cluster.

14. Verify you have a good cluster by executing: `curl http://xxx.xxx.xxx.xxx:9200/_cluster/health?pretty`, check for the number of nodes and that you have a green status.

   **Note:** The next steps are done on the Morpheus “master” node.

15. Upgrade Morpheus as usual by executing the package upgrade command `dpkg -i morpheus-appliance_3.2.0-1_amd64.deb` or `rpm -U morpheus-appliance-3.2.0-1.el7.x86_64.rpm`, and run `morpheus-ctl reconfigure` to complete the upgrade process.
16. You can start Morpheus on the master node only at this point to bring up the Morpheus application by executing:

```
morpheus-ctl start morpheus-ui
```

**Note:** Make sure that Morpheus is fully started before moving on to the next step.

17. Once the application has started, a new ElasticSearch node is created with default data, to import your data from the backup execute:

```
```

**Note:** The restore may take several hours depending on the amount of data to restore. You can run this while running Morpheus.

18. Move to the next Morpheus appliance and upgrade it by executing the package upgrade command:

```
dpkg -i morpheus-appliance_3.2.0-1_amd64.deb
```

or

```
rpm -U morpheus-appliance-3.2.0-1.el7.x86_64.rpm
```

and run

```
morpheus-ctl reconfigure
```

to complete the upgrade process.

19. Start Morpheus by executing:

```
morpheus-ctl start morpheus-ui
```

20. Upgrade the rest of the Morpheus appliances in your environment.

### 12.13 v3.3.1

Release Date 4/15/2018

**Important:** If upgrading from versions earlier than 3.2.0 please follow the 3.2.0+ upgrade instructions below the release notes.

**Important:** Appliance Elasticsearch communication in 3.3.1 switches from transport protocol 9300 port to http 9200

#### 12.13.1 3.3.1 New Features

- Azure Scale Sets support added
- Azure: Network Security Group selection no longer required
- Bluecat: Network filter option added to Integration settings
- Cypher: TFvars added for Terraform. Allows variable files stored in cypher to be used with Terraform Templates.
- Global Search: Apps & Library Items categories added
- Infoblox: Host and Zone Record Sync added
- Infoblox: Manual Host and Zone record creation, deletion and reservations added
- Infrastructure- Hosts: Typing DELETE now required when removing infrastructure
- Instances: Mute Checks option added on shutdown
- Instance Details: Last Deployment Name and Version added
• KeyPairs: Validation and conversion service added
• Library: Morpheus Node Types for CentOS 7.3 for Nutanix and ESXi added
• Load Balancers: F5 Pool Creation Validation, VIP Creation Validation, VIP Creation SSL Profile and Remove Policies Options added
• Morpheus Appliance: Major Speed and resource utilization improvements. Please note Appliance Elasticsearch communication in 3.3.1 switches from transport protocol 9300 port to http 9200
• Networks- IP Pools: Used and Total IPs progress bar added
• Networks- IP Pools: IP Pool Detail Pages added
• Networks - Services: IPAM Service Detail Pages added with Host Record Grids and List views.
• Networks - IP Pools: Created date and created by user tracking added to IP assignments.
• Networks: Domain Detail Pages added
• Networks - Services: DNS Services Zone Record sync added
• Oracle Cloud: Ability to provision by OCID added
• Oracle Cloud: Multiple Compartment support and default Compartment selection added
• Oracle Cloud: Provisioning improvements
• Oracle Cloud: Reconfigure added
• Plans: Cores Per Socket specification added to VMware type plans
• Provisioning - Automation: Scale Thresholds section added. Scale Thresholds can be pre-defined and selected when scaling Instances.
• Reports: Costs added to Virtual Machine Inventory Summary report
• Reports: Provision Times added to exported Virtual Machine Inventory Summary reports
• Templates: TFvars selection added
• VCD: Custom Library Nodes added
• VCD: Virtual Image upload added
• Virtual Images: Minimum Ram Requirement field added. Limits which plans will be available for selection at provision time.

12.13.2 3.3.1 Fixes

• Fix for Windows domain join guest user and password not being set
• Fix for Error when setting custom group access on subtenant role
• Fix for Favicon resetting to default on whitelabeling
• Analytics Group and Cloud filter fix
• Fix for API: groups list timing out in high usage environments
• Fix for Nutanix Cloudbase-Init metadata
• Fix for editing and saving Bluecat Integration creating duplicate networks
• Fix for Baremetal: Convert to Managed - creating docker check
• Fix for synced service plans remaining after some cloud deletions
• Fix for KeyPairs 403 error when invalid KeyPair exists
• Fix for Azure Managed Disk error when no Azure Storage Accounts exists
• Fix for NetScaler: unable to add load balancer when using SSL
• Fix for VMware and Nutanix duplicate VM records
• Fix for VMware parent host record sync
• Fix for error creating an App with Existing Instance
• Fix for edit option shown in sub-tenant groups cloud tab on clouds owned by master tenant
• Auto cleanup of Azure Deployment records added

Important: If upgrading from versions earlier than 3.2.0 please follow the 3.2.0+ upgrade instructions below

12.13.3 3.2.0+ Upgrades

Upgrading from previous versions of Morpheus to 3.2.0 or later requires upgrading ElasticSearch to 5.4.1 or 5.x. We do not support ElasticSearch 6.x at this time. This upgrade requires an export and import of Morpheus ElasticSearch data if you want to retain logs, backup history, statistics, and check history of your instances. If you do not need to retain that data you can skip the ElasticSearch migration. Upgrading to 3.2.0 will create a blank ElasticSearch node with no data. Your Morpheus layout configuration will determine how to migrate your ElasticSearch data: all-in-one or distributed high availability.

This deployment configuration is the default mode for Morpheus and contains a single ElasticSearch instance on the appliance. The migration steps are as follows:

1. Login to your appliance as a user that has sudo privileges and can switch to the root user sudo su -. You can run the following commands under sudo, but you will need to pass the PATH to the Morpheus embedded directory. Export the Morpheus embedded path to your environment by executing: export PATH=/opt/morpheus/sbin:/opt/morpheus/sbin:/opt/morpheus/embedded/sbin:/opt/morpheus/embedded/bin:$PATH

2. Verify that you are using the Morpheus embedded gem by executing the command: which gem. You should see the path /opt/morpheus/embedded/bin/gem

3. Install the elastic-util gem by executing: gem install elastic-util if you don’t want the documentation then execute gem install elastic-util --no-ri --no-rdoc

4. Stop the Morpheus application by executing morpheus-ctl stop morpheus-ui, this will stop creating new documents in ElasticSearch.

5. Create a backup of the ElasticSearch indices by executing: elastic-util backup http://localhost:9200 /root/es_backup, you can change the location of the backup to any file location. You can also pass the --force argument to overwrite the existing location if you are repeating the backup.

6. Upgrade Morpheus as usual by executing the package upgrade command dpkg -i morpheus-appliance_3.2.0-1_amd64.deb or rpm -U morpheus-appliance-3.2.0-1.el7.x86_64.rpm, and run morpheus-ctl reconfigure to complete the upgrade process.

7. You can start Morpheus at this point to bring up the Morpheus application by executing: morpheus-ctl start morpheus-ui.

Note: Make sure that Morpheus is fully started before moving on to the next step.
Once the application has started, a new ElasticSearch node is created with default data, to import your data from the backup execute: morpheus-ctl elastic-util restore http://localhost:9200 /root/es_backup, substitute the path you used during the backup if different from above.

**Note:** The restore may take several hours depending on the amount of data to restore. You can run this while running Morpheus.

This deployment configuration assumes that you manage an ElasticSearch cluster externally from Morpheus. The steps for upgrading ElasticSearch from 1.x to 5.x are located on the ElasticSearch website. Run the following from a “master” appliance, it has the required Ruby installed in the Morpheus full stack directory. Ensure that the appliance can reach at least one ElasticSearch node over port 9200 (http). Also, make sure there is enough disk space to hold the exported data on the appliance.

1. Login to the master appliance as a user that has sudo privileges and can switch to the root user `sudo su -`. You can run the following commands under sudo, but you will need to pass the PATH to the Morpheus embedded directory.

2. Export the Morpheus embedded path to your environment by executing: `export PATH=/opt/morpheus/sbin:/opt/morpheus/embedded/sbin:/opt/morpheus/embedded/bin:$PATH`

3. Verify that you are using the Morpheus embedded gem by executing the command: `which gem`. You should see the path `/opt/morpheus/embedded/bin/gem`

4. Install the elastic-util gem by executing: `gem install elastic-util` if you don’t want the documentation then execute `gem install elastic-util --no-ri --no-rdoc`

5. Stop all the Morpheus application instances by executing `morpheus-ctl stop morpheus-ui` on each appliance node, this will stop creating new documents in ElasticSearch.

6. Create a backup of the ElasticSearch indices by executing: `elastic-util backup http://xxx.xxx.xxx.xxx:9200 /root/es_backup`, you can change the location of the backup to any file location. You can also pass the `--force` argument to overwrite the existing location if you are repeating the backup.

**Note:** The next steps are done on the ElasticSearch node(s).

7. Stop ElasticSearch on each node.

8. Backup the ElasticSearch config directory for each node, normally located at `/etc/elasticsearch/`

9. Since the index data between 1.x and 5.x is incompatible, delete the data from the data directory normally located at `/var/lib/elasticsearch`. To prepare for future upgrades make sure that you delete the cluster name directory as well, ie morpheus.

10. Upgrade ElasticSearch, use the method that best fits your situation ie pkg, tar, or zip.

11. Remove unsupported configuration from the existing ElasticSearch configuration

    - `index.number_of_shards`
    - `index.number_of_replicas`
    - `discovery.zen.ping.multicast`

12. Replace or update the package installed configuration with your existing configuration if it was overwritten.

    - `Set network.host or network.bind_ip and network.publish_ip accordingly to your network configuration.`

13. Start ElasticSearch on each node and form a new cluster.
14. Verify you have a good cluster by executing: `curl http://xxx.xxx.xxx.xxx:9200/_cluster/health?pretty`, check for the number of nodes and that you have a green status.

**Note:** The next steps are done on the Morpheus “master” node.

15. Upgrade Morpheus as usual by executing the package upgrade command `dpkg -i morpheus-appliance_3.2.0-1_amd64.deb` or `rpm -U morpheus-appliance-3.2.0-1.el7.x86_64.rpm`, and run `morpheus-ctl reconfigure` to complete the upgrade process.

16. You can start Morpheus on the master node only at this point to bring up the Morpheus application by executing: `morpheus-ctl start morpheus-ui`.

**Note:** Make sure that Morpheus is fully started before moving on to the next step.

17. Once the application has started, a new ElasticSearch node is created with default data, to import your data from the backup execute: `morpheus-ctl elastic-util restore http://xxx.xxx.xxx.xxx:9200 /root/es_backup`, substitute the path you used during the backup if different from above.

**Note:** The restore may take several hours depending on the amount of data to restore. You can run this while running Morpheus.

18. Move to the next Morpheus appliance and upgrade it by executing the package upgrade command `dpkg -i morpheus-appliance_3.2.0-1_amd64.deb` or `rpm -U morpheus-appliance-3.2.0-1.el7.x86_64.rpm`, and run `morpheus-ctl reconfigure` to complete the upgrade process.


20. Upgrade the rest of the Morpheus appliances in your environment.

### 12.14 v3.3.0

**Release Date 3/20/2018**

**Important:** Morpheus v3.2.0+ introduces Global Search, which requires an Elasticsearch upgrade. Upgrading from previous versions of Morpheus to a 3.2.0 or later requires you to upgrade ElasticSearch to 5.4.1 or 5.x. We do not support ElasticSearch 6.x at this time. This upgrade requires you to export and import your Morpheus ElasticSearch data if you want to retain logs, backup history, statistics, and check history of your instances. If you do not need to retain that data you can skip the ElasticSearch migration. Upgrading to 3.2.0+ will create a blank ElasticSearch node with no data. Your Morpheus layout configuration will determine how to migrate your ElasticSearch data: all-in-one, distributed high availability, or Morpheus clustered appliances.

Please refer to upgrade instructions below the release notes.

**Note:** Upgrading from 3.2.0 to 3.3.0 does not require an Elasticsearch upgrade.
12.14.1 New Features

- Clouds: Oracle Cloud added
- Apps & Blueprints: ARM Blueprints added
- Apps & Blueprints: Teraform Blueprints
- Localization: Spanish, French, German translations added
- Azure: All provisioning now utilizes ARM Blueprints
- Apps & Blueprints: Blueprint type and icons added
- Hosts: RPC Port now configurable on Edit -> Host
- API: Scheduling added
- KeyPairs: Additional Keypair Validation added
- Administration -> Provisioning -> Settings: Require Environment Selection Flag added
- Administration -> Provisioning -> Environments: Actions - Hide added for Environments
- Identity Sources: SAML error handling enhancements
- VMware: Task customization domain join enhancements

12.14.2 Fixes

- Fix for Static IP address field losing focus in App Blueprints
- Updates to UI Header for Localizations
- Fix for error on searching for Cloud Foundry marketplace service
- Fix for VMware 2 Disk Blueprints where 2nd disk is named *.2.vmdk
- Fix for Instance Configuration dropdown sorted randomly
- Fix for VMware Image sync duplications

Important: For upgrades to 3.2.0+ please follow the 3.2.0+ upgrade instructions below!

12.14.3 3.2.0+ Upgrades

Upgrading from previous versions of Morpheus to 3.2.0 or later requires upgrading ElasticSearch to 5.4.1 or 5.x. We do not support ElasticSearch 6.x at this time. This upgrade requires an export and import of Morpheus ElasticSearch data if you want to retain logs, backup history, statistics, and check history of your instances. If you do not need to retain that data you can skip the ElasticSearch migration. Upgrading to 3.2.0 will create a blank ElasticSearch node with no data. Your Morpheus layout configuration will determine how to migrate your ElasticSearch data: all-in-one or distributed high availability.

This deployment configuration is the default mode for Morpheus and contains a single ElasticSearch instance on the appliance. The migration steps are as follows:

1. Login to your appliance as a user that has sudo privileges and can switch to the root user sudo su -.
   You can run the following commands under sudo, but you will need to pass the PATH to the Morpheus embedded directory. Export the Morpheus embedded path to your environment
by executing: `export PATH=/opt/morpheus/sbin:/opt/morpheus/sbin:/opt/morpheus/ embedded/sbin:/opt/morpheus/embedded/bin:$PATH`

2. Verify that you are using the Morpheus embedded gem by executing the command: `which gem`. You should see the path `/opt/morpheus/embedded/bin/gem`

3. Install the elastic-util gem by executing: `gem install elastic-util` if you don’t want the documentation then execute `gem install elastic-util --no-ri --no-rdoc`

4. Stop the Morpheus application by executing `morpheus-ctl stop morpheus-ui`, this will stop creating new documents in ElasticSearch.

5. Create a backup of the ElasticSearch indices by executing: `elastic-util backup http://localhost:9200 /root/es_backup`, you can change the location of the backup to any file location. You can also pass the `--force` argument to overwrite the existing location if you are repeating the backup.

6. Upgrade Morpheus as usual by executing the package upgrade command `dpkg -i morpheus-appliance_3.2.0-1_amd64.deb` or `rpm -U morpheus-appliance-3.2.0-1.el7.x86_64.rpm`, and run `morpheus-ctl reconfigure` to complete the upgrade process.

7. You can start Morpheus at this point to bring up the Morpheus application by executing: `morpheus-ctl start morpheus-ui`.

**Note:** Make sure that Morpheus is fully started before moving on to the next step.

Once the application has started, a new ElasticSearch node is created with default data, to import your data from the backup execute: `morpheus-ctl elastic-util restore http://localhost:9200 /root/es_backup`, substitute the path you used during the backup if different from above.

**Note:** The restore may take several hours depending on the amount of data to restore. You can run this while running Morpheus.

This deployment configuration assumes that you manage an ElasticSearch cluster externally from Morpheus. The steps for upgrading ElasticSearch from 1.x to 5.x are located on the ElasticSearch website. Run the following from a “master” appliance, it has the required Ruby installed in the Morpheus full stack directory. Ensure that the appliance can reach at least one ElasticSearch node over port 9200 (http). Also, make sure there is enough disk space to hold the exported data on the appliance.

1. Login to the master appliance as a user that has sudo privileges and can switch to the root user `sudo su -`. You can run the following commands under sudo, but you will need to pass the PATH to the Morpheus embedded directory.

2. Export the Morpheus embedded path to your environment by executing: `export PATH=/opt/morpheus/sbin:/opt/morpheus/sbin:/opt/morpheus/embedded/sbin:/opt/morpheus/embedded/bin:$PATH`

3. Verify that you are using the Morpheus embedded gem by executing the command: `which gem`. You should see the path `/opt/morpheus/embedded/bin/gem`

4. Install the elastic-util gem by executing: `gem install elastic-util` if you don’t want the documentation then execute `gem install elastic-util --no-ri --no-rdoc`

5. Stop all the Morpheus application instances by executing `morpheus-ctl stop morpheus-ui` on each appliance node, this will stop creating new documents in ElasticSearch.

6. Create a backup of the ElasticSearch indices by executing: `elastic-util backup http://xxx.xxx.xxx:9200 /root/es_backup`, you can change the location of the backup to any file location. You can also pass the `--force` argument to overwrite the existing location if you are repeating the backup.
7. Stop ElasticSearch on each node.

8. Backup the ElasticSearch config directory for each node, normally located at /etc/elasticsearch/.

9. Since the index data between 1.x and 5.x is incompatible, delete the data from the data directory normally located at /var/lib/elasticsearch. To prepare for future upgrades make sure that you delete the cluster name directory as well, ie morpheus.

10. Upgrade ElasticSearch, use the method that best fits your situation ie pkg, tar, or zip.

11. Remove unsupported configuration from the existing ElasticSearch configuration
   - index.number_of_shards
   - index.number_of_replicas
   - discovery.zen.ping.multicast

12. Replace or update the package installed configuration with your existing configuration if it was overwritten.
   - Set network.host or network.bind_ip and network.publish_ip accordingly to your network configuration.

13. Start ElasticSearch on each node and form a new cluster.

14. Verify you have a good cluster by executing: curl http://xxx.xxx.xxx.xxx:9200/_cluster/health?pretty, check for the number of nodes and that you have a green status.

Note: The next steps are done on the Morpheus "master" node.

15. Upgrade Morpheus as usual by executing the package upgrade command dpkg -i morpheus-appliance_3.2.0-1_amd64.deb or rpm -U morpheus-appliance-3.2.0-1.el7.x86_64.rpm, and run morpheus-ctl reconfigure to complete the upgrade process.

16. You can start Morpheus on the master node only at this point to bring up the Morpheus application by executing: morpheus-ctl start morpheus-ui.

Note: Make sure that Morpheus is fully started before moving on to the next step.

17. Once the application has started, a new ElasticSearch node is created with default data, to import your data from the backup execute: morpheus-ctl elastic-util restore http://xxx.xxx.xxx.xxx:9200 /root/es_backup, substitute the path you used during the backup if different from above.

Note: The restore may take several hours depending on the amount of data to restore. You can run this while running Morpheus.

18. Move to the next Morpheus appliance and upgrade it by executing the package upgrade command dpkg -i morpheus-appliance_3.2.0-1_amd64.deb or rpm -U morpheus-appliance-3.2.0-1.el7.x86_64.rpm, and run morpheus-ctl reconfigure to complete the upgrade process.


20. Upgrade the rest of the Morpheus appliances in your environment.
12.15 v3.2.2

Release Date 5/2/2018

**Important:** Morpheus v3.2.0+ introduces Global Search, which requires an Elasticsearch upgrade. Upgrading from previous versions of Morpheus to a 3.2.0 or later requires you to upgrade Elasticsearch to 5.4.1 or 5.x. We do not support Elasticsearch 6.x at this time. This upgrade requires you to export and import your Morpheus Elasticsearch data if you want to retain logs, backup history, statistics, and check history of your instances. If you do not need to retain that data you can skip the Elasticsearch migration. Upgrading to 3.2.0+ will create a blank Elasticsearch node with no data. Your Morpheus layout configuration will determine how to migrate your Elasticsearch data: all-in-one, distributed high availability, or Morpheus clustered appliances.

Please refer to upgrade instructions below the release notes.

### 12.15.1 New Features

- Alibaba - Docker Host provisioning added
- ServiceNow: Kingston support for SNOW Morpheus plug-in

### 12.15.2 Fixes

- Apps: Fix for unintended firewall evaluation when using shared resource in an app
- Backups: Fix for expired backup archives not deleting on S3 backup storage provider
- Billing: Fix for billing API not returning usages for zones that no longer exist
- Cloudbase-init: Fix for user data and DNS client settings missing
- Cloud Foundry: Better handling when creating a space with a user that does not have the correct permissions
- Deployments: Fix for deployment modal automatically selecting the last deployment used
- F5 Load Balancer: Fix for syncing in duplicate unmanaged virtual servers
- Load Balancers: Fix for edit modal typo & styling issue
- MacStadium: Fix for duplicate Virtual Machines
- NetScaler: Fix for adding load balancer when using SSL
- Policies: Lifecycle extension message fixes
- Pricing: Fix for platform price missing at provisioning stage
- SCVMM: Fix for cloud deletion
- Veeam: Fix for Templates/Jobs not populating
- VMware: Fix for VM hypervisor host sync
- Windows: Fix for wrong Ethernet adapter type for being set on uploaded windows images.
- Xen: Fix for snapshots not being cleaned up

**Important:** For upgrades to 3.2.0 please follow the 3.2.0 upgrade instructions below!
12.15.3 3.2.0+ Upgrades

Upgrading from previous versions of Morpheus to 3.2.0 or later requires upgrading ElasticSearch to 5.4.1 or 5.x. We do not support ElasticSearch 6.x at this time. This upgrade requires an export and import of Morpheus ElasticSearch data if you want to retain logs, backup history, statistics, and check history of your instances. If you do not need to retain that data you can skip the ElasticSearch migration. Upgrading to 3.2.0 will create a blank ElasticSearch node with no data. Your Morpheus layout configuration will determine how to migrate your ElasticSearch data: all-in-one or distributed high availability.

This deployment configuration is the default mode for Morpheus and contains a single ElasticSearch instance on the appliance. The migration steps are as follows:

1. Login to your appliance as a user that has sudo privileges and can switch to the root user sudo su -. You can run the following commands under sudo, but you will need to pass the PATH to the Morpheus embedded directory. Export the Morpheus embedded path to your environment by executing:

   ```bash
   export PATH=/opt/morpheus/sbin:/opt/morpheus/sbin:/opt/morpheus/embedded/sbin:/opt/morpheus/embedded/bin:$PATH
   ```

2. Verify that you are using the Morpheus embedded gem by executing the command: `which gem`. You should see the path `/opt/morpheus/embedded/bin/gem`

3. Install the elastic-util gem by executing:

   ```bash
   gem install elastic-util
   ```

   If you don't want the documentation then execute
   ```bash
   gem install elastic-util --no-ri --no-rdoc
   ```

4. Stop the Morpheus application by executing `morpheus-ctl stop morpheus-ui`, this will stop creating new documents in ElasticSearch.

5. Create a backup of the ElasticSearch indices by executing:

   ```bash
   elastic-util backup http://localhost:9200 /root/es_backup
   ```

   You can change the location of the backup to any file location. You can also pass the `--force` argument to overwrite the existing location if you are repeating the backup.

6. Upgrade Morpheus as usual by executing the package upgrade command

   ```bash
   dpkg -i morpheus-appliance_3.2.0-1_amd64.deb
   ```

   or

   ```bash
   rpm -U morpheus-appliance-3.2.0-1.el7.x86_64.rpm
   ```

   and run `morpheus-ctl reconfigure` to complete the upgrade process.

7. You can start Morpheus at this point to bring up the Morpheus application by executing:

   ```bash
   morpheus-ctl start morpheus-ui
   ```

Note: Make sure that Morpheus is fully started before moving on to the next step.

Once the application has started, a new ElasticSearch node is created with default data, to import your data from the backup execute:

```bash
```

Note: The restore may take several hours depending on the amount of data to restore. You can run this while running Morpheus.

This deployment configuration assumes that you manage an ElasticSearch cluster externally from Morpheus. The steps for upgrading ElasticSearch from 1.x to 5.x are located on the ElasticSearch website. Run the following from a “master” appliance, it has the required Ruby installed in the Morpheus full stack directory. Ensure that the appliance can reach at least one ElasticSearch node over port 9200 (http). Also, make sure there is enough disk space to hold the exported data on the appliance.

1. Login to the master appliance as a user that has sudo privileges and can switch to the root user sudo su -. You can run the following commands under sudo, but you will need to pass the PATH to the Morpheus embedded directory.
2. Export the Morpheus embedded path to your environment by executing: export PATH=/opt/morpheus/sbin:/opt/morpheus/embedded/sbin:$PATH

3. Verify that you are using the Morpheus embedded gem by executing the command: which gem. You should see the path /opt/morpheus/embedded/bin/gem

4. Install the elastic-util gem by executing: gem install elastic-util if you don’t want the documentation then execute gem install elastic-util --no-ri --no-rdoc

5. Stop all the Morpheus application instances by executing morpheus-ctl stop morpheus-ui on each appliance node, this will stop creating new documents in ElasticSearch.

6. Create a backup of the ElasticSearch indices by executing: elastic-util backup http://xxx.xxx.xxx:9200 /root/es_backup, you can change the location of the backup to any file location. You can also pass the --force argument to overwrite the existing location if you are repeating the backup.

**Note:** The next steps are done on the ElasticSearch node(s).

7. Stop ElasticSearch on each node.

8. Backup the ElasticSearch config directory for each node, normally located at /etc/elasticsearch/.

9. Since the index data between 1.x and 5.x is incompatible, delete the data from the data directory normally located at /var/lib/elasticsearch. To prepare for future upgrades make sure that you delete the cluster name directory as well, ie morpheus.

10. Upgrade ElasticSearch, use the method that best fits your situation ie pkg, tar, or zip.

11. Remove unsupported configuration from the existing ElasticSearch configuration

   • index.number_of_shards
   • index.number_of_replicas
   • discovery.zen.ping.multicast

12. Replace or update the package installed configuration with your existing configuration if it was overwritten.

   • Set network.host or network.bind_ip and network.publish_ip accordingly to your network configuration.

13. Start ElasticSearch on each node and form a new cluster.

14. Verify you have a good cluster by executing: curl http://xxx.xxx.xxx.xxx:9200/_cluster/health?pretty, check for the number of nodes and that you have a green status.

**Note:** The next steps are done on the Morpheus “master” node.

15. Upgrade Morpheus as usual by executing the package upgrade command dpkg -i morpheus-appliance_3.2.0-1_amd64.deb or rpm -U morpheus-appliance-3.2.0-1.el7.x86_64.rpm, and run morpheus-ctl reconfigure to complete the upgrade process.

16. You can start Morpheus on the master node only at this point to bring up the Morpheus application by executing: morpheus-ctl start morpheus-ui.

**Note:** Make sure that Morpheus is fully started before moving on to the next step.
17. Once the application has started, a new ElasticSearch node is created with default data, to import your data from the backup execute: `morpheus-ctl elastic-util restore http://xxx.xxx.xxx.xxx:9200 /root/es_backup`, substitute the path you used during the backup if different from above.

**Note:** The restore may take several hours depending on the amount of data to restore. You can run this while running Morpheus.

18. Move to the next Morpheus appliance and upgrade it by executing the package upgrade command `dpkg -i morpheus-appliance_3.2.0-1_amd64.deb` or `rpm -U morpheus-appliance-3.2.0-1.el7.x86_64.rpm`, and run `morpheus-ctl reconfigure` to complete the upgrade process.


20. Upgrade the rest of the Morpheus appliances in your environment.

### 12.16 v3.2.1

Release Date 3/23/2018

**Important:** Morpheus v3.2.0+ introduces Global Search, which requires an Elasticsearch upgrade. Upgrading from previous versions of Morpheus to a 3.2.0 or later requires you to upgrade Elasticsearch to 5.4.1 or 5.x. We do not support Elasticsearch 6.x at this time. This upgrade requires you to export and import your Morpheus Elasticsearch data if you want to retain logs, backup history, statistics, and check history of your instances. If you do not need to retain that data you can skip the Elasticsearch migration. Upgrading to 3.2.0+ will create a blank Elasticsearch node with no data. Your Morpheus layout configuration will determine how to migrate your Elasticsearch data: all-in-one, distributed high availability, or Morpheus clustered appliances.

Please refer to upgrade instructions below the release notes.

### 12.16.1 New Features

- Instances: Last Deployment Name/Version added to Instance list & details sections
- Library: Minimum Memory field added to Layouts. Only the service plan options meeting this requirement will be displayed during provisioning.
- Load Balancers: F5- VIP Creation Validation added
- Load Balancers: F5- Pool Creation Validation added
- Load Balancers: F5- SSL Profile Option during VIP Creation added
- Load Balancers: F5- SSL Remove Policies Option during VIP Creation added
- Networks: Network filter added to Bluecat Service.
- Virtual Images: Minimum Memory field add to Virtual Images. Only the service plan options meeting this requirement will be displayed during provisioning. Note this will override any memory requirement set on the virtual image.
- VMware: Cores per Socket Added to VMware type Service Plans
- VMware: Sync time optimizations & memory utilization improvements
12.16.2 Fixes

- Fix for VMware MV inventory issue when VM's exist with same name in different resource pools
- Fix for setting custom group access on legacy subtenant role.
- Fix for white labeling favicon resetting to default
- Fix for Analytics filter issues when filtering by Cloud or Group
- Fix for API & CLI groups list timeouts in high usage environments
- Fix for Nutanix Cloudbase-init metadata
- Fix for Instance Removal from CLI not recording user
- Fix for Bare metal: Convert to Managed creating Docker type check
- Fix for Cloud Delete: service plan foreign key constraint prevents deleting of service plans during cloud delete
- Fix for the global search HA replica count being set to 0 instead of 1

Important: For upgrades to 3.2.0 please follow the 3.2.0 upgrade instructions below!

12.16.3 3.2.0+ Upgrades

Upgrading from previous versions of Morpheus to 3.2.0 or later requires upgrading ElasticSearch to 5.4.1 or 5.x. We do not support ElasticSearch 6.x at this time. This upgrade requires an export and import of Morpheus ElasticSearch data if you want to retain logs, backup history, statistics, and check history of your instances. If you do not need to retain that data you can skip the ElasticSearch migration. Upgrading to 3.2.0 will create a blank ElasticSearch node with no data. Your Morpheus layout configuration will determine how to migrate your ElasticSearch data: all-in-one or distributed high availability.

This deployment configuration is the default mode for Morpheus and contains a single ElasticSearch instance on the appliance. The migration steps are as follows:

1. Login to your appliance as a user that has sudo privileges and can switch to the root user sudo su -. You can run the following commands under sudo, but you will need to pass the PATH to the Morpheus embedded directory. Export the Morpheus embedded path to your environment by executing: export PATH=/opt/morpheus/sbin:/opt/morpheus/sbin:/opt/morpheus/embedded/sbin:/opt/morpheus/embedded/bin:$PATH
2. Verify that you are using the Morpheus embedded gem by executing the command: which gem. You should see the path /opt/morpheus/embedded/bin/gem
3. Install the elastic-util gem by executing: gem install elastic-util if you don’t want the documentation then execute gem install elastic-util --no-ri --no-rdoc
4. Stop the Morpheus application by executing morpheus-ctl stop morpheus-ui, this will stop creating new documents in ElasticSearch.
5. Create a backup of the ElasticSearch indices by executing: elastic-util backup http://localhost:9200 /root/es_backup, you can change the location of the backup to any file location. You can also pass the --force argument to overwrite the existing location if you are repeating the backup.
6. Upgrade Morpheus as usual by executing the package upgrade command dpkg -i morpheus-appliance_3.2.0-1_amd64.deb or rpm -U morpheus-appliance-3.2.0-1.el7.x86_64.rpm, and run morpheus-ctl reconfigure to complete the upgrade process.
7. You can start Morpheus at this point to bring up the Morpheus application by executing: `morpheus-ctl start morpheus-ui`.

Note: Make sure that Morpheus is fully started before moving on to the next step.

Once the application has started, a new ElasticSearch node is created with default data, to import your data from the backup execute: `morpheus-ctl elastic-util restore http://localhost:9200 /root/es_backup`, substitute the path you used during the backup if different from above.

Note: The restore may take several hours depending on the amount of data to restore. You can run this while running Morpheus.

This deployment configuration assumes that you manage an ElasticSearch cluster externally from Morpheus. The steps for upgrading ElasticSearch from 1.x to 5.x are located on the ElasticSearch website. Run the following from a “master” appliance, it has the required Ruby installed in the Morpheus full stack directory. Ensure that the appliance can reach at least one ElasticSearch node over port 9200 (http). Also, make sure there is enough disk space to hold the exported data on the appliance.

1. Login to the master appliance as a user that has sudo privileges and can switch to the root user `sudo su -`. You can run the following commands under sudo, but you will need to pass the PATH to the Morpheus embedded directory.

2. Export the Morpheus embedded path to your environment by executing: `export PATH=/opt/morpheus/sbin:/opt/morpheus/sbin:/opt/morpheus/embedded/sbin:/opt/morpheus/embedded/bin:$PATH`.

3. Verify that you are using the Morpheus embedded gem by executing the command: `which gem`. You should see the path `/opt/morpheus/embedded/bin/gem`.

4. Install the elastic-util gem by executing: `gem install elastic-util` if you don’t want the documentation then execute `gem install elastic-util --no-ri --no-rdoc`.

5. Stop all the Morpheus application instances by executing `morpheus-ctl stop morpheus-ui` on each appliance node, this will stop creating new documents in ElasticSearch.

6. Create a backup of the ElasticSearch indices by executing: `elastic-util backup http://xxx.xxx.xxx.xxx:9200 /root/es_backup`, you can change the location of the backup to any file location. You can also pass the `--force` argument to overwrite the existing location if you are repeating the backup.

Note: The next steps are done on the ElasticSearch node(s).

7. Stop ElasticSearch on each node.

8. Backup the ElasticSearch config directory for each node, normally located at `/etc/elasticsearch/`.

9. Since the index data between 1.x and 5.x is incompatible, delete the data from the data directory normally located at `/var/lib/elasticsearch`. To prepare for future upgrades make sure that you delete the cluster name directory as well, ie morpheus.

10. Upgrade ElasticSearch, use the method that best fits your situation ie pkg, tar, or zip.

11. Remove unsupported configuration from the existing ElasticSearch configuration:
    
    - `index.number_of_shards`
    - `index.number_of_replicas`
12. Replace or update the package installed configuration with your existing configuration if it was overwritten.

13. Start Elasticsearch on each node and form a new cluster.

14. Verify you have a good cluster by executing:
   
   ```
   ```
   
   check for the number of nodes and that you have a green status.

   **Note:** The next steps are done on the Morpheus “master” node.

15. Upgrade Morpheus as usual by executing the package upgrade command
   
   ```
   dpkg -i morpheus-appliance_3.2.0-1_amd64.deb
   or rpm -U morpheus-appliance-3.2.0-1.el7.x86_64.rpm,
   and run morpheus-ctl reconfigure to complete the upgrade process.
   ```

16. You can start Morpheus on the master node only at this point to bring up the Morpheus application by executing:

   ```
   morpheus-ctl start morpheus-ui
   ```

   **Note:** Make sure that Morpheus is fully started before moving on to the next step.

17. Once the application has started, a new Elasticsearch node is created with default data, to import your data from the backup execute:

   ```
   morpheus-ctl elastic-util restore http://xxx.xxx.xxx.xxx:9200/root/es_backup,
   substitute the path you used during the backup if different from above.
   ```

   **Note:** The restore may take several hours depending on the amount of data to restore. You can run this while running Morpheus.

18. Move to the next Morpheus appliance and upgrade it by executing the package upgrade command

   ```
   dpkg -i morpheus-appliance_3.2.0-1_amd64.deb or rpm -U morpheus-appliance-3.2.0-1.el7.x86_64.rpm,
   and run morpheus-ctl reconfigure to complete the upgrade process.
   ```

19. Start Morpheus by executing:

   ```
   morpheus-ctl start morpheus-ui
   ```

20. Upgrade the rest of the Morpheus appliances in your environment.

### 12.17 v3.2.0

**Important:** Morpheus v3.2.0+ introduces Global Search, which requires an Elasticsearch upgrade. Upgrading from previous versions of Morpheus to a 3.2.0 or later requires you to upgrade Elasticsearch to 5.4.1 or 5.x. We do not support Elasticsearch 6.x at this time. This upgrade requires you to export and import your Morpheus Elasticsearch data if you want to retain logs, backup history, statistics, and check history of your instances. If you do not need to retain that data you can skip the Elasticsearch migration. Upgrading to 3.2.0+ will create a blank Elasticsearch node with no data. Your Morpheus layout configuration will determine how to migrate your Elasticsearch data: all-in-one, distributed high availability, or Morpheus clustered appliances.

Please refer to upgrade instructions below the release notes.
12.17.1 New Features

- New Global Search: All of Morpheus can now be searched from the header or at /search.
- UI: Updated header including Global Search, User Avatar, Morpheus Support/Documentation links
- Active Directory: Nested Group Support added
- AWS: GovCloud (West) Region added
- Bluecat: Sync and DNS Improvements
- Domains: Workflows added
- Domains: Guest User setting added
- Library: Morpheus CentOS 7.3 for Azure, Softlayer, Bluemix, DigitalOcean, Xen added
- Library: Templates renamed File Templates
- Policies: Sequence numbers no longer reused once freed
- Power Schedule: Total number of hours saved per month added
- Provisioning: Additional error messages surfaced
- SCVMM: Support for static ip pools added
- SCVMM: Inventory existing VMs added
- VMware: Support for VMware 6.5 Hypervisor Console
- Windows Agent: TLS 1.2 Support added
- CLI: Monitoring - Apps added
- CLI: Monitoring - Groups added
- CLI: User Groups added

12.17.2 Fixes

- Alibaba: Fix for Release Elastic IP
- Alibaba: Fix for Edit Cloud not populating region/vpc
- Alibaba: Fix for Networks recreated on sync
- Alibaba: Fix for issue deleting VM that has backups
- Alibaba: Fix for Elastic IP not surfaced in morpheus
- Hosts: Fix for Add host modal in sub-tenant is not respecting user role group permissions
- Hosts: Fix for bare metal convert to managed not displayed correctly.
- Hosts: Fix for deleting orphaned vm’s
- Infoblox: Fix for add integration not working with fqdn
- Load Balancers: Fix for blank Settings tab for non-system admin roles
- macOS: Fix for macOS User creation
- User Groups: Fix for User Groups only available for master account
- vCD: Fix for invalid instance/computer names
Important: For upgrades to 3.2.0 please follow the 3.2.0 upgrade instructions below!

12.17.3 3.2.0+ Upgrades

Upgrading from previous versions of Morpheus to 3.2.0 or later requires upgrading ElasticSearch to 5.4.1 or 5.x. We do not support ElasticSearch 6.x at this time. This upgrade requires an export and import of Morpheus ElasticSearch data if you want to retain logs, backup history, statistics, and check history of your instances. If you do not need to retain that data you can skip the ElasticSearch migration. Upgrading to 3.2.0 will create a blank ElasticSearch node with no data. Your Morpheus layout configuration will determine how to migrate your ElasticSearch data: all-in-one or distributed high availability.

This deployment configuration is the default mode for Morpheus and contains a single ElasticSearch instance on the appliance. The migration steps are as follows:

1. Login to your appliance as a user that has sudo privileges and can switch to the root user sudo su - . You can run the following commands under sudo, but you will need to pass the PATH to the Morpheus embedded directory. Export the Morpheus embedded path to your environment by executing: export PATH=/opt/morpheus/sbin:/opt/morpheus/sbin:/opt/morpheus/embedded/sbin:/opt/morpheus/embedded/bin:$PATH

2. Verify that you are using the Morpheus embedded gem by executing the command: which gem. You should see the path /opt/morpheus/embedded/bin/gem

3. Install the elastic-util gem by executing: gem install elastic-util if you don’t want the documentation then execute gem install elastic-util --no-ri --no-rdoc

4. Stop the Morpheus application by executing morpheus-ctl stop morpheus-ui, this will stop creating new documents in ElasticSearch.

5. Create a backup of the ElasticSearch indices by executing: elastic-util backup http://localhost:9200 /root/es_backup. You can change the location of the backup to any file location. You can also pass the --force argument to overwrite the existing location if you are repeating the backup.

6. Upgrade Morpheus as usual by executing the package upgrade command dpkg -i morpheus-appliance_3.2.0-1_amd64.deb or rpm -U morpheus-appliance-3.2.0-1.el7.x86_64.rpm, and run morpheus-ctl reconfigure to complete the upgrade process.

7. You can start Morpheus at this point to bring up the Morpheus application by executing: morpheus-ctl start morpheus-ui.

Note: Make sure that Morpheus is fully started before moving on to the next step.

Once the application has started, a new ElasticSearch node is created with default data, to import your data from the backup execute: morpheus-ctl elastic-util restore http://localhost:9200 /root/es_backup, substitute the path you used during the backup if different from above.

Note: The restore may take several hours depending on the amount of data to restore. You can run this while running Morpheus.

This deployment configuration assumes that you manage an ElasticSearch cluster externally from Morpheus. The steps for upgrading ElasticSearch from 1.x to 5.x are located on the ElasticSearch website. Run the following from a “master” appliance, it has the required Ruby installed in the Morpheus full stack directory. Ensure that the appliance
can reach at least one ElasticSearch node over port 9200 (http). Also, make sure there is enough disk space to hold the exported data on the appliance.

1. Login to the master appliance as a user that has sudo privileges and can switch to the root user sudo su -.
   You can run the following commands under sudo, but you will need to pass the PATH to the Morpheus embedded directory.

2. Export the Morpheus embedded path to your environment by executing: export PATH=/opt/morpheus/sbin:/opt/morpheus/sbin:/opt/morpheus/embedded/sbin:/opt/morpheus/embedded/bin:$PATH

3. Verify that you are using the Morpheus embedded gem by executing the command: which gem. You should see the path /opt/morpheus/embedded/bin/gem

4. Install the elastic-util gem by executing: gem install elastic-util if you don’t want the documentation then execute gem install elastic-util --no-ri --no-rdoc

5. Stop all the Morpheus application instances by executing morpheus-ctl stop morpheus-ui on each appliance node, this will stop creating new documents in ElasticSearch.

6. Create a backup of the ElasticSearch indices by executing: elastic-util backup http://xxx.xxx.xxx.xxx:9200 /root/es_backup, you can change the location of the backup to any file location. You can also pass the --force argument to overwrite the existing location if you are repeating the backup.

   Note: The next steps are done on the ElasticSearch node(s).

7. Stop ElasticSearch on each node.

8. Backup the ElasticSearch config directory for each node, normally located at /etc/elasticsearch/.

9. Since the index data between 1.x and 5.x is incompatible, delete the data from the data directory normally located at /var/lib/elasticsearch. To prepare for future upgrades make sure that you delete the cluster name directory as well, ie morpheus.

10. Upgrade ElasticSearch, use the method that best fits your situation ie pkg, tar, or zip.

11. Remove unsupported configuration from the existing ElasticSearch configuration
   - index.number_of_shards
   - index.number_of_replicas
   - discovery.zen.ping.multicast

12. Replace or update the package installed configuration with your existing configuration if it was overwritten.
   - Set network.host or network.bind_ip and network.publish_ip accordingly to your network configuration.

13. Start ElasticSearch on each node and form a new cluster.

14. Verify you have a good cluster by executing: curl http://xxx.xxx.xxx.xxx:9200/_cluster/health?pretty, check for the number of nodes and that you have a green status.

   Note: The next steps are done on the Morpheus “master” node.

15. Upgrade Morpheus as usual by executing the package upgrade command dpkg -i morpheus-appliance_3.2.0-1_amd64.deb or rpm -U morpheus-appliance-3.2.0-1.el7.x86_64.rpm, and run morpheus-ctl reconfigure to complete the upgrade process.
16. You can start Morpheus on the master node only at this point to bring up the Morpheus application by executing: `morpheus-ctl start morpheus-ui`.

**Note:** Make sure that Morpheus is fully started before moving on to the next step.

17. Once the application has started, a new ElasticSearch node is created with default data, to import your data from the backup execute: `morpheus-ctl elastic-util restore http://xxx.xxx.xxx.xxx:9200 /root/es_backup`, substitute the path you used during the backup if different from above.

**Note:** The restore may take several hours depending on the amount of data to restore. You can run this while running Morpheus.

18. Move to the next Morpheus appliance and upgrade it by executing the package upgrade command `dpkg -i morpheus-appliance_3.2.0-1_amd64.deb` or `rpm -U morpheus-appliance-3.2.0-1.el7.x86_64.rpm`, and run `morpheus-ctl reconfigure` to complete the upgrade process.


20. Upgrade the rest of the Morpheus appliances in your environment.

### 12.18 v3.1.5

#### 12.18.1 New Features & Fixes

- VMware: Cloud Sync Performance Improvements (10x)
- Multiple Domain Join Improvements and Fixes
- Alibaba: Technology Filter Type added
- UI: Localization fixes
- Fix for VMware Network and Folder Tenant Assignment
- Windows Agent 1.4.3.0 with Agent Install and Chef Bootstrap Fixes

### 12.19 v3.1.4

#### 12.19.1 New Features

- Cisco ACI: Morpheus now integrates with Cisco ACI. 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.
- Load Balancers: F5 Improvements: Virtual Servers, Nodes and Pools can now be created, edited and deleted.
- Openstack: Network Improvements including Multi-network, Static IP and IP Pool support
- Hyper-V: Network Improvements including Multi-network, Static IP and IP Pool support
- VMware Performance Improvements- 4x increase in VMware sync and performance
- Clouds: New Alibaba Cloud Integration
• UI- Localization support expanded
• Morpheus Windows Agent 1.4.1 with script execution via agent command bus
• Infrastructure: Instance Node Type added to VM detail pages
• Library: New Search Filters
• Library: Option Types can now be re-ordered
• Plans & Pricing: Prices: INCUR CHARGES setting added with running, stopped, and always options.
• vCloud Direct: IP Pools sync added
• SCVMM- Generation option added to provisioning
• Openstack: API token now cached to improve performance
• Instance Details: App associations added
• Amazon: Improved provisioning error details
• XEN: XVA Import added
• Containerized CLI: https://hub.docker.com/r/morpheusdata/morpheus-cli/

12.19.2 Fixes

• Infrastructure: Fix for Hosts stop/start power indicator
• Load Balancers: Fix for Default cloud selected when adding Load Balancer from cloud detail pages
• AWS: Fix for AWS Docker Host service plan assignment
• Networks: Fix for Assign Pool dropdown timeouts
• Network Services: Consul - fix for name requirement not enforced
• Virtual Images: Fix for Morpheus VMware Ubuntu 16.04 image
• Tenancy: Assign to Tenant bulk action listing removed
• Openstack: Keypairs are now removed on zone delete
• vCloud Director: Fix for Provisioning - Datastore selection
• vCloud Director: Fix for error on cloud sync
• Provisioning: Fix for No host selection available for some System Instance types
• Instances - fix for exported variables
• Provisioning: Fix for 32-bit and macOS agent install

12.20 v3.1.3

12.20.1 New Features

• Administration: Local user accounts can now be disabled
• API: Storage Providers added
• Cloud Foundry: Allow free form username input for space user management in Cloud Foundry
• Cloud Foundry: Ability to create a space and add/remove users from a space
• Google Cloud: Network Tagging support added
• Instances: “Open Console” Action added
• Instance Types: Morpheus Ubuntu 16.04 added for AWS, Hyper-V, Xen, ESXi and SCVMM
• Library: Workflows added to Layouts

12.20.2 Fixes

• Apps: Fix for broken image placeholder when creating a new app template in latest Chrome build.
• AWS: Instances: Add Node: not propagating settings from original instance
• Google: Provisioning: Fix for External IP list missing static IPs
• High Availability: Implementation of the quartz lock handler
• Image Builder: Fix for start time displayed in UTC
• Instances: Provisioning: Fix for 500 error if disk size has decimal
• Instances: Removed inaccessible links in sub-tenants for master tenant hosts and cloud
• Library: Scripts: Fix for “Run as User”
• Library: Scripts: Fix for sudo flag
• OracleVM: Fix for Library: add OVM Node Type
• Performance: WinRM Optimizations
• PXE Boot: Fix for validation of Supermicro container and VM server mode boot mapping.

12.21 v3.1.2 & v2.12.5

12.21.1 New Features

3.1.2
• Automation: Services section added
• Cloud Foundry: Space deletion added
• Cloud Foundry: Synced services provisioning added
• Deployments: Services section added
  Instances: Ubuntu 16.04 Added to Morpheus OpenStack, Google, Nutanix and Azure Instance Types
• Load Balancers: LoadFortiADC Load Balancer Integration
• Policies: “Remove Expiration” Action added to Instances for Users with Full Policies Role access
• UI: Column Sorting added to multiple sections
• vCenter: Cluster of Clusters- “All” option added to VMware cloud settings Cluster selection
• vCloud Director: “Add User” option during provisioning added

3.1.2 & 2.12.5
• API: Archives section added
• API: Networks section added
• OracleVM: Virtual Image disk count and sizes now auto-populate in provisioning wizard
• Plans & Pricing: Additional decimal places allowed for in Prices and Costs
• Policies: Lifecycle extension links in emails are now one-time use
• Roles: System “User Admin” role is no longer multitenant

12.21.2 Fixes

• API: Billing query optimizations
• API: Costs removed from API billing when accessing from sub-tenant user
• App Template: Fix for App Template wizard not loading local Amazon Images
• AWS: Fix for “Assign EIP” flag when subnet not set to auto-assign Public IP by default.
• AWS: Fix for Converted to managed Instances attaching service plans and pricing
• Azure: Fix for US Gov pricing shown on EU Azure plans
• Clouds: Fix for starting VM from Virtual Machine list tab within Cloud
• Guidance: Fix when using multiple filters in
• IBM Cloud (Bluemix Platform): Fix for cloud deletion and record cleanup
• Instances: Fix for error on Actions -> Backup from main instances list on converted to managed Instances
• Instances: Fix for inability to select a service plan when deploying HAProxy Instance Type in some environments
• Instances: Fix for Virtual Machine link on Instance with Pending or Denied Approval status
• Instances: Multiple regional Morpheus Virtual Image seed fixes
• Library: Fix for Option Type variables not parsing when exported as Environment Variables
• Monitoring: Fix for Incident re-open button
• OracleVM: Fix for issue with multi-disk Virtual Images
• OracleVM: Fix for Virtual Image dropdown showing unsupported Virtual Images
• OracleVM: Fix for IP Assignment with Infoblox Integration
• Plans and Pricing: Descriptions added for Volume Types
• Reports: Fix for Analytics Report typos
• Reports: Fixes for Sub-Tenants Cloud Reports
• Reports: Tenant report removed from Sub-Tenants
• Roles: Fix for Multitenant User Roles not propagating permission changes
• UI: Fix for lower menu bar moving
• Usage: Fix for multiple and duplicate records
• vCenter: Fix for Hypervisor Console issue when multiple VMware clouds are sharing ESXi Hosts
• vCenter: Fix for additional users not being created for Windows VMware instances when using static ip’s & Virtual Image credentials not populated
• vCloud Director: Sync Status fix
• vCloud Director: Security groups tab added
• vCloud Director: Invalid Apache node type seed removed
• vCloud Director: Fix for Virtual Image sync cleanup
• vCloud Director: Fix for Custom Cores
• vCloud Director: Fix for “Stop Server” Action not fully stopping VM
• vCloud Director: Fix for host record when deleting VM
• Virtual Images: Download option for Synced Virtual Images removed
• Virtual Images: Fixes for error when adding Virtual Image with url with CIFS storage provider

12.22 v3.1.1

12.22.1 New Features

Scheduling Detail Pages New detail pages for Operations -> Scheduling show schedule configurations and the resources schedules are applied to.

Azure Tags Azure Tags can be created using metadata values, and existing Azure tags are now synced.

12.22.2 Other Improvements and Fixes

• Fix for Library Template content edits
• Currency symbol & other styling updates
• VMware Multi-Disk Reconfigure fixes
• Fix for HA Proxy Load Balancer deployment when using Firefox
• Fix for Oracle VM Virtual Image list displaying unsupported Images
• Oracle VM Multi-Disk fixes
• Fix for Removing Azure Load Balancers
• Morpheus Library CentOS AMI regional seed fixes
• Updated vCloud Director artwork
• VMware Hypervisor Console Improvements
• Security improvements
• Sub-tenant HA Proxy Load Balancer provisioning restrictions for Master Tenant Docker Hosts
• Includes everything in v2.12.4

12.23 v3.1.0

12.23.1 New Features

Power Scheduling New Operations: Power Scheduling Feature. 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.
Currency Conversions  Pricing is now converted to the currency set on a Tenant with nightly currency conversions for pricing using exchange rates.

Datastore Group Permissions  Set which Groups can access a Datastore in the Datastore’s Group Access settings.

HP OneView Summary tab  Summary tab added to HP OneView Cloud Detail pages displaying Type, Name, Slot, Model, Serial Number, and Status of Chassis Blades

Network Groups - Round Robin per Instance support  Instance Networks now selected via round robin when using a Network Group, including multiple networks on the same VM, or multiple VMs in the same instance.

Legacy App Blueprint Conversion  App Blueprints from earlier Morpheus builds are converted to support v3.0+ App Blueprint features.

New Cloud Types  vCloud Director and IBM Bluemix Platform Cloud Types added (beta).

12.23.2 Other Additions

- Reports -> Print added
- Azure Multi-network Support added
- VMware async provisioning
- 32-bit Morpheus Agent
- Ubuntu 16.04 added for SoftLayer, DigitalOcean, and Bluemix Morpheus Instance Types
- API and CLI updates: Image Builder, Apps, Blueprints, Archives, --yaml support added.
- Fix for java args in Apps Deployments

Important: There is a potential issue with application startup on fresh installs using Ubuntu 14.04 with Kernel 3.19.xx. If the Morpheus app does not start properly, please upgrade the Linux kernel and restart the morpheus-ui.

12.24 v3.0.1

12.24.1 New Features

New App & Blueprint wizard  Completely rebuilt Provisioning -> Apps and Blueprints sections with multi-config, raw json and yaml input/output, locking fields and boot order added.

New Analytics  Completely rebuilt Analytics section with Cost, Utilization, Instance and Instance Type analytic reports and data visualizations. Quickly analyze storage, cpu or ram usage across clouds or teams, or compare utilization vs cost per resource.

Guidance  The new Guidance feature can analyze your infrastructure and recommend actions to optimize resource utilization with projected cost savings. Morpheus can then act on those recommendations by resizing, shutting down or moving the resources to ensure money isn’t being wasted on underutilized assets.

Image Builder Service  Automate your image builds directly in Morpheus. Configure your builds, add scripts and run to generate vmdk ovf, qcow2, vhd templates from iso’s. Requires VMware cloud with Hypervisor Console enabled.

Expanded User Settings  Users can now set default Group and Cloud Preferences, Linux and Windows User settings, add User Photos.
User Groups  User Groups can be created and then selected during provisioning to add each group members credentials to the Instance.

Kubernetes  Inventory and provision to existing Kubernetes clusters, or provision new Kubernetes clusters.

Expanded Reports  Provisioning, Infrastructure, and Tenant Inventory Reports Added to Operations -> Reports. JSON and CSV Exports added.

Container Mode  Container Mode option added to Cloud settings, can be set to Default Docker, Swarm or Kubernetes. Determines the type of Docker Host that will be provisioned into the Cloud. *Mode must be set before the first Docker Host is provisioned into a Cloud.

12.24.2 New Integrations

- UpCloud
- Cloud Foundry
- IBM Bluemix
- HP OneView
- SCVMM
- Kubernetes
- Jenkins
- Github

12.24.3 Other Additions

- Support added for guest execution on VMware Windows Templates with renamed Administrator user.
- USER CONFIG and DNS OPTIONS sections section added to Provisioning Wizard.
- Disable Agent Based Firewall Management option added to Cloud Settings.
- COST THIS MONTH and AVG MONTHLY COST data added to Cloud Detail pages.
- Service Plans scoping added to Resource Pools and Folders.
- EBS ENCRYPTION option added to Cloud settings
- API & CLI Updates
- Multiple other additions and Improvements.

12.25 v2.12.4

12.25.1 New Features

- Performance Improvements including optimization of Monitoring Availability Service
- Ansible Windows Support
- Error handling and tracking of Ansible runs in Instance History
- Forced sync on Identity Source logins such as Active Directory
- Policies added to CLI
• Optimizations for Tenant creation via API
• HAProxy LoadBalancer restrictions for Tenants.
• Identity Sources: Mapped Roles - Users now get default role & mapped role
• <%=instance.createdByUsername%> variable added

12.25.2 Fixes

• Ansible provision - Instance warning status no longer shown when Ansible is not enabled during provisioning.
• API account creation optimizations
• Fix for Active Directory Group Role removal
• Fix for Trial Version setting on Virtual Image not saving
• Network Services: Bind DNS - wont load
• Fix for Policy: Fixed Host Name not being enforced
• Fix for Delete Tenant nested error messages
• Instance Shutdown: Extend Now styling fix
• Usage host status fixes
• Softlayer/Bluemix: Environment Variables IP Address fix
• Fix for OVM Bug when base image contains more disks than are configured in provision wizard
• Fix for Permissions: Instance Types not respected account level role

Morpheus v2.12.4 is available in the Downloads section of ‘morpheushub.com<https://morpheushub.com/>’.

12.26 v2.12.3

v2.12.3 release date 10/24/2017

12.26.1 New Features

32-bit Agent Support  Morpheus Agent now supports 32-bit images

Cypher User Permission  New Roles Permission CYPHER -> USER allows user level decrypt permissions.

Improved VMware vCenter Session Management. Connections pools significantly reduce vCenter API sessions from Morpheus.

Other Improvements

• Parallel Instance Delete Improvements
• Provisioning Status Task Improvements
• Tenant Delete Improvements
• Security Improvements
12.26.2 Fixes

- Fix for VMware Datastore selection not populating during provisioning in certain circumstances
- Fix for System AMI Virtual Image region sync
- Approval and Workflow inputs restored on shutdown policy form.

Morpheus v2.12.3 is available in the Downloads section of `morpheushub.com<https://morpheushub.com/>`_.

12.27 v2.12.2

v2.12.2 release date 10/9/2017

Morpheus v2.12.2 adds the ServiceNow CMDB Integration, improvements to existing Features and Integrations, and bug fixes and enhancements.

- ServiceNow CMDB Integration: The Morpheus ServiceNow CMDB integration creates a CMDB record upon Instance provision, updates the CMDB state when an instance is removed, and syncs changed Instance states nightly.
- Additional ServiceNow Plugin Improvements
- “Disable Management of Firewall by Agent” option added to Cloud settings.
- Editing existing Environment Variables support added for Windows
- VMware Folder support added to apps and templates
- Nutanix Unmanaged Network Static IP support added
- vmxnet3 set as default VMware Network Adapter type.
- Chef bootstrap process output added to Instance History
- Improved Tenant Deletion
- Improved VMware Folder and Resource Pool sync
- Mobile layout improvements
- Local Chef install url for windows msi added.
- Email layout improvements for broader email client support.
- Chef Integration now determines when FQDN should not be added.
- Improved Provisioning error outputs
- Improvements to User scoped permissions for monitoring, logs and backups.

Fixes:

- Fix for Bulk Network Edit
- Fix for DHCP flag being reset on Nutanix networks upon cloud sync.
- Fix for Agent timestamp handling
- Fix for Dashboard 500 error when user Role Permissions = Monitoring : User
- Fix for Netscaler SSL cert upload
• Fix for server stop/start when inventoried server is converted to managed and Instance Type is applied.
• Additional character handling in Automation Scripts
• Fix for Remove Shutdown Instance Action hanging
• Fix for Instance History purge
• Various other bug fixes and improvements

Morpheus v2.12.2 is available in the Downloads section of ‘morpheushub.com<https://morpheushub.com/>’.

12.28 v2.12.1

Morpheus v2.12.1 adds Console Copy & Paste, VMware Folders, expanded User Scoping Permissions, Nutanix additions, Infoblox additions, and many other Improvements and Fixes.

12.28.1 New Features

Console Copy & Paste
• Copy button added to copy selected text to local Clipboard.
• Paste field added to paste text from local Clipboard. Right click in console to then paste to target.

Additional User Scoping
• Role permissions can now be set to User for Monitoring, Backup, and Logs sections.
• Users will only see information related to their Instances in the corresponding sections, as well as on the Dashboard, when Role permission is set to User

VMware
• VMware Folders now sync and can be targeted for VM and Image destinations, set to active/inactive, and assigned Tenant permissions.
• Storage Type can now be set to Thick or Thin in VMware Cloud settings.
• Boot from ISO support added. ISO’s can now be selected to boot from for VMware provisioning, and can fully be installed using the Hypervisor Console.
• Eject Disk Action also added for VMware technology Instance Types.

Nutanix
• Instances can now be converted to Images in Nutanix using the Import as Image Action. A Virtual Image record with matching meta-data will also be automatically created.
• Disk and Network type selection added to Nutanix technology Instance Types.
• Network Interface Type Selection can be enabled in Nutanix Cloud settings.

Infoblox
• Display Name column added to IP Pools to better identify IP Pools synced from Nutanix.
• Network Filter field added to Infoblox settings. Allows for filtering by field, exact match or regular expression, as well as searching on extended attributes. EX: [network_view=default&*Building=work]
• Tenant Match Attribute field added to Infoblox settings. Allow for auto-assignment of IP pool Groups and individual IP Pools to a tenant.
12.28.2 Other Additions and Improvements

- **Trial Version** flag added under *Virtual Images -> Edit Virtual Image -> Advanced Options*. Flagging a Windows Image as Trial Version will re-arm the trial during provisioning.

- F5 Load Balancer improvements
- HA Proxy Load Balancer improvements
- Citrix Load Balancer improvements
- Chef improvements
- Provisioning: Allow Force Delete
- UI/API/CLI Security Improvements
- Process Service Improvements
- Add Node Action will now only show compatible clouds as target options.
- Windows 2012 R2 AMI System Image improvements.
- Redis System Images improvements.
- New Role Permission: *Provisioning: Allow Force Delete*

12.28.3 Fixes

- Fix for browser language settings adding commas in *Plans & Pricing -> Pricing*.
- Fix for Hyper-V and Openstack technology types in Library -> Node Type -> Image dropdown.
- Fix for File Upload in Virtual Images and Archives when using NFSv3 Storage Provider target.
- Fixes for synced Image Record duplication.
- Fix for extra Sub-Tenant Groups automatically being created during Sub-Tenant creation.
- Fix for Nutanix - Windows- Create Additional user.
- Fix for respecting Xen Custom Cores value.
- Fix for CentOS 6 agent install when using multiple LVM based volumes.
- Fix for *Infrastructure -> Network -> Services -> Add Service -> Consul* modal.
- Fix for Morpheus Wordpress Images: Load Balancer - no port available.
- Fix for Dual name fields in *Networks -> Services -> add Microsoft DNS*

12.29 v2.12.0

12.29.1 2.12.0 Release Notes

Contains everything from 2.11.4 release, plus:

- Azure Custom Image Support: Morpheus users can now upload private images into Morpheus, and then provision those onto an Azure cloud.
- User Provisioning Notifications: Provisioning e-mail notifications are configurable in user settings.
- Fix for removing Clouds from Groups
• Fix for Puppet agent install for Tasks and Group/Cloud integrations
• Fix for Nutanix backup and restore when using custom library items
• Additional Openstack ssl support

12.30 v2.11.4

12.30.1 New Features

Network IP Override  Networks can now be configured to allow overriding IP configuration and selecting between DHCP, Static IP entry, or IP Pools at provision time.

Windows License Management  Windows license can now be assigned to virtual images a applied during provision- ing. License can be managed in the new Licenses section under Admin - Provisioning.

Salt Windows Support  Salt Minions can now be installed on Windows Operating Systems via the Automation Engine. The source repo can also be customized and the minions can be successfully registered to both syndic master layouts as well as standard master layouts

Xen Reconfigure  Memory, Cores, Disk Size, Disks, and Networks can now be reconfigure on Xen instances and Hosts.

Debian 8 OS Support  Support for Debian 8 and 9 added to Agent. Debian 8.8 vmdk added to Morpheus Catalog.

Cloud Sync Update  90%+ reduction in VMware cloud sync time. Last Sync date and Sync Duration added to cloud detail pages.

Agent time normalization  Logging and stats data is now converted to appliance time in the cases VM time is offset.

Added support for querying ESXi hosts for Virtual Switch UUID:: vCenter user used for VMware cloud integra- tion no longer requires propagating datacenter permissions for provisioning.

Hostname routing added for Amazon ALB’s  Allows multiple hosts to share the same port

Shutdown renewals  Shutdown policy extension lease timeframe now begins at the time of extension approval for instances already shut down by the policy, rather than from the end of the previous lease.

12.30.2 Additional updates:

• Source column added to Virtual Images list page
• Tenants columns added to Networks list view
• Cloud Status column added to Cloud list view
• Improvements to host cpu, power and memory statistics.
• SEK currency support added
• Asynchronous cloud delete added

12.30.3 Fixes

• Fix for agent install and stop/start in inventoried AWS instances that are converted to Managed.
• Fix for Openstack disabled forced SSL validation
• Fix for Nutanix image sync issue with region codes
• Scaling improvements
• Windows agent install improvements
• Fix for editing Appliance Backup settings
• Fix for Role Permissions: Apps = User
• Fix for Max Storage policy enforcement
• Fix for uploaded OVA’s Virtual Image type
• Linux ssh console aspect ratio change in 2.11.3 reverted
• Network Groups improvements
• Security Improvements

12.31 v2.11.3 & 2.10.8

Important: ACCOUNTS has been renamed to TENANTS in v2.11.3

12.31.1 New Features

Task phase execution  Set phase and execution order for tasks in Workflows. Workflow detail pages added. Drag n’ drop reordering added to scripts in node types. Restart task type added.

Load Balancer improvements  New Balance mode, sticky mode, shared VIP address options, Load Balancer Detail Pages

ServiceNow Plugin  Add Morpheus clouds and Instance types for complete provisioning within Service now

Archives Service  Archives provides a way to store your files and make them available for download by your Scripts and Users.

Network Groups  Network Groups provide round robin network pooling capabilities when provisioning instances. These are most useful when scaling multiple vms across various subnets or availability zones.

Groups Access added to Networks  Networks can now be assigned to individual Groups and set as the default choice for a group.

Featured Instance Types  Instance types in the Library can now be flagged as Featured to be added to the new Featured Instance Types filter in the Provisioning wizard. Please note once at least one Instance Type is featured, the provisioning wizard will default to the Featured filter. Simply click the All Instance Types filter to see your entire catalog.

Group Lifecycle Policies  Now apply to instances that are converted from unmanaged to managed

New Reports section  Completely rebuilt reports section. Customizable capacity and usage reports with versioning.

Cost Tracking  Instance and host cost reporting available via UI and API. Prices added to instance and host detail pages.

Refreshed Instances Section  Instance list makeover with new charts, cloud, group and health info added.

Instance Locking  Instances can now be locked to prevent deletion.

Move Instances  Instances can now be moved between groups by editing the instance and selecting the group drop-down to assign the instance to a new group.
"User” Provisioning permission added to Roles  Allows permitting a user to only see their own instances.

“Remote Console Auto-Login” permission added to Roles  Please note NLA must be disabled in Windows RPD settings if auto-login is set to “no”. This permission does not apply when using VMware hypervisor console option.

New storage Provider types  NFSv3 and CIFS (Windows Samba File Sharing) added

Expanded variable support  Custom variables can now be used in Naming policies, including variables from options types.

Process output added to instance history  See process output per action in new Instance History detail modal.

Instance notes section  Add custom notes to instances, with markdown support.

Expanded Inventorying  Inventory Existing Instance option added to Softlayer and VMware fusion cloud types

Salt, Ansible and Chef improvements  Includes Ansible and Salt integration detail pages.

Integration detail page  Detail pages added for all integration with added functionality per integration.

Timezone option added to cloud settings  Users can now specify which timezone to set during guest customization.

Force guest customization added  Flag added for vmdk Virtual Images configuration (Advanced Settings- Force Guest Customization)

Enable Settings Flag on library items configuration  This setting exposes the Settings tab for appropriate instance types in the Instance Detail page.

• Deployment option added to Provisioning wizard
• IBMid support added to Softlayer*
• Windows 2012 AMI option added to default Windows Instance Type*
• Starting, stopping phases added to Instance status
• Manage Network Interfaces from Instance and Host detail pages
• Advanced Options- Status selection for Instances
• White Label mobile formatting improvements
• Source Image info and link added to Instance and Host detail pages
• Restart task type added (restarts target)
• API Allowed Origins support added
• Accounts renamed to tenants
• Multi-select added for tenant network assignment*
• Inventory Level setting added for Azure clouds with Basic and Full (API Heavy)
• Xen NFS, Multi-network support added
• KVM Multi-Network support added, Multi-network driver
• ESXi Multi-Network support added

12.31.2 2.11.3 and 2.10.8 Fixes

• Fixed issue with deleted Tenants stuck in removing due to Openstack cloud security groups not flushing
• Fixed Nutanix- Virtual Image duplication and cleanup
• Fixed Nutanix images not available in Node Type image dropdown
• Fixed Hostname field in Apps and Templates not applying to Windows instances.
• Fixed fields Apps Wizard Layout section not saving when custom Service Plan was selected.
• Fix for Chef bootstrap on Windows instances in Azure
• Instance list layout fixes.
• Xen Image sync fix
• Fix for instance list for sub-accounts
• Fix for Bluecat network query
• Dashboard- Recent Activity now only shows activity from Groups the user has access to
• User permission fixes
• Stopping an Azure instance now deallocates it in Azure
• Fix for Group user permission when Clouds permission is set to “none”
• Digital Ocean Naming Fixes
• Fix for duplicate price entries on public cloud price sync