## Contents

### 1 Getting Started
1.1 Requirements ......................................................... 1
1.2 Installation .......................................................... 5
1.3 Initial Appliance Setup .............................................. 10
1.4 Upgrading ............................................................ 12
1.5 Advanced Configuration ............................................ 13
1.6 High Availability Configuration ................................. 17
1.7 Morpheus CLI ......................................................... 38
1.8 Morpheus Agent ....................................................... 43

### 2 Provisioning
2.1 Provisioning Concepts .............................................. 45
2.2 Instances ............................................................. 47
2.3 Remote Console .................................................... 50
2.4 Apps ................................................................. 54
2.5 Blueprints ........................................................... 61
2.6 Automation .......................................................... 66
2.7 Virtual Images ....................................................... 69
2.8 Library ............................................................... 73
2.9 Migrations ............................................................ 83
2.10 Deployments ......................................................... 87

### 3 Infrastructure
3.1 Groups ............................................................... 91
3.2 Clouds ............................................................... 94
3.3 Hosts ................................................................. 97
3.4 Network ............................................................. 102
3.5 Load Balancers ...................................................... 110
3.6 Storage .............................................................. 113
3.7 Key Pairs & Certificates ........................................... 116
3.8 PXE Boot ............................................................ 116
3.9 Policies ............................................................... 120

### 4 Administration
4.1 Tenants & Tenant Users ............................................. 127
4.2 Identity Sources ..................................................... 142
4.3 Plans & Pricing ..................................................... 144
# 4.4 Roles .................................................. 148
# 4.5 Users & User Groups .................................. 153
# 4.6 Integrations ............................................ 157
# 4.7 Provisioning Settings ................................. 157
# 4.8 Monitoring Settings .................................. 160
# 4.9 Backup Settings ...................................... 161
# 4.10 Logging Settings ..................................... 163
# 4.11 Appliance Settings .................................. 163

## 5 Monitoring ............................................. 171
### 5.1 Overview ............................................ 171

## 6 Logs .................................................... 177
### 6.1 Overview ............................................ 177
### 6.2 Integrations ......................................... 178
### 6.3 Exporting Logs ...................................... 178
### 6.4 Agent Logs .......................................... 179
### 6.5 Morpheus Server Logs ............................... 179
### 6.6 Activity Log ......................................... 180

## 7 Backups ............................................... 181

## 8 Operations ............................................ 183
### 8.1 Dashboard ........................................... 183
### 8.2 Reports ............................................. 183
### 8.3 Analytics ........................................... 185
### 8.4 Guidance ........................................... 188
### 8.5 Scheduling .......................................... 189
### 8.6 Approvals ........................................... 192
### 8.7 Usage ................................................ 195
### 8.8 Activity ............................................. 196

## 9 Services ............................................... 197
### 9.1 Cypher .............................................. 197
### 9.2 Archives ............................................ 199

## 10 Integration Guides ................................. 201
### 10.1 Automation ......................................... 201
### 10.2 Backups ........................................... 216
### 10.3 Clouds ............................................. 218
### 10.4 Containers ......................................... 303
### 10.5 Deployment ......................................... 305
### 10.6 DNS ................................................ 305
### 10.7 Identity Management ............................... 306
### 10.8 ITSM ............................................... 316
### 10.9 Load Balancers ..................................... 319
### 10.10 Logs ................................................ 320
### 10.11 Monitoring ........................................ 321
### 10.12 Networking ....................................... 322
### 10.13 Service Discovery ................................. 329
### 10.14 Storage ............................................ 330

## 11 Troubleshooting ....................................... 331
### 11.1 Common Ports & Requirements .................... 331
### 11.2 Morpheus Agent Install Troubleshooting .......... 333
11.3 Remote Console .................................................. 337
11.4 Cannot Login .................................................. 342
11.5 Morpheus UI not loading after upgrade or reconfigure .... 343
11.6 Unable to Provision a Custom Image .......................... 344
11.7 Restart a Morpheus Installation ............................... 344
11.8 Variables ....................................................... 345
11.9 Blank Dashboard ................................................. 351
11.10 Unable to Delete Tenant ...................................... 351

12 Release Notes ..................................................... 353
  12.1 v3.5.0 ....................................................... 353
  12.2 v3.4.1 ....................................................... 357
  12.3 v3.4.0 ....................................................... 358
  12.4 v3.3.2 ....................................................... 360
  12.5 v3.3.1 ....................................................... 366
  12.6 v3.3.0 ....................................................... 370
  12.7 v3.2.2 ....................................................... 373
  12.8 v3.2.1 ....................................................... 377
  12.9 v3.2.0 ....................................................... 381
  12.10 v3.1.5 ...................................................... 385
  12.11 v3.1.4 ...................................................... 385
  12.12 v3.1.3 ...................................................... 386
  12.13 v3.1.2 & v2.12.5 .......................................... 387
  12.14 v3.1.1 ...................................................... 388
  12.15 v3.1.0 ...................................................... 389
  12.16 v3.0.1 ...................................................... 390
  12.17 v2.12.4 ...................................................... 391
  12.18 v2.12.3 ...................................................... 392
  12.19 v2.12.2 ...................................................... 392
  12.20 v2.12.1 ...................................................... 393
  12.21 v2.12.0 ...................................................... 395
  12.22 v2.11.4 ...................................................... 395
  12.23 v2.11.3 & 2.10.8 .......................................... 397
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**: 8 GB minimum
- **Storage**: 100 GB storage minimum
- **Network connectivity from your users to the appliance over TCP 443 (HTTPS)**
- **Inbound connectivity access from provisioned vm’s and container hosts on ports 443 and 80 (needed for agent communication)**
- **Internet Connectivity from Appliance (To download from Morpheus’ public docker repositories and virtual image catalog)**
- **Superuser privileges via the sudo command for the user installing the Morpheus Appliance package.**
- **An Appliance URL that is accessible 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. Morpheus also utilizes SSH (Port 22) and Windows Remote Management (Port 5985) to initialize a server.**
- **An Appliance License is required for any operations involving provisioning.**
Note: Ubuntu 16.10 and Amazon Linux are not supported.

1.1.2 Storage

Morpheus needs storage space for a few items. One is for the built-in Elasticsearch store (used for log aggregation and stats collection metrics). Morpheus also keeps a workspace and local virtual image cache for doing virtual image conversion and blueprint upload. While the permanent store of these can be offloaded via a Storage Provider some space is still recommended for dealing with non streamable virtual image formats.

In many common scenarios it might be prudent to configure a shared datastore on a storage cluster and mounted to /var/opt/morpheus/morpheus-ui (this is where all user based data and database data is persisted). There are several folders located within here that can be independently located as desired.

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>
<th></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>
<td></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>
<td></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</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Virtual Images configured</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SSH Enabled on Virtual Image</td>
<td></td>
</tr>
<tr>
<td>WinRM</td>
<td>Windows</td>
<td>Windows</td>
<td>Node</td>
<td>Appliance</td>
<td>5985</td>
<td>DNS Resolution from node to appliance url</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Virtual Images configured</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>WinRM Enabled on Virtual Image(winrm quickconfig)</td>
<td></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</td>
<td></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 Admin -&gt; Provisioning</td>
<td></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>
<td></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</td>
<td></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 Admin -&gt; Provisioning</td>
<td></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>
<td></td>
</tr>
<tr>
<td>VMtools</td>
<td>All</td>
<td>All</td>
<td></td>
<td></td>
<td></td>
<td>VMTools installed on template</td>
<td></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 Administration -&gt; Provisioning when using Static IP’s</td>
<td></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>
<td></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>
<td></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>
<td></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>
<td></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 Administration -&gt; Provisioning</td>
<td></td>
</tr>
</tbody>
</table>

---

**Chapter 1. Getting Started**

Network configured in Morpheus (Gateway, Primary and Secondary DNS, CIDR populated, DHCP disabled)
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 (Ubuntu is recommended).

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`

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

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

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:

   ```
   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. Installation 5
1.2.2 CentOS

To get started installing Morpheus on CentOS/RHEL 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.
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`
   - 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.

4. 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`

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

   `sudo rpm -i morpheus-appliance-x.x.x-1.x86_64.rpm`
   `sudo morpheus-ctl reconfigure`

6. 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`. 
1.2.3 RHEL

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

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.e17 python-rhsm: 1.10.12-2.e17
```

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.e17 python-rhsm: 1.10.12-2.e17
```

If the subscription manager returns 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
```

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.gomorpheus.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
```

(continues on next page)
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 your username 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 page without specifying their subdomain.

1.3.3 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.

### 1.5 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 an 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:
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.

**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.

---

### 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 appliance url (if needed, hostname will be automatically set). Edit appliance_url to resolvable url (if not configured correctly by default)

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

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 a proxy, when adding or editing a cloud there is a setting called “API Proxy” under “Advanced Options”. This is where the proxy of choice can be selected to instruct the Provisioning engine how to communicate with the public cloud. Simply adjust this setting and the cloud should start being able to receive/issue instructions.

#### Provisioning with Proxies

Proxy configurations can vary from operating system to operating system and in some cases it is necessary for these to be configured in the blueprints as a prerequisite. In other cases it can also be configured automatically. Mostly with the use of cloud-init (which all of our out of the box service catalog utilizes on all clouds). When editing/creating a cloud there is a setting for “Provisioning Proxy” in “Provisioning Options”. If this proxy is set, Morpheus will automatically apply these proxy settings to the guest operating system.
Overriding proxy settings can also be done on the Network record. Networks (or subnets) can be configured in Infrastructure -> Networks or on the Networks tab of the relevant Cloud detail page. Here, a proxy can also be assigned as well as additional options like the No Proxy rules for proxy exceptions.

**Docker**

When provisioning Docker based hosts within a Proxy environment it is up to the user to configure the docker 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:

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

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

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

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

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

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

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

```
[root@app-server-new ~] /opt/morpheus/embedded/mysql/bin/mysql -u morpheus -h 10.1.2.2 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:
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 scenarios rabbitmq can manage. If doing a cross-region HA rabbitmq cluster it is recommended to have at least 3 rabbit queue clusters per region. Typically to handle HA a RabbitMQ cluster should be placed between a load balancer and the front-end application server to handle cross host connections. The ports necessary to forward in a Rabbit MQ cluster are (5672, and 61613). A rabbitmq cluster can run on smaller memory machines depending on how frequent large requests bursts occur. 4–8gb 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

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

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

**Requirements**

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

- 3306
- 4444
- 4567
- 4568
Percona also recommends setting the selinux policy to permissive. You can temporarily set the permission to permissive by running

```
sudo setenforce 0
```

You will need to edit the selinux configuration file if you want the permission to take affect permanently which can be found in `/etc/selinux/config`

### Add Percona Repo

1. Add the percona repo to your Linux Distro.

```
  →percona-release-0.1-4.noarch.rpm
```

2. Check the repo by running the below command.

```
sudo yum list | grep percona
```

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

```
sudo yum clean all
sudo yum update -y
```

### Installing Percona XtraDB Cluster

1. The below command will install the Percona XtraDB Cluster software and it’s dependences.

```
sudo yum install Percona-XtraDB-Cluster-57
```

**Note:** During the installation you will receive the below message. Accept the Percona PGP key to install the software.

```
retrieving key from file:///etc/pki/rpm-gpg/RPM-GPG-KEY-Percona
Importing GPG key 0xCD2EFD2A:
Userid : "Percona MySQL Development Team <mysql-dev@percona.com>"
Fingerprint: 430b df5c 56e7 c94e 848e e60c 1c4c bdcd cd2e fd2a
Package : percona-release-0.1-4.noarch (installed)
From : /etc/pki/rpm-gpg/RPM-GPG-KEY-Percona
Is this ok [y/N]: y
```

2. Next we need enable the mysql service so that the service started at boot.

```
sudo systemctl enable mysql
```

3. Next we need to start mysql

```
sudo systemctl start mysql
```

4. Next we will log into the mysql server and set a new password. To get the temporary root mysql password you will need to run the below command. The command will print the password to the screen. Copy the password.
sudo grep 'temporary password' /var/log/mysqld.log

5. Login to mysql

```bash
mysql -u root -p
password: 'enter password copied above'
```

6. Change the root user password to the mysql db

```sql
ALTER USER 'root'@'localhost' IDENTIFIED BY 'MySuperSecurePasswordhere';
```

7. Create the sstuser user and grant the permissions.

```sql
mysql> CREATE USER 'sstuser'@'localhost' IDENTIFIED BY 'M0rpheus17';
```

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

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

8. Exit mysql then stop the mysql services:

```bash
mysql> exit
Bye
$ sudo systemctl stop mysql.service
```

9. Now install the Percona software on to the other nodes using the same steps.

Once the service is stopped on all nodes move onto the next step.

### Add [mysqld] to my.cnf in /etc/

1. Copy the below contents to /etc/my.cnf. The node_name and node_address needs to be unique on each of the nodes. The first node does not require the gcomm value to be set.

```ini
$ sudo vi /etc/my.cnf

[mysqld]
wsrep_provider=/usr/lib64/galera3/libgalera_smm.so
wsrep_cluster_name=popeye
wsrep_cluster_address=gcomm:// #Leave blank for Master Node. The other nodes require this field. Enter the IP address of the primary node first then remaining nodes. Separating the ip addresses with commas like this 10.30.20.196,10.30.20.197,10.30.20.198#
wssrep_node_name=morpheus-node01
wsrep_node_address=10.30.20.57
wsrep_sst_method=xtrabackup-v2
wsrep_sst_auth=sstuser:M0rpheus17
pxc_strict_mode=PERMISSIVE
```

(continues on next page)
2. Save `/etc/my.cnf`

### Bootstrapping the first Node in the cluster

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

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

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

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

2. To verify the bootstrap, on the master node login to `mysql` and run `show status like 'wsrep%';`

   ```sql
   # mysql -u root -p
   mysql> show status like 'wsrep%';
   
   +----------------------------------|--------------------------------------+
   | Variable_name | Value                                      |
   +----------------------------------|--------------------------------------+
   | wsrep_local_state_uuid | 591179cb-a98e-11e7-b9aa-07df8a228fe9 |
   | wsrep_protocol_version | 7                                      |
   | wsrep_last_committed | 1                                      |
   | wsrep_replicated | 0                                      |
   | wsrep_replicated_bytes | 0                                      |
   | wsrep_repl_keys | 0                                      |
   | wsrep_repl_keys_bytes | 0                                      |
   | wsrep_repl_data_bytes | 0                                      |
   | wsrep_repl_other_bytes | 0                                      |
   | wsrep_received | 2                                      |
   | wsrep_received_bytes | 141                                     |
   | wsrep_local_commits | 0                                      |
   | wsrep_local_cert_failures | 0                                     |
   | wsrep_local_replays | 0                                      |
   | wsrep_local_send_queue | 0                                     |
   | wsrep_local_send_queue_max | 1                                     |
   | wsrep_local_send_queue_min | 0                                     |
   | wsrep_local_send_queue_avg | 0.000000                               |
   | wsrep_local_recv_queue | 0                                     |
   | wsrep_local_recv_queue_max | 2                                     |
   | wsrep_local_recv_queue_min | 0                                     |
   | wsrep_local_recv_queue_avg | 0.500000                               |
   | wsrep_local_cached_downto | 0                                      |
   | wsrep_flow_control_paused_ns | 0                                     |
   | wsrep_flow_control_paused | 0.000000                               |
   | wsrep_flow_control_sent | 0                                      |
   | wsrep_flow_control_recv | 0                                      |
   ```

(continues on next page)
| wsrep_flow_control_interval | [ 100, 100 ] |
| wsrep_flow_control_interval_low | 100 |
| wsrep_flow_control_interval_high | 100 |
| wsrep_flow_control_status | OFF |
| wsrep_cert_deps_distance | 0.000000 |
| wsrep_apply_oooe | 0.000000 |
| wsrep_apply_oool | 0.000000 |
| wsrep_apply_window | 0.000000 |
| wsrep_commit_oooe | 0.000000 |
| wsrep_commit_oool | 0.000000 |
| wsrep_commit_window | 0.000000 |
| wsrep_local_state | 4 |
| wsrep_local_state_comment | Synced |
| wsrep_cert_index_size | 0 |
| wsrep_cert_bucket_count | 22 |
| wsrep_gcache_pool_size | 1320 |
| wsrep_causal_reads | 0 |
| wsrep_cert_interval | 0.000000 |
| wsrep_ist_receive_status | |
| wsrep_ist_receive_seqno_start | 0 |
| wsrep_ist_receive_seqno_current | 0 |
| wsrep_ist_receive_seqno_end | 0 |
| wsrep_incoming_addresses | 10.30.20.196:3306 |
| wsrep_desync_count | 0 |
| wsrep_evs_delayed | |
| wsrep_evs_evict_list | |
| wsrep_evs_repl_latency | 0/0/0/0/0 |
| wsrep_evs_state | OPERATIONAL |
| wsrep_gcomm_uuid | 07c8c8fe-a998-11e7-883e-06949cfe5af3 |
| wsrep_cluster_conf_id | 1 |
| wsrep_cluster_size | 1 |
| wsrep_cluster_state_uuid | 591179cb-a98e-11e7-b9aa-07df8a228fe9 |
| wsrep_cluster_status | Primary |
| wsrep_connected | ON |
| wsrep_local_bf_aborts | 0 |
| wsrep_local_index | 0 |
| wsrep_provider_name | Galera |
| wsrep_provider_vendor | Codership Oy <info@codership.com> |
| wsrep_provider_version | 3.22 (r8678538) |
| wsrep_ready | ON |

A table will appear with the status and rows.

3. Next Create the Database you will be using with morpheus.

```sql
mysql> CREATE DATABASE morpheusdb;

mysql> show databases;
```

4. 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 'morpheusadmin'@'%' IDENTIFIED BY 'Cloudy2017';
```

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

### 1.6. High Availability Configuration
6. Checking Permissions for your user.

```sql
SHOW GRANTS FOR 'morpheusadmin'@'%;
```

**Bootstrap the Remaining Nodes**

1. To bootstrap the remaining nodes into the cluster run the following command on each node:

```shell
sudo systemctl start mysql.service
```

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

*Note:* Bootstrap failures are commonly caused by misconfigured `/etc/my.cnf` files.

**Verification**

1. To verify the cluster, on the master login to mysql and run `show status like 'wsrep%';`

```sql
$ mysql -u root -p
mysql> show status like 'wsrep%';
```

```
+-------------------------------+-----------------------------+
<table>
<thead>
<tr>
<th>Variable_name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>wsrep_local_state_uuid</td>
<td>591179cb-a98e-11e7-b9aa-07df8a228fe9</td>
</tr>
<tr>
<td>wsrep_protocol_version</td>
<td>7</td>
</tr>
<tr>
<td>wsrep_last_committed</td>
<td>4</td>
</tr>
<tr>
<td>wsrep_replicated</td>
<td>3</td>
</tr>
<tr>
<td>wsrep_replicated_bytes</td>
<td>711</td>
</tr>
<tr>
<td>wsrep_rep1_keys</td>
<td>3</td>
</tr>
<tr>
<td>wsrep_rep1_keys_bytes</td>
<td>93</td>
</tr>
<tr>
<td>wsrep_rep1_data_bytes</td>
<td>426</td>
</tr>
<tr>
<td>wsrep_rep1_other_bytes</td>
<td>0</td>
</tr>
<tr>
<td>wsrep_received</td>
<td>10</td>
</tr>
</tbody>
</table>

(continues on next page)
### 1.6. High Availability Configuration

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>wsrep_received_bytes</td>
<td>774</td>
<td>wsrep_local_commits</td>
<td>0</td>
</tr>
<tr>
<td>wsrep_local_cert_failures</td>
<td>0</td>
<td>wsrep_local_replays</td>
<td>0</td>
</tr>
<tr>
<td>wsrep_local_send_queue</td>
<td>0</td>
<td>wsrep_local_send_queue_max</td>
<td>1</td>
</tr>
<tr>
<td>wsrep_local_send_queue_min</td>
<td>0</td>
<td>wsrep_local_send_queue_avg</td>
<td>0.000000</td>
</tr>
<tr>
<td>wsrep_local_recv_queue</td>
<td>0</td>
<td>wsrep_local_recv_queue_max</td>
<td>2</td>
</tr>
<tr>
<td>wsrep_local_recv_queue_min</td>
<td>0</td>
<td>wsrep_local_recv_queue_avg</td>
<td>0.100000</td>
</tr>
<tr>
<td>wsrep_local_cached_downto</td>
<td>2</td>
<td>wsrep_flow_control_paused_ns</td>
<td>0</td>
</tr>
<tr>
<td>wsrep_flow_control_paused</td>
<td>0.000000</td>
<td>wsrep_flow_control_sent</td>
<td>0</td>
</tr>
<tr>
<td>wsrep_flow_control_recv</td>
<td>0</td>
<td>wsrep_flow_control_interval</td>
<td>[173, 173]</td>
</tr>
<tr>
<td>wsrep_local_state_comment</td>
<td>Synced</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wsrep_cert_index_size</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wsrep_cert_bucket_count</td>
<td>22</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wsrep_gcache_pool_size</td>
<td>2413</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wsrep_causal_reads</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wsrep_cert_interval</td>
<td>0.000000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wsrep_ist_receive_status</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wsrep_ist_receive_seqno_start</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wsrep_ist_receive_seqno_current</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wsrep_ist_receive_seqno_end</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wsrep_incoming_addresses</td>
<td>10.30.20.196:3306, 10.30.20.197:3306, 10.30.20.198:3306</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wsrep_desync_count</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wsrep_evs_delayed</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wsrep_evs_evict_list</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wsrep_evs_repl_latency</td>
<td>0/0/0/0/0/0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wsrep_evs_state</td>
<td>OPERATIONAL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wsrep_gcomm_uuid</td>
<td>07c8c8fe-a998-11e7-883e-06949cfe5af3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wsrep_cluster_conf_id</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wsrep_cluster_size</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wsrep_cluster_state_uuid</td>
<td>591179cb-a98e-11e7-b9aa-07df8a228fe9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wsrep_cluster_status</td>
<td>Primary</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wsrep_connected</td>
<td>ON</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wsrep_local_bf_aborts</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wsrep_local_index</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wsrep_provider_name</td>
<td>Galera</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wsrep_provider_vendor</td>
<td>Codership Oy <a href="mailto:info@codership.com">info@codership.com</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wsrep_provider_version</td>
<td>3.22(r8678538)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wsrep_ready</td>
<td>ON</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
2. Verify that you can login to the MSQL server by running the below command on the Morpheus Application server(s).

```
mysql -u morpheusadmin -p -h 192.168.10.100
```

**Note:** This command requires mysql client installed. If you are on a windows machine you can connect to the server using mysql work bench which can be found here [https://www.mysql.com/products/workbench/](https://www.mysql.com/products/workbench/)

### 1.6.3 RabbitMQ Cluster

**RabbitMQ Installation and Configuration**

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

**Prerequisites**

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

**Install RabbitMQ on the 3 nodes**

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

**On Node 1:**

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

Copy this value

**On Nodes 2 & 3:**

1. Overwrite `/var/lib/rabbitmq/.erlang.cookie` with value from previous step and change its permissions using the follow commands.
chown rabbitmq:rabbitmq /var/lib/rabbitmq/*
chmod 400 /var/lib/rabbitmq/.erlang.cookie

2. edit /etc/hosts file to refer to shortname of node 1
   example:
   10.30.20.100 rabbit-1

3. Run the commands to join each node to the cluster
   rabbitmqctl stop
   rabbitmq-server -detached
   rabbitmqctl stop_app
   rabbitmqctl join_cluster rabbit@<<node 1 shortname>>
   rabbitmqctl start_app

On Node 1:
   rabbitmqctl add_user <<admin username>> <<password>>
   rabbitmqctl set_permissions -p / <<admin username>> ".*" ".*" ".*"
   rabbitmqctl set_user_tags <<admin username>> administrator

On All Nodes:
   rabbitmq-plugins enable rabbitmq_stomp

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:
Installation

1. Download and Install Elasticsearch

Elasticsearch can be downloaded directly from elastic.co in zip, tar.gz, deb, or rpm packages. For CentOS, it’s best to use the native rpm package which will install everything you need to run Elasticsearch. Download it in a directory of your choosing with the command:

```
wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-5.6.10.rpm
```

Then install it in the usual CentOS way with the rpm command like this:

```
sudo rpm -ivh elasticsearch-5.6.10.noarch.rpm
```

This results in Elasticsearch being installed in `/usr/share/elasticsearch/` with its configuration files placed in `/etc/elasticsearch` and its init script added in `/etc/init.d/elasticsearch`.

To make sure Elasticsearch starts and stops automatically, add its init script to the default runlevels with the command:

```
sudo systemctl enable elasticsearch.service
```

Note: If you manage an ElasticSearch cluster externally from Morpheus, follow the steps located on the ElasticSearch website to upgrade to the latest version compatible with Morpheus

1. 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.

Node 1

```
cluster.name: morpheusha1
node.name: "morpheuses1"
discovery.zen.ping.unicast.hosts: ["10.30.20.91","10.30.20.149","10.30.20.165"]
```

Node 2

1.6. High Availability Configuration
cluster.name: morpheusha1
node.name: "morpheuses2"
discovery.zen.ping.unicast.hosts: ["10.30.20.91","10.30.20.149","10.30.20.165"]

Node 3

cluster.name: morpheusha1
node.name: "morpheuses3"
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

2. Testing

By now, Elasticsearch should be running on port 9200. You can test it with curl, the command line client-side URL transfers tool and a simple GET request like this:

```
[..]$ sudo curl -X GET 'http://10.30.20.149:9200'
{
   "status" : 200,
   "name" : "morpheuses1",
   "cluster_name" : "morpheusha1",
   "version" : {
      "number" : "1.7.3",
      "build_hash" : "05d4530871ef0ea4660f6a89e64db9ce8659682",
      "build_timestamp" : "2015-10-15T09:14:17Z",
      "build_snapshot" : false,
      "lucene_version" : "4.10.4"
    },
},
```

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:

```
sudo rpm -i morpheus-appliance-x.x.x-1.x86_64.rpm
```

1. 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.
1. Reconfigure Morpheus

```
sudo morpheus-ctl reconfigure
```

1.6.6 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 `/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://downloads.gomorpheus.com/example/path/
morpheus-appliance-offline-3.1.5-1.noarch.rpm
[root@app-server-1 ~]# wget https://downloads.gomorpheus.com/example/path/
morpheus-appliance-3.1.5-1.el7.x86_64.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.

```bash
[root@app-server-1 ~] rpm -i morpheus-appliance-3.1.5-1.el7.x86_64.rpm
[root@app-server-1 ~] rpm -i morpheus-appliance-offline-3.1.5-1.noarch.rpm
```

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

**Node 1**

```ruby
appliance_url 'https://morpheus1.localdomain'
elasticsearch['es_hosts'] = {'10.100.10.121' => 9200, '10.100.10.122' => 9200,
                           '10.100.10.123' => 9200}
elasticsearch['node_name'] = '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**

```ruby
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**

```ruby
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 ex-
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

```bash
[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.

```bash
[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

```bash
[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.

```bash
[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.

```bash
[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 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
```
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 10.130.3.38 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
```

(continues on next page)
run: elasticsearch: (pid 19207) 5326s;
run: log: (pid 565) 8401s
run: guacd: (pid 601) 8401s;
run: log: (pid 573) 8401s
run: morpheus-ui: (pid 17976) 7633s;
run: log: (pid 555) 8401s
run: nginx: (pid 581) 8401s;
run: log: (pid 544) 8401s
run: rabbitmq: (pid 17850) 7708s;
run: log: (pid 542) 8401s
run: redis: (pid 572) 8401s;
run: log: (pid 548) 8401s

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

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

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

```
[root@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 Elastic-
search.

```
[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 7 32 0.22 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:

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

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

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

The challenge with RabbitMQ is that it is load balanced behind Morpheus for requests, but each Morpheus application server needs to bootstrap the RabbitMQ tied into it. Thus, if it cannot reach its own RabbitMQ startup for it will fail.

Similarly, if a Morpheus UI service cannot reach the database, startup will fail. However, if the database is externalized and failover is configured for Master/Master, then there should be ample opportunity for Morpheus to connect to the database tier.

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

```
[root@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`.

---

1.6. High Availability Configuration
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 2.0.0+ installed (2.3.0 recommended). Once the ruby runtime is installed simply use rubygems to install the CLI

```
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 http://rubyinstaller.org/downloads and download at least Ruby version 2.0.0 (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

```
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.

```
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.

```
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

```
morpheus remote
```

### Getting Started

To get started with the morpheus CLI it’s 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 let’s check our authentication information:

```
morpheus> whoami
Current User
==================
ID: 1
Account: Labs (Master Account)
First Name: Demo
Last Name: Environment
Username: david
Email: david@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. Let’s 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
```

(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, let’s 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:
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]
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`.

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
```

1.8 Morpheus Agent

The Morpheus Agent is an important and powerful facet of Morpheus as an 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
CHAPTER 2

Provisioning

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 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.

2.1.1 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.

2.1.2 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).

2.1.3 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 inject “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.

2.1.4 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.

2.1.5 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.
2.2 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.

### 2.2.1 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.)

### 2.2.2 Instance Details

The instance detail page is where you can view and fully manage an instance. To get to an instance detail page, navigate to provisioning, instances, and click on an instance. Please note instance details and actions differ between instance types and user permissions.

There are several sections within an Instance page that provide useful capabilities to the user.

- **Summary** Stats and status information
- **Deploy** Track deployment history for instance types that support deployments or manually kick off a deployment (only visible for instance types that support deployments)
- **Settings** Some instance types support custom configuration settings (i.e. mysql presents the my.ini)
- **Network** Useful for configuring security groups and access to the instance.
- **Monitoring** Quick summary of the monitoring system and all checks that were configured to test the state of the instance
- **Backups** Quick backup dashboard. Useful for viewing historical backups as well as kicking off new ones.
- **Logs** View all aggregated logs from the containers or VM’s representing the instance.
- **Environment** View the environment variables presented to the instances or exported by the instances via Apps (more on this in the Apps section). Even see Imported environment variables that may be referenced by the running instance.
- **Scale** For instances that support load balancing and auto scaling. Easily configure auto scaling thresholds and load balancer settings that pertain to a particular instance.
- **Console** Access the instance or container via a client-less Console supporting SSH, RDP, VNC, and even hypervisor level remote consoles.

### 2.2.3 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, or Group 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.

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 button.

Tip: Markdown Syntax is supported in Instance Notes.

2.3 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.

2.3.1 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.

2.3.2 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 (VMware Hypervisor Console)** The VNC protocol will be used for all platform types in VMware Clouds with the Hypervisor Console option enabled in cloud settings. A unique port is assigned per per Virtual Machine starting at 5900.

**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 VMware cloud settings, the VNC protocol will be used for all platform types that VMware Cloud.

When using VNC Hypervisor Console, the Morpheus Appliance connects directly to the ESXi host the VM is on, not directly to the VM. A VNC port is assigned per Virtual Machine starting at 5900 and a complex VNC password is generated. VNC is then enabled and the port and password are set on the VMs settings in vSphere.

Morpheus features Remote Console support directly to VMware ESXi hypervisors. To enable this feature a few prerequisites must be met:

- The gdbserver Firewall setting needs to be enabled on each ESXi host the console will connect to. This can be done in vSphere under firewall configuration on the ESXi hosts by checking the gdbserver option on each required host. This will open up the necessary ports VNC ports on the ESXi host(s), starting at port 5900.

**Note:** The most common cause of Remote Console connection issues when using hypervisor console is gdbserver not being enabled on the ESXi hosts firewall settings.

- The Morpheus Appliance must have network access to the ESXi hosts within vCenter, specifically to the host the VM is on when using Remote Console, over the VNC port range, typically 5900-6000. The connection does not go through the vCenter server(s).

- The Morpheus Appliance must be able to resolve the ESXi hostnames.

- VMware tools or equivalent must be installed on the VM.

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 VVM 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. The

**Important:** All VMs that are inventoried or provisioned into a VMware cloud with Hypervisor Console enabled will have their Console Type set to VNC. Disabling Hypervisor Console will only apply to newly inventoried or provisioned VM’s. VM’s inventoried or provisioned when Hypervisor Console was enabled will continue to use the VNC protocol even after Hypervisor Console is disabled. To revert a VM

### 2.3.3 Copy and Paste

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.

### 2.3.4 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 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 guacd processes: `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 successful.
```

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`

2.4 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.
2.4.1 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.
2.4.2 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.
2.4.3 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.
CHOOSE A CONFIGURATION FOR EACH INSTANCE

STRUCTURE

- Spud Marketing
  - Web
    - Tomcat
      - Group: All Clouds Demo, Cloud: Appliance KVM & Docker
      - Group: All Clouds Demo, Cloud: Labs UCS
  - Database
    - MySQL
      - Group: All Clouds Demo, Cloud: Appliance KVM & Docker
      - Group: All Clouds Demo, Cloud: Labs UCS

DOWNLOAD CONFIGURATION
2.5 Blueprints

2.5.1 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:

```
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 {"tier": {"bootOrder": 1}) object structure.

Configuration Scopes

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

```javascript
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 let’s look at a Blueprint that deploys a single nginx container to a target cloud:

```javascript
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.
2.5.2 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.

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.

---

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

---

**2.6.1 Tasks**

Available Task Types:

- Ansible Playbook
- Chef Bootstrap
- Groovy Script*
- HTTP
- Javascript*
- jRuby Script*
- Library Script: Adds an existing script from the Library section as a task
- Library Template: Adds an existing script from the Library section as a task
- Puppet Agent Install
- Python Script (jython)*
- Shell Script
- SSH Script
- WinRM Script
- Restart: Executes a restart on the Instance. Morpheus will wait until the restart is complete to execute the next task in the workflow phase.

**Note:**
- executes locally

**To Add Tasks:**

1. Select the Provisioning link in the navigation bar.
2. Select Automation from the sub-navigation menu.
3. Click the **Add** button.
4. From the New Task Wizard input a name for the task.
5. Select the type of task from from the type dropdown.
6. Input the appropriate details dependent on the task type you selected from the dropdown.
7. Save

**Edit 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 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.

2.6.2 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.

## 2.7 Virtual Images

_Provisioning -> Virtual Images_

### 2.7.1 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.

### 2.7.2 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.

### 2.7.3 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.

**Note:** Editing System Images is disabled.

**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.
   - **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 via Cloud-Init, Cloudbase-Init, or guest processes (VMware).
   - **Password** Password for the Existing User on the image.
   - **Cloud-Init User Data** Accepts what would go in runcmd and can assume bash syntax.
   - **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).
   - **VirtIO Drivers Loaded?** Enable if VirtIO Drivers are installed on the image for provisioning to KVM based Hypervisors.
   - **Force Guest Customization?** VMware only, forces sys-prep on image during provisioning.
   - **Trial Version** Enable to automatically re-arm the expiration on Windows Trial Images during provisioning.

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.

### 2.7.4 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.

2.7.5 Add Virtual Images

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).

To Add Virtual Image:

1. Select + Add in the Virtual Images page.
2. Select Image format:
   - 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.
   - 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 via Cloud-Init, Cloudbase-Init, or guest processes (VMware).
   - Password: Password for the Existing User on the image.
   - 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.

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).

VirtIO Drivers Loaded? Enable if VirtIO Drivers are installed on the image for provisioning to KVM based Hypervisors.

Force Guest Customization? VMware only, forces sys-prep on image during provisioning.

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

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.

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: Morpheus provides a file upload progress. The Virtual Image configuration can be saved while the upload is in progress, and the upload will finish in the background.
2.8 Library

2.8.1 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.
2.8.2 Instance Types

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.
2.8.3 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>

### 2.8.4 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.

### 2.8.5 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.

**Note:** Layouts cannot be added to Morpheus provided library items at this time.

- **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.

2.8.6 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).
2.8.7 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.
2.9 Migrations

2.9.1 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

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.

2.9.2 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.

2.9.3 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.

2.9.4 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.

2.9.5 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:

```json
{
"Version": "2012-10-17",
"Statement": [ 
  { 
    "Effect": "Allow",
    "Action": [ 
      "s3:GetObject",
      "s3:ListBucket"
    ],
    "Resource": "arn:aws:s3:::disk-image-file-bucket/*"
  }
]
}
```

(continues on next page)
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.

```
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.
2.10 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.

2.10.1 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.

2.10.2 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.

#### 2.10.3 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.

#### 2.10.4 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.

#### 2.10.5 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.

### 2.10.6 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.

### 2.10.7 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 are used to organize clouds, roles, and hosts.

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
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
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 search feature and provides the option to edit, delete, and add 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
- DigitalOcean
• Google Cloud
• HPE
• HPE OneView
• Hyper-V
• Kubernetes
• MacStadium
• Metacloud
• Morpheus (generic)
• Nutanix
• Open Telekom Cloud
• OpenStack
• Oracle Public Cloud
• Oracle VM
• Platform 9
• SCVMM
• SoftLayer
• Supermicro
• UCS
• UpCloud
• VMWare ESXi
• VMware Fusion
• VMware vCenter
• VMware vCloud Air
• VMware vCloud Director
• VirtualBox
• 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 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
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 form 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
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).

- 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.

3.4 Network

3.4.1 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.

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
  • 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

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.
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

**F5 LineRate**
• API Host
• API Port
• Username
• Password
• Internal IP
• Public IP
• VIP Address
• VIP Port

**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.

F5 Load Balancers

Overview

3.5.3 Add F5 Load Balancer

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 Idenetifying 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/
5. Save Changes

3.6 Storage

3.6.1 Overview

The default Storage path for Virtual Images, Backups, Deployment Archives, Archive Server, and Archived Snapshots is /var/opt/morpheus. Additional Storage providers can be added and mapped for these targets in the Infrastructure -> Storage section. Adding Storage providers are also required for scenarios like AWS migrations.

3.6.2 Supported Storage Provider Types

- Local
- NFSv3
- CIFS (Samba Windows File Sharing)
- Amazon S3
- Azure
• Rackspace CDN
• OpenStack Swift

3.6.3 To View Storage

1. Select the Infrastructure link in the navigation bar.
2. Select the Storage link in the sub navigation bar.

3.6.4 Add Storage Provider

To Add Storage Provider:

1. Select the Infrastructure link in the navigation bar.
2. Select the Storage link in the sub navigation bar.
3. Click the Add Storage Provider button.
4. From the New Storage Provider Wizard input the following:
   - **Name** Name of the storage provider.
   - **Provider Type**
     - Local Storage
       - Storage Path
     - NFSv3
       - Host
       - Export Folder
     - CIFS (Samba Windows File Sharing)
       - Host
       - Username
       - Password
       - Share Path
     - Amazon S3
       - Access Key
       - Secret Key
       - Bucket Name
       - Endpoint URL (Optional endpoint URL if pointing to an object store other than amazon that mimics the Amazon S3 APIs.)
     - Azure
       - Storage Account
       - Storage Key
       - Share Name
     - Rackspace CDN
To Edit Storage Provider:

1. Select the Infrastructure link in the navigation bar.
2. Select the Storage link in the sub navigation bar.
3. Click the Edit pencil icon on row of the Storage Provider to edit.
4. Edit required information.
5. Click the Save Changes button to save.

To Delete Storage Provider:

1. Select the Infrastructure link in the navigation bar.
2. Select the Storage link in the sub navigation bar.
3. Click the Delete icon on row of the Storage Provider to delete.
3.7 Key Pairs & Certificates

3.7.1 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.

3.7.2 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.

3.7.3 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.

3.8 PXE Boot

3.8.1 Overview

Morpheus includes a built in PXE Server to enable easy and rapid bare metal provisioning.
3.8.2 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;
```

**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**

**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`.

3.8.3 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.

3.8.4 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.

3.8.5 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 down 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.

3.9 Policies

3.9.1 Overview

Policies add governance, ease of use, cost-savings, and auditing features to Morpheus. Policies can be created in the Policies tabs in Groups and Clouds. Policy generation is a role permission.

Policies apply towards any instance provisioned into a group or cloud with active policies. Cloud policies will override matching or conflicting group policies during provisioning.

Available Policy Types

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 as ServiceNow.

**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.

**3.9.2 Creating Policies**

Policies can be created, edited, and set to active or inactive in the a group or cloud detail pane under the Policies tab.

**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 Type sections below for Configuration options.
6. Select SAVE CHANGES
3.9.3 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 emaila. The default message is

\[
\text{Instance } ${instance?.name} \text{ is set to expire on } ${instance?.expireDate}
\]

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}
- ${userId}
An example Instance Name Policy using a naming pattern with User Initials, Cloud Code, Instance Type, and a sequential number starting at 3000 is `${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.

TENANTS  Leave blank for the Policy to apply to all Tenants, or search for and select Tenants to enforce the Policy on specific Tenants.
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 & Tenant Users

4.1.1 Overview

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.

4.1.2 Tenants

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.

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.)*

. 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)

. 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
• Library Instance Types
• Pricing
• Policies
• Workflows
• Roles

Note: Virtual Image Blueprints can also be made available to multiple select Tenants when set to private.

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.

![Edit Cloud Modal](image-url)
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 an Tenant is assigned to that Tenant. If these resources are in the Master Tenant, they can be assigned to sub Tenants. Assigning one of these resources will make it unavailable to the Master Tenant, but it will still be visible and editable by the Master Tenant. This allows Master Tenant resources to be isolated for use by sub-Tenants while still under the control of the Master Tenant.

Resources assigned to sub-Tenants from the Master Tenant will be visible and available for use by that sub-Tenant, however they cannot be edited or re-assigned by the sub-tenant.

**Set the Visibility of a Host, Virtual Machine or Bare metal Server to Public or Private**

1. From the Master Tenant, navigate to Infrastructure, Hosts
2. Select either the Hosts, Virtual Machines or Bare Metal tab
3. Click the name of the resource
4. Select *Edit* in the 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 an Tenant

1. From the Master Tenant, navigate to Infrastructure, Hosts
2. Select either the Hosts, Virtual Machines or Bare Metal tab
3. Click the name of the resource
4. From the “Actions” dropdown in the 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
Assign a 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
Set the Visibility or assign a datastore to a 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
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
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.

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

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.

<table>
<thead>
<tr>
<th>Feature Access</th>
<th>Controls Tenant and User access level for sections and features in Morpheus.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Access</td>
<td>Controls User access level for Groups. (Groups are not Multi-Tenant.)</td>
</tr>
<tr>
<td>Cloud Access</td>
<td>Controls Sub-Tenant access level for Master Tenant publicly visible Clouds.</td>
</tr>
<tr>
<td>Instance Type Access</td>
<td>Controls Tenant and User access level for Instance Types.</td>
</tr>
</tbody>
</table>

#### 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)
- Infrastructure: Storage (None, Read, Full)
- Logs (None, Read, User, Full)
- Monitoring (None, Read, User, Full)
- Operations: Analytics (None, Read, Full)
- Operations: Approvals (None, Read, Full)
- Operations: Dashboard (None, Read)
- Operations: Guidance (None, Read, Full)
Operations: Reports (None, Read, Full)
Operations: Scheduling - Power (None, Read, Full)
Operations: Usage (None, Read, Full)
Provisioning: (None, Read, User, Full)
Provisioning: Allow Force Delete: (None, Full)
Provisioning: Apps: (None, Read, User, Full)
Provisioning: Automation Services (None, Read, Full)
Provisioning: Deployment Services (None, Read, Full)
Provisioning: Deployments (None, Read, Full)
Provisioning: Library (None, Read, Full)
Provisioning: Migrations (None, Read, Full)
Provisioning: Tasks (None, Read, Full)
Provisioning: Tasks - Script Engines (None, Full)
Provisioning: Blueprints (None, Read, Full)
Provisioning: Blueprints - ARM (None, Provision, Full)
Provisioning: Blueprints - Terraform (None, Provision, Full)
Provisioning: Thresholds (None, Read, Full)
Provisioning: Virtual Images (None, Read, Full)
Remote Console (None, Provisioned, Full)
Remote Console: Auto Login (No, Yes)
Services: Archives (None, Read, Full)
Services: Cypher (None, Read, Full, Full Decrypted)
Services: Image Builder (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:

   **Username & Email**
   
   - First Name
   - Last Name
   - Username
   - Email address

   **Receive Notifications** Enable to receive Provisioning and Policy email notifications.

   **Roles** Role(s) to be inherited by the user. If multiple roles are selected, the higher permission levels of one role will override the other role(s).

   **Password** Password must contain at least one uppercase letter, one lowercase letter, a number, and a symbol.
Enabled  If unchecked, the user will no longer be able to sign into Morpheus, but their user data will remain.

Password Expired  If enabled, the User will be forced to create a new password upon next login. The expired password cannot be used again.

Linux Settings  Creates a User with the supplied Username, Password and/or Key-pair on Linux Instances when “Create my User” is selected during provisioning, or a User Group is added to an Instance of which this Morpheus user is a member of.

Windows Settings  Creates a User with the supplied Username, Password and/or Key-pair on Windows Instances when “Create my User” is selected during provisioning, or a User Group is added to an Instance of which this Morpheus user is a member of.

Important:  Please ensure password entered is allowable by Windows.

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 groupld 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 groupld to assign Group members to in linux.
   - SUDO ACCESS Enable to give Group members sudo access
   - USERS Search for and select existing Users to add to the User Group.
5. Select SAVE CHANGES.

Editing User Groups

1. Navigate to Administration -> Users.
2. Select the USER GROUPS tab.
3. Select the ACTIONS dropdown next to the target User Group.
4. Select **EDIT**

5. Make changes, add or remove users from the group.

6. Select **SAVE CHANGES**.

**Adding a User Group when Provisioning**

1. When provisioning, in the CONFIG section expand the USER section.

2. Select an existing Group from the USER GROUP dropdown.

3. Users will be created for members in the selected User Group on the provisioned Instance(s).

### 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 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.

#### 4.7.1 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.*

#### 4.7.2 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.

4.6. Integrations
• **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.

### 4.7.3 PXE Boot Settings

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

**Environments**

*Administration -> Provisioning -> Environments*

### 4.7.4 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.

### 4.7.5 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.

**Licenses**

*Administration -> Provisioning -> Licenses*

### 4.7.6 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.
4.7.7 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

4.7.8 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 Instance types (VMware, AWS, Nutanix, Openstack etc). Virtual Images can be removed from a License by editing the License.

4.7.9 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.
4.8 Monitoring Settings

4.8.1 Overview

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

4.8.2 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.

4.8.3 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.
4.8.4 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>

4.8.5 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.

4.9 Backup Settings

Administration -> Backups

4.9.1 Overview

The Backups Settings page allows you to 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.)
4.9.2 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

Backup Appliance  When enabled, a Backup will be created to backup the Morpheus appliance database. Select the 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.

4.9.3 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.”
4.9.4 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)

4.10 Logging Settings

4.10.1 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.

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

4.10.2 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.

4.10.3 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.

4.10.4 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.

4.11 Appliance Settings

The Administration -> Settings section sets global configuration parameters for the Appliance, Tenant Registration, Email, Proxy and sets which Cloud types are enabled.
4.11.1 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.

```bash
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.

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
- SMTP Password

**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
• Hyper-V
• MacStadium
• Oracle VM
• HP
• Supermicro
• Dell
• SCVMM
• UpCloud
• Kubernetes
• Cloud Foundry

4.11.2 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
- Footer Background
- Footer Foreground
- Login Background

Override CSS

Override CSS settings by entering CSS in Override CSS field.

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

```
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.
4.11.3 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.
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 reattempts the check after 30 seconds to eliminate false positives. This will convert the check into a Failed state and raise the appropriate severity incident depending on the grouping of the check. When a check recovers it automatically goes into a Warning state. This will remain in the warning state until 10 successful check runs have completed.
Options

All check types have several core options and some of these default options can be configured in Admin -> Monitoring. This includes the default check interval time. By default a check is run every 5 minutes. This can however be changed to run as frequently as once every minute.

- **Max Severity**: The maximum severity level impact for a created incident that can occur if the check fails (defaults to Critical).
- **Check Interval**: The frequency with which a check is run (default 5 minutes).
- **Affects Availability**: Whether or not this check impacts overall system availability calculations.

SSH Tunneling

In many cases when it comes to monitoring databases, and services they may not be fronted on the public ip’s for external monitoring. To reach these safely, and securely Morpheus provides an SSH Tunneling mechanism for its check servers. This allows the check to be confirmed via an ssh port tunnel securely using a keypair.

Check Servers

On a base installation of Morpheus a single check server is installed on the appliance. This is used for running any custom user checks. This services 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.

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 targeting specific checks, groups, or apps, and adding the appropriate recipients to be notified during a situation in which those filters are impacted.

- **Min Duration**: This setting delays notification to the recipients by the entered number of minutes required for the incident to be opened.

- **Min Severity**: Some executives might want to be notified of an outage but only if the severity impact goes above a certain level. This is very useful for scoping escalations.

To add recipients to a rule just start typing their name in the Recipients section towards the bottom 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 AppDynamics 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

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

   ```conf
   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.
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. 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.

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.

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.

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:
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

8.3. Analytics
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 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 days Schedule. Green sections indicate Power on, red sections indicate Power Off. Time indicated applies to selected Time Zone.
8.5.3 Add Power Schedule to Instance

1. Navigate to Provisioning -> Instances
2. Select an Instance

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.
3. Select EDIT
4. In the POWER SCHEDULE dropdown, select a Power Schedule.
5. Select SAVE CHANGES

### 8.5.4 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

### 8.5.5 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

### 8.5.6 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.

8.6 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:

8.6. 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 ServiceNow, 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 ins *Administration -> Provisioning* and Service Plans configured with Prices 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.
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/mypassword` generates a 15 character password).

**Key** Pattern “password/character_length/key”

Example: `password/10/mypassword`

**Value** Leave the Value field 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 field 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')%>

Important: Cypher keys are not multi-tenant and only usable in the Tenant they are created. Please consider this when using cypher keys in library scripts used in multi-tenant/public workflows and library items.

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. The 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

Morpheus appliance supports Ansible integration for configuration management. Morpheus accomplishes this by integrating with an existing repository of playbooks as the master in a master-slave Ansible architecture. To get started the only requirement is an existing repository for playbooks in a very simple structure.

Add Ansible Integration

1. Navigate to Administration -> 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.
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 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.
- **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.

10.1.2 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 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

10.1.3 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
1. Save Changes

10.1.4 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

![Add Salt Integration](image)

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
<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TYPE</td>
<td>Salt Master</td>
</tr>
<tr>
<td>NAME</td>
<td>Labs Salt Master</td>
</tr>
<tr>
<td>SALT MASTER</td>
<td>192.168.162.51</td>
</tr>
<tr>
<td>SSH PORT</td>
<td>22</td>
</tr>
<tr>
<td>USERNAME</td>
<td>morpheus</td>
</tr>
<tr>
<td>PASSWORD</td>
<td><em>........................</em></td>
</tr>
<tr>
<td>KEY PAIR</td>
<td>Select</td>
</tr>
<tr>
<td>WORKING DIRECTORY</td>
<td>/srv/salt</td>
</tr>
<tr>
<td>SALT VERSION</td>
<td></td>
</tr>
</tbody>
</table>
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

```
salt '*' test.ping
```

will return empty unless there are existing Minions with accepted keys on the Master. However, provisioning Minions via Morpheus is extremely easy.

**Provisioning with Saltstack**

To do so, provision as usual and Instances within the Group tied to the Saltstack Integration will now show additional options on the Configure pane
Minion ID defaults to the hostname, and a State can be applied directly at provision time.

**Note:** Only States served from the Master’s Working Directory can be applied at provision, not States from a git backend

Once your instance is provisioned and key negotiation has completed you will be able to access it and run commands via the integrated Salt command center in your Group.
If you did not apply a state at provision time now you will be able to run State commands through Morpheus.

In our example the Apache State from a git backend was applied successfully to our newly created vm.
10.1.5 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.

**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.
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.

   ```bash
   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 App Blueprint
   - **DESCRIPTION** Description for your 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 field 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 Administration -> Backups
2. Expand the Commvault section
3. Enable the integration
4. Fill in the following:
   - **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.
   - **Username**: Admin Username for Commvault
   - **Password**: Password for Username provided (encrypted in Morpheus).
5. **SAVE**

### 10.2.2 Veeam

**Adding Veeam Integration**

1. Navigate to *Administration -> Backups*
2. Expand the Veeam section
3. Enable the integration
4. Fill in the following:
   - **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.
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”.

10.3 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.

**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.
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

```json
{
    "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:CreateSnapshot",
                "ec2:CreateInstanceExportTask",
                "ec2:CreateKeyPair",
                "ec2:CreateNetworkAcl",
                "ec2:CreateNetworkAclEntry",
                "ec2:CreateNetworkInterface",
                "ec2:CreateSecurityGroup",
                "ec2:CreateSnapshot",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteKeyPair",
                "ec2:DeleteNetworkAcl",
                "ec2:DeleteNetworkAclEntry",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteSnapshot",
                "ec2:DeleteTags",
                "ec2:DeleteVolume",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAddresses",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeClassicLinkInstances",
                "ec2:DescribeConversionTasks",
                "ec2:DescribeExportTasks",
                "ec2:DescribeImageAttribute",
            ]
        }
    ]
}
```

(continues on next page)
"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:

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "rds:AddRoleToDBCluster",
                "rds:AddTagsToResource",
                "rds:ApplyPendingMaintenanceAction",
                "rds:AuthorizeDBSecurityGroupIngress",
                "rds:CopyDBClusterParameterGroup",
                "rds:CopyDBClusterSnapshot",
                "rds:CopyDBInstance",
                "rds:CreateDBCluster",
                "rds:CreateDBClusterSnapshot",
                "rds:CreateDBInstance",
                "rds:CreateDBInstanceReadReplica",
                "rds:CreateDBSecurityGroup",
                "rds:CreateDBSnapshot",
                "rds:DeleteDBCluster",
                "rds:DeleteDBInstance",
                "rds:DeleteDBSecurityGroup",
                "rds:DeleteDBSnapshot",
                "rds:DescribeAccountAttributes",
                "rds:DescribeCertificates",
                "rds:DescribeDBClusterParameterGroups",
                "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:DescribeSourceRegions",
                "rds:ListTagsForResource",
            ]
        }
    ]
}
```

(continues on next page)
<table>
<thead>
<tr>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;rds:ModifyDBCluster&quot;</td>
</tr>
<tr>
<td>&quot;rds:ModifyDBClusterParameterGroup&quot;</td>
</tr>
<tr>
<td>&quot;rds:ModifyDBClusterSnapshotAttribute&quot;</td>
</tr>
<tr>
<td>&quot;rds:ModifyDBInstance&quot;</td>
</tr>
<tr>
<td>&quot;rds:ModifyDBParameterGroup&quot;</td>
</tr>
<tr>
<td>&quot;rds:ModifyDBSnapshot&quot;</td>
</tr>
<tr>
<td>&quot;rds:ModifyDBSnapshotAttribute&quot;</td>
</tr>
<tr>
<td>&quot;rds:PromoteReadReplica&quot;</td>
</tr>
<tr>
<td>&quot;rds:PromoteReadReplicaDBCluster&quot;</td>
</tr>
<tr>
<td>&quot;rds:RebootDBInstance&quot;</td>
</tr>
<tr>
<td>&quot;rds:RemoveRoleFromDBCluster&quot;</td>
</tr>
<tr>
<td>&quot;rds:RemoveTagsFromResource&quot;</td>
</tr>
<tr>
<td>&quot;rds:RestoreDBClusterFromS3&quot;</td>
</tr>
<tr>
<td>&quot;rds:RestoreDBClusterFromSnapshot&quot;</td>
</tr>
<tr>
<td>&quot;rds:RestoreDBClusterToPointInTime&quot;</td>
</tr>
<tr>
<td>&quot;rds:RestoreDBInstanceFromDBSnapshot&quot;</td>
</tr>
<tr>
<td>&quot;rds:RestoreDBInstanceToPointInTime&quot;</td>
</tr>
<tr>
<td>&quot;rds:RevokeDBSecurityGroupIngress&quot;</td>
</tr>
</tbody>
</table>

S3

```json
{
  "Version": "2012-10-17",
  "Statement": [
  {
    "Sid": "access-1",
    "Effect": "Allow",
    "Action": [
      "s3:AbortMultipartUpload",
      "s3:DeleteObject",
      "s3:DeleteObjectVersion",
      "s3:GetBucketLocation",
      "s3:GetObject",
      "s3:GetObjectVersion",
      "s3:ListBucket",
      "s3:ListBucketMultipartUploads",
      "s3:ListBucketVersions",
      "s3:ListMultipartUploads",
      "s3:PutObject"
    ],
    "Resource": [
      "arn:aws:s3:::bucketname",
      "arn:aws:s3:::bucketname/*"
    ]
  }
]}
```
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:

```
{
  "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"
    }
  }
}
```

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:

Old and New Portal Naming Conventions:

<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 ID 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.

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 virtual network](image)

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 an 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 AdminSettings. 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:

---

**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 FOUNDRY** 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.

**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 Integraiton 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.
2. Then, click `+ Add Resource`.
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](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:

```yaml
---
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](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.

10.3. Clouds
• The \textit{random-route} parameter, as well as all other parameters described in the Cloud Foundry documentation will simply be passed through to Cloud Foundry.

\section*{Adding Marketplace Items}

1. Navigate to \texttt{Infrastructure -> Clouds} and select your Cloud Foundry Cloud
2. Select the \texttt{MARKETPLACE} tab
3. Select + \texttt{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 \texttt{SAVE CHANGES}

A Node Type and layout will be created in the \texttt{Provisioning -> Library} section and the layout will be automatically added to the Instance Type selected when adding the Marketplace Item.

\section*{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 \texttt{Provisioning -> Instances} and select an Instance Type with a Cloud Foundry layout (MySQL, Redis and RabbitMQ plus Marketplace additions)
2. Select \texttt{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 \texttt{NEXT}
7. Select Version and Instance Configuration for a Cloud Foundry layout, ex: \textit{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 \texttt{NEXT}
12. Optionally configure Automation options
13. Select \texttt{NEXT}
14. Select \texttt{COMPLETE}

\textbf{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.

**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 integration 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.

**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

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, begging 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.

**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!

10.3.8 Hyper-V

Hyper-V is the virtualized server computing environment introduced by Microsoft. Hyper-V is consumed by Morpheus as a private cloud offering and is a common hypervisor technology in data centers. Morpheus provides an avenue to aggregate Hyper-V resources together to allow efficient and seamless deployment of applications as a virtual machine (VM) or Docker host in the world of Hyper-V.

Features

- Virtual Machine Provisioning
- 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:

```
$ winrm set winrm/config/service/Auth @{Basic="true"}
$ winrm set winrm/config/service @{AllowUnencrypted="false"}
$ winrm set winrm/config/service/Auth @{Kerberos="true"}
```

Kerberos authentication will also need to be configured on the Morpheus appliance to support Windows domain accounts to access the remote host with WINRM_INTERNAL connection type.

On the Morpheus appliance the krb5-user package must be installed.

For Ubuntu the command is as follows:

```
$ sudo apt-get install krb5-user
```

For Centos the command is as follows:

```
$ 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 communicated 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.
Docker

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
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.

**10.3.10 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.

10.3.11 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.
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.

10.3.12 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 scapable 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.

### 10.3.13 Oracle VM

**Add a 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.

### 10.3.14 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:
   - **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

4. The Cloud can now be added to a Group or configured with additional Advanced options.
10.3.15 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.

10.3.16 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

10.3.17 UpCloud

Overview

UpCloud is a cloud hosting provider that offers both Linux and Windows virtual machines on their MAXIOPS in-
frastucture 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 be 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
- GRAILS
- JAVA
- MONGO
- MYSQL
- NGINX
- PHP
- RABBITMQ
- REDIS
- OMCAT
- UBUNTU
- WINDOWS
- GRAILS

10.3.18 vCloud Director

How to create vCloud Director templates for Morpheus

To create a Windows Template

Create a new machine in VMware vCenter and install a base version of your preferred Windows build.

1. Apply any service packs / updates to the operating system.
2. Set the Network location to Private the below PowerShell will set the location.

```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.
7. Shutdown the virtual machine and convert to a template.

**Note:** Do not run sysprep

---

### To create a Linux Centos template

Create a new machine in VMware vCenter and install a base version of your preferred Linux distro build. If you are using cloud init as part of your image you will need to ensure your virtual machine has a cdrom.

1. Before installing the operating system setup a single `ext` or `xfs` partition without a swap disk (This is so that `growpart` can extend the disk. `growpart` currently does not support lvm)
2. Install the distro and apply any updates to the operating system and security updates
3. Install cloud-init using command `yum install cloud-init`
4. Install cloud-utils-growpart using command `yum install cloud-init-utils-growpart`
5. Install vmware tools
6. Install git by running `yum install git`
7. epel-release
8. selinux set to permissive (enforced can cause problems with cloud-init)

---

### To create a Linux Ubuntu template

Create a new machine in VMware vCenter and install a base version of your preferred Linux distro build. If you are using cloud init as part of your image you will need to ensure your virtual machine has a cdrom.

1. Before installing the operating system setup a single `ext` 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. 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 administrator.

Once logged into vCloud director you will then need select Manage Organizations and then select your organization.

From within the organisation click on Catalogues > select an existing catalogue or create a new catalogue.

**Note:** Please note once you connect Morpheus to your vCD environment, it will create a catalogue called Auto Morpheus. This is a working catalogue and is ignored by Morpheus when searching for images, so any images in the catalogue will not be synced into Morpheus.

Open the catalogue and select the import template from vCenter and then browse the data stores for your templates. Select your template and the type in a new name and description then check the copy template into vCloud director.

Once you click ok the import process will begin. When the import has completed the template will appear in Morpheus within Provisioning > Virtual Images

If the image does not appear within the virtual images you may need to use the filters to filter the virtual images by the vmware ( vmdk / ovf / ova) type.

You may also need to refresh the cloud. To do this go to Infrastructure > Clouds > select the vCloud Director cloud > select Refresh.

### 10.3.19 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 /urs/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.

**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 Integraiton 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.

**10.3.20 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.

10.3. Clouds 287
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.

**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

10.3.21 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’)
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.
- **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 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*
   - **USERNAME**  Xen Host Username
   - **PASSWORD**  Xen Host Password
   - **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.

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.

**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.

### 10.3.23 Windows Image with Cloudbase-Init

Morphues 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-Init\conf, 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.

```conf
[DEFAULT]
# username=Admin
# groups=Administrators
# inject_user_password=true
inject_user_password=false
first_logonBehaviour=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\
verbose=true
debug=true
logdir=C:\Program Files\Cloudbase Solutions\Cloudbase-Init\log\logfile=cloudbase-init.log
default_log_levels=comtypes=INFO,suds=INFO,iso8601=WARN,requests=WARN
logging_serial_port_settings=
mtu_use_dhcp_config=true
ntp_uce_dhcp_config=true
local_script_path=C:\Program Files\Cloudbase Solutions\Cloudbase-Init\LocalScripts\

# 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
```

(continues on next page)
# 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\
verbose=true
debug=true
logdir=C:\Program Files\Cloudbase Solutions\Cloudbase-Init\log\
logfile=cloudbase-init-unattend.log
default_log_levels=comtypes=INFO,suds=INFO,iso8601=WARN,requests=WARN
logging_serial_port_settings=
mtu_use_dhcp_config=true
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.metadata.
cloudbaseinit.metadata.services.maasservice.
cloudbaseinit.plugins=cloudbaseinit.plugins.common.mtu.MTUPlugin,cloudbaseinit.plugins.common.
sethostname.SetHostNamePlugin,cloudbaseinit.plugins.windows.extendvolumes.
ExtendVolumesPlugin
allow_reboot=false
stop_service_on_exit=false
check_latest_version=false
```

## unattend.xml

```xml
<?xml version="1.0" encoding="utf-8"?>
<unattend xmlns="urn:schemas-microsoft-com:unattend">
  <settings pass="generalize">
    <component name="Microsoft-Windows-Security-SPP" processorArchitecture="amd64"
      publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
      <SkipRearm>1</SkipRearm>
    </component>
    <component name="Microsoft-Windows-PnpSysprep" processorArchitecture="amd64"
      publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
      <PersistAllDeviceInstalls>false</PersistAllDeviceInstalls>
      <DoNotCleanUpNonPresentDevices>false</DoNotCleanUpNonPresentDevices>
    </component>
  </settings>
</unattend>
```

(continues on next page)
<settings pass="oobeSystem">
    <InputLocale>en-US</InputLocale>
    <SystemLocale>en-US</SystemLocale>
    <UILanguage>en-US</UILanguage>
    <UserLocale>en-US</UserLocale>
  </component>
    <OOBE>
      <HideEULAPage>true</HideEULAPage>
      <ProtectYourPC>1</ProtectYourPC>
      <NetworkLocation>Home</NetworkLocation>
      <HideWirelessSetupInOOBE>true</HideWirelessSetupInOOBE>
    </OOBE>
    <TimeZone>UTC</TimeZone>
    <UserAccounts>
      <AdministratorPassword>
        <Value>administratorPassword</Value>
        <PlainText>true</PlainText>
      </AdministratorPassword>
      <LocalAccounts>
        <LocalAccount wcm:action="add">
          <Password>
            <Value>password</Value>
            <PlainText>true</PlainText>
          </Password>
          <Group>administrators</Group>
          <DisplayName>morpheus</DisplayName>
          <Name>morpheus</Name>
          <Description>Morpheus User</Description>
        </LocalAccount>
      </LocalAccounts>
    </UserAccounts>
  </component>
</settings>

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:

```
cd C:\Program Files\Cloudbase Solutions\Cloudbase-Init\conf
```
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.

### 10.3.24 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:

```
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`.

### 10.3. Clouds
Firstly we need to adjust our bootloader to disable interface naming like this.

```bash
sed -i -e 's/quiet/quiet net.ifnames=0 biosdevname=0/ /etc/default/grub
grub2-mkconfig -o /boot/grub2/grub.cfg
```

The above command adds a few arguments to the kernel args list (namely `net.ifnames=0` and `biosdevname=0`). It may be useful to view the `/etc/default/grub` file and ensure these settings were indeed applied.

The next step is to adjust the network-scripts in CentOS. We need to ensure we have a file called `/etc/sysconfig/network-scripts/ifcfg-eth0`

Below is a script that we run on our packer builds to prepare the machines network configuration files.

```bash
export iface_file=$(basename "$(find /etc/sysconfig/network-scripts/ -name 'ifcfg*' -not -name 'ifcfg-lo' | head -n 1)")
export iface_name=${iface_file:6}
echo $iface_file
echo $iface_name
sudo mv /etc/sysconfig/network-scripts/$iface_file /etc/sysconfig/network-scripts/
˓→ifcfg-eth0
sudo sed -i -e "s/$iface_name/eth0/" /etc/sysconfig/network-scripts/ifcfg-eth0
sudo bash -c 'echo NM_CONTROLLED="no" >> /etc/sysconfig/network-scripts/ifcfg-eth0'
```

This script tries to ensure there is a new ifcfg-eth0 config created to replace the old ens config file. Please do verify this config exists after running. If it does not you will have to be sure to build one on your own.

```plaintext
TYPE=Ethernet
DEVICE=eth0
NAME=eth0
ONBOOT=yes
NM_CONTROLLED="no"
BOOTPROTO="dhcp"
DEFROUTE=yes
```

Gotyas

SELinux can cause issues with cloud-init when in enforced mode. It may be advisable to set this to permissive unless it is mandatory within your organization to use an enforced SELinux configuration. If that is the case please see the documentation for the cloud_init_t security policies.

Network Manager will also prevent the required restart of the Network Service when assigning static IP’s. Disable Network Manager when possible or Static IP assignment may not work until the Network Service is restarted manually.

A Note on Proxies

Proxy configurations are known to vary in some organizations and makes building a base blueprint a little more difficult. In order to fully configure proxies a few environment variables must be set in the `/etc/environment` file (This can be done automatically in a default user-data script for cloud-init as well in edit cloud).

```plaintext
http_proxy="http://myproxyaddress:8080"
https_proxy="http://myproxyaddress:8080"
ftp_proxy="http://myproxyaddress:8080"
no_proxy=127.0.0.1,localhost,applianceUrl
https_no_proxy=127.0.0.1,localhost,applianceUrl
```
Important: It is very important to properly set the no_proxy list (applianceUrl) should be replaced with the actual appliance url. In future releases, morpheus plans to automatically take care of this.

Note: If using cloud-init agent install mode these settings need to be set in the custom Cloud-Init User data section of “Edit Cloud” or “Edit Virtual Image”

Important: If using this virtual machine as a docker host, proxy settings must also be configured in the docker config. See Docker guides for instructions on how to properly set this. If necessary this can be wrapped in a task automation workflow for your own use.

10.4 Containers

10.4.1 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.

10.4.2 Docker Registry

Overview

Without any additional configuration Morpheus can provision images from Docker’s public hub at https://hub.docker.com/ using their public api at https://index.docker.io/v1/

However, many organizations maintain private Docker registries for security measures. Additional public and private Docker registries can be added to Morpheus.

Adding a Docker Registry Integration

1. Navigate to Administration -> Integrations
2. Click “New Integration”
3. Select the Docker Repository Type
4. Add the following:
   - Name Name for the Registry in Morpheus
   - Repository url Docker Registry url or IP address
   - Username Username if private registry
   - Password Password if private registry
5. Save Changes

Note: You must either have signed certificates for your registry or configure your docker host(s) to accept insecure registries

Provisioning an Instance from Docker Registry

Docker images from the Integrated Registry can be provisioned using the generic Docker Instance Type, or by adding images to Node Types for custom Library Instance Types.
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.
3. 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.

10.7 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 IDENTIFY SOURCES
4. Select + IDENTIFY 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 Settings -> Accounts
2. Select an account.
3. Select IDENTITY SOURCES in the Account 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

- **TYPE**: SAML [Beta]
- **ACTIVE**: Yes
- **NAME**: SAML
- **DESCRIPTION**: onelogin SAML

SAML Configuration

- **LOGIN REDIRECT URL**: https://morpheusdata-dev.onelogin.com/trust/saml2/http-
  - Do not include SAMLRequest parameter
- **LOGOUT POST URL**: https://morpheusdata-dev.onelogin.com/trust/saml2/http-
- **SIGNING PUBLIC KEY**: MIIEFzCCAv+gAwIBAgIUayYdMuoXBTGcalAARanxhr.JwwtQwDQYJKoZlhlcNAQEF

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">
```

**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 conneciton 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):

   ```
   MIIC8ECCAdigAwIBAgIQEOZX1N5wY9Dc60wsKEMzANBgkqhkiG9w0BAQsFADA0MTIwMAYDVQQDEylNaWNyb3NvZnQgQXp1cmUgRmVkZXJhdGVkIFNTTyBDZX...TlaMDQxMjAwBgNVBAMTTU1pY3Jvc29mdCBBenVyZSBGZWRlcmF0ZWQgU1NPIENlcnRpZmljYXRlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2kJ6GcBpRkoxJd0DLbhubwa0kp651d9i5PUy2ohBHvFAy3S204mXoH7LWvT3oNrqxaNAksbY6phOOkNF/V6GcBpRkoxJd0DLbhubw0d0kp651d9i5PUy2ohBHvFAy3S204mXoH7LWvT3oNrqxaNAksbY6phOOkNF/.../pqp3qw+nYf7DSxzy6tfS6spk64jf2DIt1sVjd7uJmItKPeOCRmeBUcnebzwKqFBO714VF5ql0EJvftT7Wpr4VVoLLe/pH6xzQVRz0GZqpo19V1QJbJqJqLm4LjWT9VU21Yqd0DngtK7QthZo4J02FdUG6qFfTPKqVn0AESxMi4JWxfiqz...y56+ksYSRP87X0dCvVTFtHYmQnD0f0qKrgpMK7LmsEwq7r0Kkh7nTCen2nEBOCFDBFV4QEmrAZrEpJnQs9nJZBN/sdeC
   ```

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 `emailaddress` Namespace url from Azure SSO config: `http://schemas.xmlsoap.org/ws/2005/05/identity/claims`
   - **SURNAME ATTRIBUTE NAME** Enter the `surname` Namespace url from Azure SSO config: `http://schemas.xmlsoap.org/ws/2005/05/identity/claims`
Configure Role Mappings

Role mappings will map Azure AD Groups to Morpheus Roles. Azure AD users will be assigned Roles in Morpheus upon signing 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
2. Select the Tenant to add the Identity Source Integration
3. Select IDENTITIES
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 Service Now

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

**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.

**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

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

<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>

10.9 Load Balancers

10.9.1 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

10.9.2 F5

Add F5 Load Balancer

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/
5. Save Changes

10.10 Logs

10.10.1 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
10.10.2 Splunk

Adding Splunk Integration

1. Navigate to Administration -> Logs
2. Expand the Splunk section
3. Enable the integration
4. 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.
5. SAVE

10.10.3 Syslog

Adding Syslog Integration

1. Navigate to Administration -> Logs
2. Expand the Morpheus logging section
3. Add the Syslog forwarding rules
4. QUICK ADD

10.11 Monitoring

10.11.1 ServiceNow Monitoring Integration

**Note:** A ServiceNow Integration must be already configured in Administration -> Integrations to enable the ServiceNow Monitoring Integration. Refer to the Service Now configuration guide for more information.

<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>
10.11.2 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.

10.11.3 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.

10.12 Networking

10.12.1 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

Adding Infoblox Integration

1. Navigate to *Infrastructure - Network - Services*
2. Select *ADD -> IPAM -> Infoblox*
3. Enter the following:

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>InfoBlox 2.3.1api</td>
</tr>
<tr>
<td>Enabled</td>
<td>☑️</td>
</tr>
<tr>
<td>URL</td>
<td><a href="https://10.30.21.25/wapi/v2.3.1/">https://10.30.21.25/wapi/v2.3.1/</a></td>
</tr>
<tr>
<td>USERNAME</td>
<td>admin</td>
</tr>
<tr>
<td>PASSWORD</td>
<td>************</td>
</tr>
<tr>
<td>Disable SSL SNI Verification</td>
<td>☐️</td>
</tr>
<tr>
<td>NETWORK FILTER</td>
<td></td>
</tr>
<tr>
<td>TENANT MATCH ATTRIBUTE</td>
<td></td>
</tr>
<tr>
<td>IP MODE</td>
<td>Static IPs</td>
</tr>
</tbody>
</table>

**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

SAVE IPAM INTEGRATION
**NETWORK FILTER**  Filter which networks are synced into Morpheus. Example: Network Filter: `[network_view=default&*Building=work ]`

**TENTANT 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)

- 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
CREATE HOST RECORD

HOSTNAME  sample
IP ADDRESS  10.30.23.88
DOMAIN  infoblox.den.bertramlabs.com

Create DNS Records

SAVE CHANGES

**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
10.12.2 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

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
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
   • 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

10.13 Service Discovery

10.13.1 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!

10.14 Storage

10.14.1 AzureStorage

To Add Azure Storage

1. Navigate to Infrastructure -> Storage
2. Select + ADD
3. From the New Storage Provider Wizard input the following:
   - **Name**: Name of the storage provider.
   - **Provider Type**: Azure
   - **Storage Account**: Add Storage Account
   - **Storage Key**: Add Storage Key
   - **Share Name**: Add Share Name
   - **Targets**
     - Default Backup Target
     - Default Deployment Archive Target
     - Default Virtual Image Store
4. Save Changes
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>WinRM</td>
<td>Windows</td>
<td>Appliance</td>
<td>Node</td>
<td>Node</td>
<td>5985</td>
<td>DNS Resolution from node to appliance url</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Virtual Images configured</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>WinRM Enabled on Virtual Image (winrm quickconfig)</td>
</tr>
<tr>
<td>Cloud-init</td>
<td>Linux</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Cloud-init installed on template/image</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Cloud-init settings populated in User Settings or in Admin -&gt; Provisioning</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Agent install mode set to Cloud-Init in Cloud Settings</td>
</tr>
<tr>
<td>Cloudbase-init</td>
<td>Windows</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Cloudbase-init installed on template/image</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Cloud-init settings populated in User Settings or in Admin -&gt; Provisioning</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Agent install mode set to Cloud-Init in Cloud Settings</td>
</tr>
<tr>
<td>VMtools</td>
<td>All</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>VMtools installed on template</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Cloud-init settings populated in Morpheus user settings or in Administration -&gt; Provisioning when using Static IP’s</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Existing User credentials entered on Virtual Image 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 Administration -&gt; Provisioning</td>
</tr>
</tbody>
</table>

332 Chapter 11. Troubleshooting
11.2 Morpheus Agent Install Troubleshooting

When provisioning and 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.

**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`
- 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/Morphues/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"
   $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()
   ```
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 stop rsyslogd
sudo apt-get -y purge morpheus-vm-node
sudo rm -rf /opt/morpheus-node
sudo usermod -l morpheus-old morpheus-node
sudo killall runsv
sudo killall runsvdir
sudo killall morphd
```

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 (VMware Hypervisor Console)**  The VNC protocol will be used for all platform types in VMware Clouds with the Hypervisor Console option enabled in cloud settings. A unique port is assigned per per Virtual Machine starting at 5900.

**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 VMware cloud settings, the VNC protocol will be used for all platform types that VMware Cloud.

When using VNC Hypervisor Console, the Morpheus Appliance connects directly to the ESXi host the VM is on, not directly to the VM. A VNC port is assigned per Virtual Machine starting at 5900 and a complex VNC password is generated. VNC is then enabled and the port and password are set on the VMs settings in vSphere.

Morpheus features Remote Console support directly to VMware ESXi hypervisors. To enable this feature a few prerequisites must be met:

• The gdbserver Firewall setting needs to be enabled on each ESXi host the console will connect to. This can be done in vSphere under firewall configuration on the ESXi hosts by checking the gdbserver option on each required host, This will open up the necessary ports VNC ports on the ESXi host(s), starting at port 5900.

**Note:** The most common cause of Remote Console connection issues when using hypervisor console is gdbserver not being enabled on the ESXi hosts firewall settings.

• The Morpheus Appliance must have network access to the ESXi hosts within vCenter, specifically to the host the VM is on when using Remote Console, over the VNC port range, typically 5900-6000. The connection does not go through the vCenter server(s).

• The Morpheus Appliance must be able to resolve the ESXi hostnames.

• VMware tools or equivalent must be installed on the VM.
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 VVM 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. The

**Important:** All VMs that are inventoried or provisioned into a VMware cloud with Hypervisor Console enabled will have their Console Type set to VNC. Disabling Hypervisor Console will only apply to newly inventoried or provisioned VM's. VM's inventoried or provisioned when Hypervisor Console was enabled will continue to use the VNC protocol even after Hypervisor Console is disabled. To revert a VM

### 11.3.3 Copy and Paste

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 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 guacd 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 successful.
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 Cannot Login

11.4.1 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.

11.4.2 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`

### 11.4.3 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.

### 11.5 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

   ```
   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:

   ```
   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:

```sql
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
```

### 11.6 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

### 11.7 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
   ```

### 11.8 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}`

**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%>
```
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>instance.displayName</td>
<td>&lt;%=instance.displayName%&gt;</td>
</tr>
<tr>
<td>instance.description</td>
<td>&lt;%=instance.description%&gt;</td>
</tr>
<tr>
<td>instance.environmentPrefix</td>
<td>&lt;%=instance.environmentPrefix%&gt;</td>
</tr>
<tr>
<td>instance.hostname</td>
<td>&lt;%=instance.hostname%&gt;</td>
</tr>
<tr>
<td>instance.domainName</td>
<td>&lt;%=instance.domainName%&gt;</td>
</tr>
<tr>
<td>instance.firewallEnabled</td>
<td>&lt;%=instance.firewallEnabled%&gt;</td>
</tr>
<tr>
<td>instance.status</td>
<td>&lt;%=instance.status%&gt;</td>
</tr>
<tr>
<td>instance.userStatus</td>
<td>&lt;%=instance.userStatus%&gt;</td>
</tr>
<tr>
<td>instance.networkLevel</td>
<td>&lt;%=instance.networkLevel%&gt;</td>
</tr>
<tr>
<td>instance.instanceLevel</td>
<td>&lt;%=instance.instanceLevel%&gt;</td>
</tr>
<tr>
<td>instance.deployGroup</td>
<td>&lt;%=instance.deployGroup%&gt;</td>
</tr>
<tr>
<td>instance.instanceContext</td>
<td>&lt;%=instance.instanceContext%&gt;</td>
</tr>
<tr>
<td>instance.autoScale</td>
<td>&lt;%=instance.autoScale%&gt;</td>
</tr>
<tr>
<td>instance.statusMessage</td>
<td>&lt;%=instance.statusMessage%&gt;</td>
</tr>
<tr>
<td>instance.expireDate</td>
<td>&lt;%=instance.expireDate%&gt;</td>
</tr>
<tr>
<td>instance.tags</td>
<td>&lt;%=instance.tags%&gt;</td>
</tr>
<tr>
<td>instance.storage</td>
<td>&lt;%=instance.storage%&gt;</td>
</tr>
<tr>
<td>instance.memory</td>
<td>&lt;%=instance.memory%&gt;</td>
</tr>
<tr>
<td>instance.cores</td>
<td>&lt;%=instance.cores%&gt;</td>
</tr>
<tr>
<td>instance.configId</td>
<td>&lt;%=instance.configId%&gt;</td>
</tr>
<tr>
<td>instance.configGroup</td>
<td>&lt;%=instance.configGroup%&gt;</td>
</tr>
<tr>
<td>instance.configRole</td>
<td>&lt;%=instance.configRole%&gt;</td>
</tr>
<tr>
<td>instance.containers[0]</td>
<td>&lt;%=instance.containers[0].containerTypeName%&gt;</td>
</tr>
<tr>
<td>instance.createdByUsername</td>
<td>&lt;%=instance.createdByUsername%&gt;</td>
</tr>
<tr>
<td>instance.createdByEmail</td>
<td>&lt;%=instance.createdByEmail%&gt;</td>
</tr>
<tr>
<td>instance.createdByFirstName</td>
<td>&lt;%=instance.createdByFirstName%&gt;</td>
</tr>
<tr>
<td>instance.createdByLastname</td>
<td>&lt;%=instance.createdByLastname%&gt;</td>
</tr>
<tr>
<td>instance.createdById</td>
<td>&lt;%=instance.createdById%&gt;</td>
</tr>
<tr>
<td>container.containerType</td>
<td>&lt;%=container.containerType%&gt;</td>
</tr>
<tr>
<td>container.containerTypeCode</td>
<td>&lt;%=container.containerTypeCode%&gt;</td>
</tr>
<tr>
<td>container.containerTypeShortName</td>
<td>&lt;%=container.containerTypeShortName%&gt;</td>
</tr>
<tr>
<td>container.provisionType</td>
<td>&lt;%=container.provisionType%&gt;</td>
</tr>
<tr>
<td>container.dataPath</td>
<td>&lt;%=container.dataPath%&gt;</td>
</tr>
<tr>
<td>container.logsPath</td>
<td>&lt;%=container.logsPath%&gt;</td>
</tr>
<tr>
<td>container.configPath</td>
<td>&lt;%=container.configPath%&gt;</td>
</tr>
<tr>
<td>container.planCode</td>
<td>&lt;%=container.planCode%&gt;</td>
</tr>
<tr>
<td>container.dateCreated</td>
<td>&lt;%=container.dateCreated%&gt;</td>
</tr>
<tr>
<td>container.status</td>
<td>&lt;%=container.status%&gt;</td>
</tr>
<tr>
<td>container.environmentPrefix</td>
<td>&lt;%=container.environmentPrefix%&gt;</td>
</tr>
<tr>
<td>container.version</td>
<td>&lt;%=container.version%&gt;</td>
</tr>
<tr>
<td>container.image</td>
<td>&lt;%=container.image%&gt;</td>
</tr>
<tr>
<td>container.internalHostname</td>
<td>&lt;%=container.internalHostname%&gt;</td>
</tr>
<tr>
<td>container.hostname</td>
<td>&lt;%=container.hostname%&gt;</td>
</tr>
<tr>
<td>container.domainName</td>
<td>&lt;%=container.domainName%&gt;</td>
</tr>
<tr>
<td>container.storage</td>
<td>&lt;%=container.storage%&gt;</td>
</tr>
<tr>
<td>container.memory</td>
<td>&lt;%=container.memory%&gt;</td>
</tr>
<tr>
<td>container.cores</td>
<td>&lt;%=container.cores%&gt;</td>
</tr>
<tr>
<td>container.internalIp</td>
<td>&lt;%=container.internalIp%&gt;</td>
</tr>
<tr>
<td>container.externalIp</td>
<td>&lt;%=container.externalIp%&gt;</td>
</tr>
<tr>
<td>container.sshHost</td>
<td>&lt;%=container.sshHost%&gt;</td>
</tr>
<tr>
<td>container.hostMountPoint</td>
<td>&lt;%=container.hostMountPoint%&gt;</td>
</tr>
<tr>
<td>container.configId</td>
<td>&lt;%=container.configId%&gt;</td>
</tr>
<tr>
<td>container.configGroup</td>
<td>&lt;%=container.configGroup%&gt;</td>
</tr>
<tr>
<td>container.configRole</td>
<td>&lt;%=container.configRole%&gt;</td>
</tr>
<tr>
<td>container.serverId</td>
<td>&lt;%=container.serverId%&gt;</td>
</tr>
<tr>
<td>container.server</td>
<td>&lt;%=container.server%&gt;</td>
</tr>
<tr>
<td>server.serverType</td>
<td>&lt;%=server.serverType%&gt;</td>
</tr>
</tbody>
</table>
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%>
zone.name: <%=zone.name%>
zone.code: <%=zone.code%>
zzone.location: <%=zone.location%>
zzone.cloudTypeName: <%=zone.cloudTypeName%>
zzone.cloudTypeCode: <%=zone.cloudTypeCode%>
zzone.domainName: <%=zone.domainName%>
zzone.scalePriority: <%=zone.scalePriority%>
zzone.firewallEnabled: <%=zone.firewallEnabled%>
zzone.regionCode: <%=zone.regionCode%>
zzone.agentMode: <%=zone.agentMode%>
zzone.datacenterId: <%=zone.datacenterId%>
ggroup.code: <%=group.code%>
ggroup.name: <%=group.name%>
ggroup.location: <%=group.location%>
ggroup.datacenterId: <%=group.datacenterId%>

instance {
    instanceTypeName,
    instanceTypeCode,
    provisionType,
    instanceVersion,
    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: { 
  serverTypeName, serverTypeCode, parentServerId, plan, visibility, osTypeCode, sourceImageId, name, displayName, internalName, category, description internalId, externalId, platform, platformVersion, agentVersion, nodePackageVersion, sshHost, sshPort, sshUsername, consoleType, consoleHost, consolePort, consoleUsername, internalSshUsername, internalIp, externalIp, osDevice, dataDevice, lvmEnabled,
}

(continues on next page)
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,
configRole
volumes {
    name
    id
deviceName
maxStorage
unitNumber
displayOrder
rootVolume
}
}

cloud {
    name,
code,
location,
cloudTypeName,
cloudTypeCode,
domainName,
scalePriority,
firewallEnabled,
regionCode,
agentMode,
datacenterId
}

group {
    code,
name,
location,
datacenterId
}
11.9 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

11.10 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 |
12.1 v3.5.0

Release date: 7/31/2018

12.1.1 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

12.1.2 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

12.2 v3.4.1

Release date: 7/20/2018

12.2.1 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 Template 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

12.2.2 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

• 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

12.3 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.

12.3.1 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.

12.3.2 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 .

12.4 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
12.4.1 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

12.4.2 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
• Fix for CentOS 7.2 Answer File in boot configurator for PXE

**Important:** If upgrading from versions earlier than 3.2.0 please follow the 3.2.0+ upgrade instructions below

### 12.4.3 3.2.0+ Upgrades

**Overview**

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.

**Morpheus All-In-One**

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.

### Morpheus Distributed High Availability

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.
12.5 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

### 12.5.1 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.

12.5.2 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

12.5.3 3.2.0+ Upgrades

Overview

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.

**Morpheus All-In-One**

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.

**Morpheus Distributed High Availability**

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`. 

12.5. v3.3.1 369
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.

12.6 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.

12.6.1 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

12.6.2 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!

12.6.3 3.2.0+ Upgrades

Overview

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.

Morpheus All-In-One

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.

### Morpheus Distributed High Availability

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 -`.
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.

---

**12.7 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.

12.7.1 New Features

- Alibaba - Docker Host provisioning added
- ServiceNow: Kingston support for SNOW Morpheus plug-in

12.7.2 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!
12.7.3 3.2.0+ Upgrades

Overview

Upgrading from previous versions of Morpheus to 3.2.0 or later requires upgrading ElasticSearch to 5.4.1 or 5.6. 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.

Morpheus All-In-One

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.
Morpheus Distributed High Availability

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.

### 12.8 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.

#### 12.8.1 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

12.8.2 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!

12.8.3 3.2.0+ Upgrades

Overview

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.

Morpheus All-In-One

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.

Morpheus Distributed High Availability

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.

### 12.9 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.

#### 12.9.1 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
12.9.2 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!

12.9.3 3.2.0+ Upgrades

**Overview**

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.

**Morpheus All-In-One**

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.

**Morpheus Distributed High Availability**

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.
12.10  v3.1.5

12.10.1 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

12.11  v3.1.4

12.11.1 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/
12.11.2 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

12.12 v3.1.3

12.12.1 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

12.12.2 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.

12.13 v3.1.2 & v2.12.5

12.13.1 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

12.13.2 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

12.13. v3.1.2 & v2.12.5 387
• 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

12.14 v3.1.1

12.14.1 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.

12.14.2 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

12.15 v3.1.0

12.15.1 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).
12.15.2 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.

12.16 v3.0.1

12.16.1 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.

12.16.2 New Integrations

- UpCloud
• Cloud Foundry
• IBM Bluemix
• HP OneView
• SCVMM
• Kubernetes
• Jenkins
• Github

12.16.3 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.

12.17 v2.12.4

12.17.1 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

12.17.2 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/>’.

12.18 v2.12.3

v2.12.3 release date 10/24/2017

12.18.1 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

12.18.2 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/>’.

12.19 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

• Script Variables added for Volumes: id: vol.id, name: vol.name, deviceName: vol.deviceName, maxStorage: vol.maxStorage, unitNumber: vol.unitNumber, displayOrder: vol.displayOrder, rootVolume: vol.rootVolume

• 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/>'.

### 12.20 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.
12.20.1 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.

12.20.2 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

12.20.3 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

12.21 v2.12.0

12.21.1 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

12.22 v2.11.4

12.22.1 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 provisioning. 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 integration 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.

**12.22.2 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

**12.22.3 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
12.23 v2.11.3 & 2.10.8

**Important:** ACCOUNTS has been renamed to TENANTS in v2.11.3

### 12.23.1 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 dropdown 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

12.23.2  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