Hive Fabric 6.12 Administration Guide

1. Hive Fabric Administration Guide 3
1.1 Release Notes 4
1.2 Patching and Upgrading Fabric 5
1.3 Upgrading 6.11.0 to 6.12.0 6
1.4 Requirements, Dependencies and Sizing 7
1.5 Glossary 8
1.6 Introduction 9
1.7 Appliance Installation 10
1.7.1 USB Drive 11
1.7.1.1 Windows USB Installation 12
1.7.2 Intelligent Platform Management Interface (IPMI) 13
1.7.2.1 Dell Remote Access Control 14
1.7.2.2 Lenovo Integrated Management Module 15
1.7.2.3 Supermicro Intelligent Management 16
1.7.2.4 HP Integrated Lights-Out 17
1.7.2.5 Cisco Integrated Management Controller 18
1.7.3 PXE Installation 19
1.7.4 First Boot Wizard 20
1.7.5 Initial Deployment 22
1.8 Appliance Administration 23
1.8.1 Console Management 24
1.8.1.1 Status 25
1.8.1.2 Networking 26
1.8.1.3 Management 27
1.8.2 Navigating the User Interface 28
1.8.3 Inventory 29
1.8.3.1 Overview 30
1.8.3.2 System Graphs 32
1.8.3.3 Network Graphs 33
1.8.3.4 Guest Management 34
1.8.4 Publishing 35
1.8.4.1 Storage Pools 36
1.8.4.1.1 Uploading files to a Storage Pool 38
1.8.4.2 Templates 39
1.8.4.2.1 Add an existing Template 40
1.8.4.2.2 Create a New Template 41
1.8.4.2.3 Template Management 44
1.8.4.3 Realms 53
1.8.4.4 Profiles 54
1.8.4.5 Guest Pools 56
1.8.4.6 Standalone Guest 58
1.8.5 Tools 59
1.8.5.1 Convert an Image 60
1.8.6 Settings 61
1.8.6.1 Appliance 62
1.8.6.2 Network Interfaces 63
1.8.6.3 Network Addresses 64
1.8.6.4 Administration 65
1.8.6.5 Users 67
1.9 Template Administration 68
1.9.1 VirtIO Device Drivers Installation 69
1.9.2 Desktop Image Management 70
1.9.3 Guest Session Scripts 71
1.10 Cluster Administration 72
1.10.1 Cluster Dashboard 73
1.10.2 Cluster Best Practice 74
1.10.3 Join a Cluster 75
1.10.4 Remove Appliance from a Cluster 76
1.11 VM Broker 77
1.11.1 Broker 78
1.11.2 Gateway 79

Hive Fabric Administration Guide

This guide outlines how to install, setup, and run the Hive Fabric 6.12 appliance.

Release Notes

What's new for 6.12.0?

- First Boot Wizard - The first boot wizard allows for simple configuration of the key components of Hive Fabric to occur on the console of the Appliance during initial installation of the software. The First Boot Wizard is designed to set basic networking and cluster settings prior to being managed through the Graphical User Interface via a web browser.
- Console Management - The console will guide the user through management of the appliance, should they have the need to directly interface with the appliance through the console rather than through the Web GUI.
- Cluster Enhancements - A Hive Fabric cluster has been tested to 16 physical nodes with over 2500 Guests deployed. The cluster management has been enhanced to ensure that it can scale from a small number of hosts to hundreds of hosts.
- Storage Network - A dedicated storage network can now be configured through the UI allowing isolation of management and storage traffic over the Hive Fabric network.
- User Volumes - User Volumes have been enhanced to provide a backup of the running config on local RAM or disk, increasing the end-user experience and their redundancies.

Known Issues

- APP-1146: First Boot Wizard: Networks may not be visible when attempting to create a bond. If this happens use the Web-UI to create the network bond.
- APP-765: UEFI Support. Hive Fabric does not support UEFI boot for either the install, Appliance boot, or Guests. For installation or appliance boot, use BIOS boot mode.

Resolved Issues

- ~~APP-1004:~~ It was not possible to see the hostname or IP address of an Appliance in the web dashboard. The hostname of the appliance now displays in the web UI dashboard.
- ~~APP-952:~~ There was no way to factory reset an appliance. The Console Management utility introduces a way for the appliance to be set back to the factory defaults just after initial installation.

Patching and Upgrading Fabric

Occasionally, a patch or upgrade may need to be issued for the existing version of Fabric. Upgrading the environment is a simple process, and can be done even if guest pools cannot be shut down. The following instructions given assume that guests are non-persistent and have user volumes attached. Make sure the correct package files are on hand before proceeding.
If the guest pools are in a position to be shut down:

1. From the left-hand navigation menu, click on Guest Pools. This displays the current inventory of Guest Pools.
2. Delete each Guest Pool from the inventory.
3. Navigate to the Administration Settings. Under **Software Firmware**, click on the **Upload Software** button and upload the `.pkg` patch file. Click on **Stage** to stage the package for deployment. Once the package is staged, click on **Deploy** to deploy the package. The staging and deployment process may take a few moments to complete.
4. When package deployment completes, Fabric typically restarts Hive Services automatically and runs the new deployment. If that does not occur, however, then click on **Restart Hive Services** to restart Fabric.
5. Access the Templates page. Any templates that are being applied to Guest Pools must be authored to enable VSS.
6. After enabling VSS, return to the Guest Pools inventory. Create new Guest Pools using the updated Template.

If guest pools cannot be shut down:

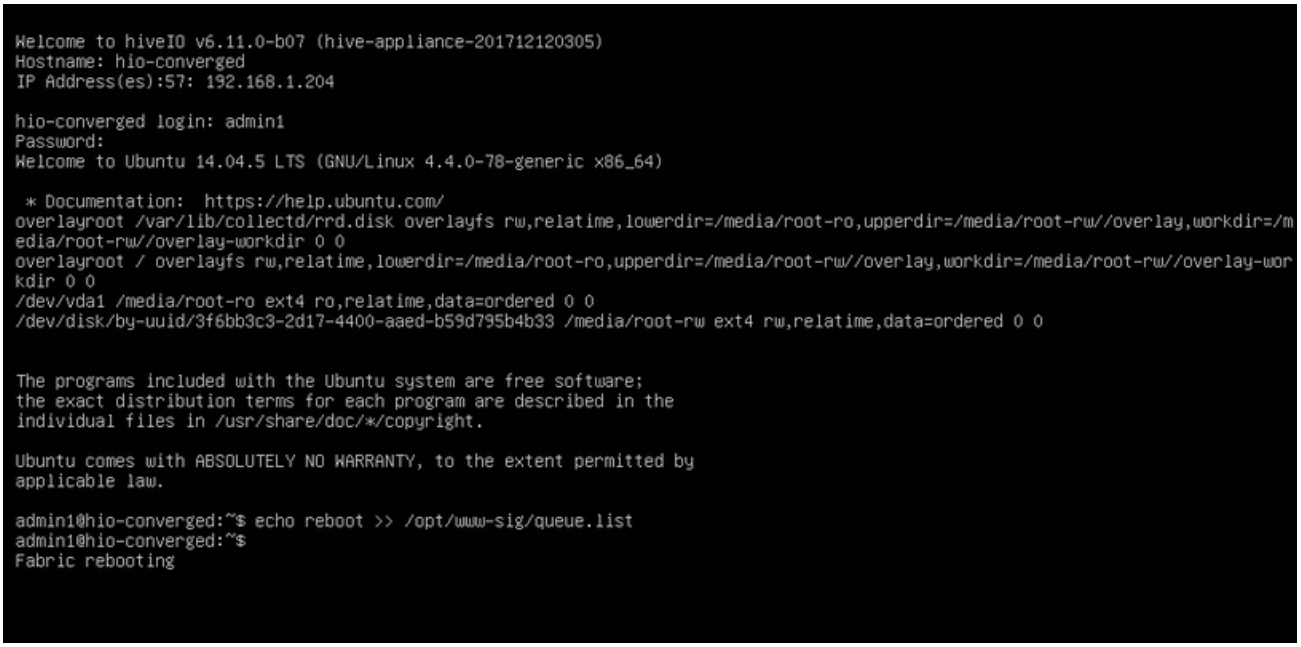
1. From the left-hand navigation menu, click on Guest Pools. This displays the current inventory of Guest Pools.
2. For each Guest Pool, set the **Available Guests** to `0`.
3. For each applicable Guest Pool, the GUID for user volumes must be deleted.
4. Access the Templates page. Any templates that are being applied to Guest Pools must be authored to inject a VSS registry.
5. Navigate to the Administration Settings. Under **Software Firmware**, click on the **Upload Software** button and upload the `.pkg` patch file. Click on **Stage** to stage the package for deployment. Once the package is staged, click on **Deploy** to deploy the package. The staging and deployment process may take a few moments to complete.
6. When package deployment completes, Fabric typically restarts Hive Services automatically and runs the new deployment. If that does not occur, however, then click on **Restart Hive Services** to restart Fabric.
7. Return to the Gu est Pools inventory and restore the size of available guests in the Guest Pool.

Upgrading 6.11.0 to 6.12.0

Hive Fabric version 6.12 introduces many new features and supported improvements. Upgrading from 6.11 is a streamlined process without the need to perform a complete re-install of Hive Fabric.

To perform the upgrade process from 6.11.0 to 6.12.0:

1. Click on **Administration** on the left Navigation Bar.
2. If appliance is a member of a cluster, have the appliance **Enter Maintenance Mode**. Migrates all guests off of the appliance before continuing.
3. Under the **Software Firmware** section, click on the **Upload Software** button. Browse for the appropriate 6.12 `.pkg` file.
4. When the package file successfully uploads, click on the **Stage** button to prepare the package for deployment. Once staged, click on the **Deploy** button and confirm the operation to install the update.
5. During the deployment process, the appliance will be in a **`System Unreachable`** state. To complete the upgrade process, access the appliance's server console. Login with the `admin1` account, and run the command: `echo reboot >> /opt/www-sig/queue.list`



6. When the command has been entered the server will display a “Fabric rebooting” message. When the appliance restarts, 6.12.0 has successfully installed.

> **Known Issue**
> If the appliance fails to reboot following the above operation, please use the server’s remote management to reboot the appliance.

7. The server console will now display the 6.12.0's new appliance console application.

Requirements, Dependencies and Sizing

Supported Hardware

Hive Fabric is a bare metal install and, as a result, has certain requirements. It has a broad range of hardware support, supporting most x86 hardware. Currently Hive Fabric mirrors the Ubuntu 14.04 hardware certification. Hive Fabric is capable of running on other hardware. However, this is only supported on a best-effort basis.

Sizing Hive Fabric

The key components to consider for Hive Fabric are CPU, Memory, Storage and Network. The hardware requirements will vary based on the number of guests intended to be served and their own resource requirements.

The following hardware specs are for illustrative purposes only and can be used to size an initial PoC or Pilot. Sizing per server based on a Guest VM with 4GB RAM:

Option	Hardware Specifications	Guests Served
Small	16 core/dual socket 128GB RAM 2 x 256G local disk 1 Gb Ethernet	up to 30
Medium	24 core/dual socket 384 GB RAM 2 x 256GB local disk 1 Gb Ethernet (shared storage or high throughput may require aggregated links or 10GB)	up to 100
Large	40 core/dual socket 1 TB RAM 2 x 512GB local disk 1 Gb Ethernet (shared storage or high throughput may require aggregated links or 10GB)	up to 225

The medium size spec depicts the typical server specifications for a Hive Fabric appliance in production.

Production Requirements

- The minimum number of appliances in a cluster is two. The recommendation for production is three. This provides further resilience and always provides a quorum to handle a "split-brain" scenario. For more information on cluster management, review the Cluster Adminsitration process.

Glossary

This guide uses a series of terminology to describe certain actions and events that are consistent throughout the use of the Hive Fabric. The following terms are referenced throughout the guide:

- **Authoring**: The act of modifying and configuring a Guest Template so that it is ready for deployment.
- **Compression**: Reducing the number of bits needed to store or transmit data.
- **Console**: A user interface that provides a direct view of the VM as if the administrator were sat in front of a screen directly attached to the guest. This is where administrators will be able to modify a template's guest OS.
- **Deduplication**: A data reduction technique for eliminating duplicate copies of repeating blocks of data.
- **D**isaster **R**ecovery, or **DR**, refers to the event that a physical location is suddenly unavailable. Taking the resources that were provisioned in that location offline. The remediation of this event can also fall under the same generalization and allows for typically temporary resource to be made available in a new or secondary location allowing users access their guest.
- **H**igh **A**vailability, or **HA**, refers to the availability of resources in the wake of component failure such as a server within a Hive Fabric Cluster. Typically other servers in the cluster will have sufficient spare resource to pick up the load imposed on the cluster in the event of failure.
- **Non-Persistent Guest**: Typically none of the changes to a guest are saved upon logout or reboot of the guest. At the end of a session, the desktop gets destroyed and the user receives a fresh image the next time they log in. If User Volumes are enabled, it will track and save the basic user's settings, such a Printers, Bookmarks, Internet Explorer, History, Map Drives.
- **Persistent Guest**: Each guest runs in its own right. Any changes to the desktop persist across a reboot or logout of the user. These types of desktops allow for more personalization, but they require more storage and backup.

Introduction

Hive Fabric is a cloud compute platform that delivers end-to-end functionality for the private and hybrid cloud. The product can integrate seamlessly into any existing private cloud stack.

Some of the private cloud components supported by HiveIO are:

- Storage Acceleration
- Guest Brokering
- Basic User Profiles
- Orchestration API
- Hypervisor Functions
- Inventory Reporting
- Host and Guest KPIs
- Persistent Guests
- Non-Persistent Guets
- High Availability and Disaster Recovery
- Basic Profile Management

The service provides increased cost benefits and efficiencies to the private cloud stack, which improves an organization's overall ROI.

Appliance Installation

Once an image has been acquired from the HiveIO website through a team member, there are multiple methods supported for installing Hive Fabric to a server. The most common method is done though the use of the Intelligent Platform Management Interface (IPMI). Users with physical access to the server may also choose to create a bootable USB installer to plug in. Users with advanced Linux knowledge may also opt to perform a PXE Install on their server.

Once the installation of Hive Fabric has been completed, the First Boot Wizard will run and prepare the appliance for deployment.

USB Drive

Hive supports multiple ways of installing the system. These steps cover installation via USB drive.

Requirements for USB Installation

There are several methods of turning a blank USB drive into a bootable drive for the server. Any method is acceptable but it is recommended to use *Universal USB Installer*, a free and effective bootable drive creator available for Windows. Other tools are available for Mac and Linux. These instructions are written under the assumption that *Universal USB Installer* is in use. For other bootable USB creators, consult the appropriate documentation.

Users who wish to install via USB drive will need the following:

- Blank USB Drive (5GB or greater)
- HiveIO Fabric ISO file
- Server capable of running HiveIO Fabric

Instructions for Creating a Bootable USB Drive on Windows

1. Insert a blank USB drive into the workstation that contains the latest Hive Fabric ISO file.
2. Open *Universal USB Installer*.
3. For Step 1, selecting a Distribution, select the appropriate distribution method from the drop down menu. This will unlock Step 2's option to browse for the ISO file.
4. Once Step 2 is unlocked, locate the latest Hive Fabric ISO file. This unlocks Step 3's selection of the correct drive.
5. Once Step 3 is unlocked, select the drive that corresponds to the blank USB drive. Verify that the Drive selected is the correct drive before proceeding.
6. Click `Create` and allow *Universal USB Installer* to build the bootable USB drive.
7. Once the boot from the USB begins, the HiveIO screen will display. Choose the `Install Appliance` option to begin installation.
8. Select the appropriate drive to install the Hive software on. This is the drive that was designated as the Boot Drive in the previous steps. Once selected, hit the **Enter** key to continue.
9. Several warnings will ask to confirm the selection. Once validated, the installation will begin.
10. When the installation completes, the server will automatically reboot. For some consoles, a series of options or a command prompt may appear instead. Select the `reboot` option or enter the `reboot` command to progress.
11. When the server reboots, the server will boot the disk image and begin the First Boot Wizard.

For information on how to create a bootable USB drive on Mac or Linux consult the appropriate product documentation.

Windows USB Installation

The following instructions are for creating a bootable USB drive for Hive Fabric installation on Windows workstations.

Instructions for Creating a Bootable USB Drive on Windows

1. Insert a blank USB drive into the workstation that contains the latest Hive Fabric ISO file.
2. Open *Universal USB Installer*.
3. For Step 1, selecting a Distribution, select the appropriate distribution method from the drop down menu. This will unlock Step 2's option to browse for the ISO file.
4. Once Step 2 is unlocked, locate the latest Hive Fabric ISO file. This unlocks Step 3's selection of the correct drive.
5. Once Step 3 is unlocked, select the drive that corresponds to the blank USB drive. Verify that the Drive selected is the correct drive before proceeding.
6. Click `Create` and allow *Universal USB Installer* to build the bootable USB drive.

Intelligent Platform Management Interface (IPMI)

Hive supports multiple ways of installing the system. These steps cover installation via IPMI.

Requirements for IPMI Installation

Access to the IPMI of the server is required. Various web interfaces are available and are dependent on hardware. For assistance with gaining access to the IPMI, consult the hardware manual.

Users who wish to install via IPMI will need the following:

- Hive Fabric installation ISO file
- Server capable of running HiveIO Fabric
- Access to the IPMI of that server

The instructions given here cover some of the common management platforms used to install the Hive software to a server. Steps may vary based on the platform and version used. For unlisted platforms, consult the IPMI's documentation for specified instructions on installing the ISO file.

> Many of these platforms require that the Java plug-in is installed on the workstation. Verify that Java is correctly installed before continuing with the system deployment.

- Cisco Integrated Management Controller
- Dell Remote Access Control
- HP Integrated Lights-Out
- Lenovo Integrated Management Module
- Supermicro Intelligent Management

Instructions for Installing the Hive Fabric Software

1. Once the boot from the CD/DVD Drive begins, the HiveIO screen will display. Choose the `Install Appliance` option to begin installation.
2. Select the appropriate drive to install the Hive software on. This is the drive that was designated as the Boot Drive in the previous steps. Once selected, hit the **Enter** key to continue.
3. Several warnings will ask to confirm the selection. Once validated, the installation will begin.
4. When the installation completes, the server will automatically reboot. For some consoles, a series of options or a command prompt may appear instead. Select the `reboot` option or enter the `reboot` command to progress.
5. When the server reboots, the server will boot the disk image and begin the First Boot Wizard.

> If installation was done through the Cisco Integrated Management Controller, the **Activate Virtual Devices** option may need to be disabled again once the installation process has completed.

Dell Remote Access Control

The following steps are for installing through the iDRAC platform. Be aware that instructions may vary based on the version used.

1. Mount the latest HiveIO ISO to the workstation as a virtual drive.
2. Access the web interface for the IPMI and sign in.
3. Click on **Console/Media** tab and select the **Virtual Consoles and Virtual Media** option. Click on the **Launch Virtual Console** button. Leave the console open for now.
4. While remaining on the **Console/Media** page, select the **Configuration** option. Under **Virtual Media**, open the **Status** tab and select **Attach**. Press **Apply** to advance.
5. Click on **Virtual Media**. Select the **Launch Virtual Media** option. Click on the **Add Image...** button and select the mounted HiveIO ISO file. Enable the **Mapped** checkbox next to the image.
6. After loading the ISO file, power on the system. At the server's POST screen, press F11 to access the boot menu. This may take a few moments to load.
7. When the menu is present, select the appropriate virtual CD/DVD Drive. The drive may vary based on server hardware and drivers.
8. The server will boot from the CD/DVD Drive and load the HiveIO startup software.

Lenovo Integrated Management Module

The following steps are for installing through the Lenovo IMM platform. Be aware that instructions may vary based on the version used.

1. Access the web interface for the IPMI and sign in. If necessary, disable the timeout value to prevent the session from timing out before deployment completes.
2. From the task menu, click on **Remote Control** and select the **Start Remote Control** option.
3. Access the **Virtual Media Sessions** window. From the Client View list, select **Add image...** as the deployment option.
4. When prompted to browse for a file, locate the latest HiveIO installation ISO file. The *Read Only* option will need to be enabled for this process.
5. After loading the ISO file, reboot the system. The Lenovo platform will detect the deployment method and boot appropriately.
6. Follow the on-screen prompts to load the HiveIO startup software.

Supermicro Intelligent Management

The following steps are for installing through the Supermicro Intelligent Management platform. Be aware that instructions may vary based on the version used.

1. Access the web interface for the IPMI and sign in.
2. Click on **Remote Control** tab and select the **Console Redirection** option. Click on **Launch Console**.
3. Click on **Virtual Media** and select the **Virtual Storage** option. After a brief moment, the **Virtual Storage** wi ndow will launch. Access the **CDROM&ISO** tab.From the **Logical Drive Type** dropdown menu, select **ISO File**.
4. When prompted to browse for a file, locate the latest HiveIO installation ISO file. Click **Plug In** to mount the image.
5. After loading the ISO file, reboot on the system. At the server's POST screen, press `F11` to access the boot menu. This may take a few moments to load.
6. When the menu is present, select the appropriate CD/DVD Drive. The drive may vary based on server hardware and drivers.
7. The server will boot from the CD/DVD Drive and load the HiveIO startup software.

HP Integrated Lights-Out

The following steps are for installing through the HP iLO platform. Be aware that instructions may vary based on the version used.

1. Access the web interface for the IPMI and sign in.
2. From the **Remote Console** option on the left side navigation menu, open a console for the server.
3. Click on **Virtual Drives** or a similar options and access the virtual CD/DVD drive option. Do not close the console yet.
4. Once prompted for a file, choose the latest HiveIO installation ISO file.
5. After loading the ISO file, the boot order needs to be selected. Click on the **Virtual Media** option on the left side navigation menu to reveal the **Boot Order** option.
6. Under **One-Time Boot Status**, select **CD/DVD Drive**. Click on **Apply** to save the change.
7. Once the boot drive has been applied, click on the **Server Reset** button below to restart the server.
8. Once the reboot has finished, the server will boot from the CD/DVD Drive and load the HiveIO startup software.

Cisco Integrated Management Controller

The following steps are for installing through the Cisco IMC platform. Be aware that instructions may vary based on the version used.

1. Access the web interface for the IPMI and sign in.
2. Click on the **Launch KVM Console** option.
3. Click on **Virtual Media** and select the **Activate Virtual Devices** option. After a brief moment, the **Virtual Media** menu will display a few new options. Select the **Map CD/DVD...** option.
4. When prompted to browse for a file, locate the latest HiveIO installation ISO file.
5. After loading the ISO file, power on the system. At the server's POST screen, press F6 to access the boot menu. This may take a few moments to load.
6. When the menu is present, select the appropriate CD/DVD Drive. The drive may vary based on server hardware and drivers.
7. The server will boot from the CD/DVD Drive and load the HiveIO startup software.

PXE Installation

Requirements

Install and configure PXE on the server that is intended to be used as the install server. This guide uses PXEInstallServer on an Ubuntu server. For instructions on installing and configuring PXE, consult the following: https://help.ubuntu.com/community/PXEInstallServer.

Additionally, a fairly advanced working knowledge of Linux and networking in general is recommended for using this solution.

Users who wish to install via PXE will need the following:

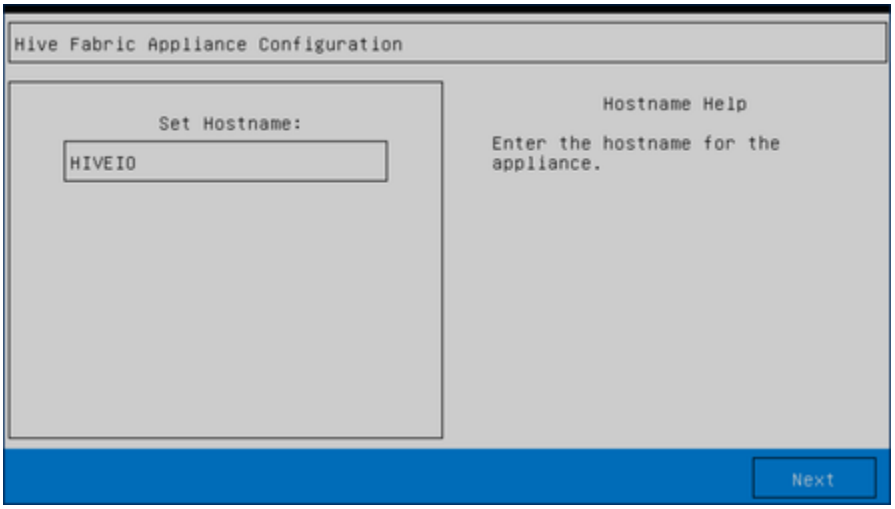
- Hive Fabric ISO image
- Server capable of running Hive Fabric
- Access to an appropriately configured PXE Server on the same network

Loading the ISO File onto the PXE Install Server

1. Complete the installation and configuration so that the PXE server is available to the HiveIO Fabric server.
2. There will be a repository for installation ISO files. Copy the Hive Fabric ISO files into the repository. Doing so will make the files available to the server booting from the network.
3. When starting the server that Hive Fabric is intended to be installed on, select `boot from network`.
4. After loading the appropriate data over the network, the HiveIO installation screen will appear. Choose the `Install Appliance` option to begin installation.
5. Select the appropriate boot drive to install the Hive software on. Once selected, hit the **Enter** key to continue.
6. Several warnings will ask to confirm the selection. Once validated, the installation will begin.
7. When the installation completes, the server will automatically reboot. For some consoles, a series of options or a command prompt may appear instead. Select the `reboot` option or enter the `reboot` command to progress.
8. When the server reboots, the server will boot the disk image and begin the First Boot Wizard.

First Boot Wizard

When the Hive Fabric boots up for the first time, the first boot wizard needs to be used for the initial setup process. This wizard helps to configure a variety of initial settings during the installation and setup of Hive Fabric. Users are advised to become familiar with these settings to best implement the first boot wizard.



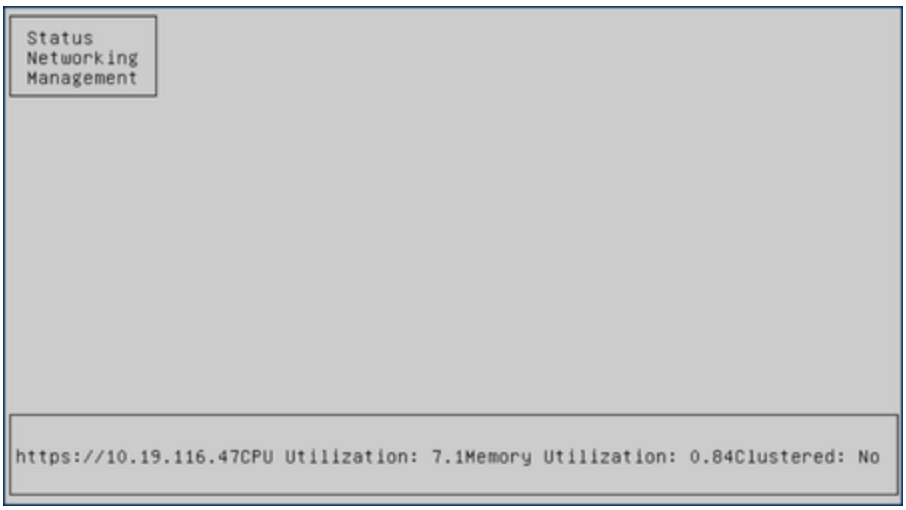
When the Hive image completes installation the first boot wizard will appear. To begin navigating the first boot wizard:

1. On the **Hostname Setup** page, enter the unique hostname for the local appliance, typically entered as `local.yourdomain.com`. Press **Enter** to advance to the next page.
2. The **Admin Password Setup** page is where a new password will be established for the default "admin" Administrator account. Enter a secure new password in the appropriate field, then re-enter the password in the following confirmation field. Use the arrow keys to select the **Next** button and press **Enter** to advance to the next page.

   > **Admin Passwords**
   > This only sets the local `admin` account password for accessing the WebUI with administrative privileges. The `admin1` account, a separate administrator account for navigating the Fabric console, must have its password changed through the shell instead.

3. Enter the HiveIO Fabric network settings in the **Configure Network Settings** page. The following options must be set:
   - **Enable DHCP:** When enabled, an IP address is automatically assigned to the device. Disabling this option will allow entry of an IP Address, Netmask, and Gateway.
     - **IP Address:** Enter the IP Address to assign to this device. Verify that this IP Address is not currently in use before assignment.
     - **Netmask:** Enter the netmask for the network's host.
     - **Gateway:** Enter the default gateway for the network.
   - **VLAN:** Enter the VLAN ID. if the device will be joining one. Otherwise, this can be left at the default value.
   - **DNS Server:** Enter the DNS server address. For common setups, this will be the same as the hostname.
   - **DNS Search Path:** Enter the DNS search path. This will typically resemble `yourdomain.com`.
4. Once the Hive services have been configured, the following pages are optional to complete. The **Join Cluster Setup** enables the Hive Fabric to gain membership to a database cluster. If a cluster has already been established, enter the IP address of the Central Management Appliance. Otherwise, this step can be performed at a later time. Use the arrow keys to select the **Next** button and press **Enter** to advance and complete the First Boot Wizard.

Once the First Boot Wizard has been completed, a status page will appear. A console menu is available to navigate with three options:



- Status
- Networking
- Management

The status page also displays the server's IP address, CPU Utilization, Memory Utilization, and Clustered status. Enter the assigned IP address into a web browser to begin using the appliance.

Initial Deployment

With installation process completed and the First Boot Wizard run, Hive Fabric is ready for deployment. Hive Fabric is accessible through any HTML5-compliant web browser. Further configurations that could not be performed within the First Boot Wizard are available within the appliance's Web user interface.

Instructions for Deploying the Hive Fabric Software

1. Ensure the appropriate media is connected to the server. Turn it on and boot from the connected boot device.
2. When starting up, the GNU GRUB screen may appear with a series of options. Select the `Ubuntu` option to advance. Otherwise, the system will simply start without any further prompting.
3. Hive will indicate a successful install when the screen displays the Console Application. The bottom of the menu page displays the IP address of the host appliance.
4. Using the IP obtained on the console after installation, open a web browser and insert the IP in the format off `https://<hiveIO-Host-IP>`.

   > **Note**
   > There may be a warning for the SSL connection. This can be safely ignored as this is a self-signed certificate. It can be replaced later to the correct certificate for the environment.

5. The following is the default Administrator ID:
   - User: admin
   - Password: This varies based on the password entered during the First Boot Wizard

6. When the login is successful, configuration may begin.

Appliance Administration

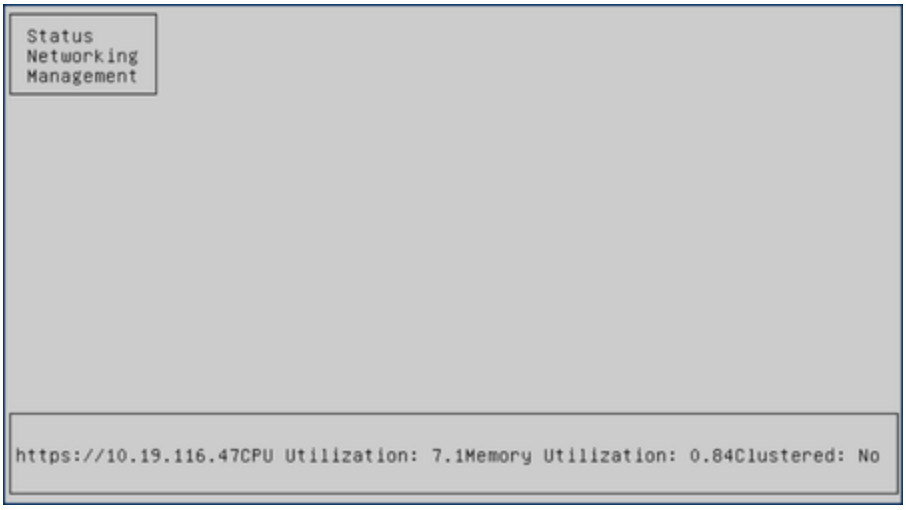
When the appliance has been deployed, it is ready for use. To begin access and prepare configurations to guests, review the process of navigating the user interface.

There are several sections used when navigating the appliance interface. Each one is integral to the configuration and maintenance of both guests and the appliance itself:

- Inventory
- Publishing
- Tools
- Settings

Console Management

An individual Hive Fabric Appliance can be managed locall through the console. This is not intended to be the primary point of management for Hive Fabric but does allow for configuration of certain operations from the console of the Appliance for example when a machine isn't available to run the Web UI. The Manu will show when not in use and is ready for user-interaction. All commands in this tool are available through the Web GUI.



There are three main areas to this tool:

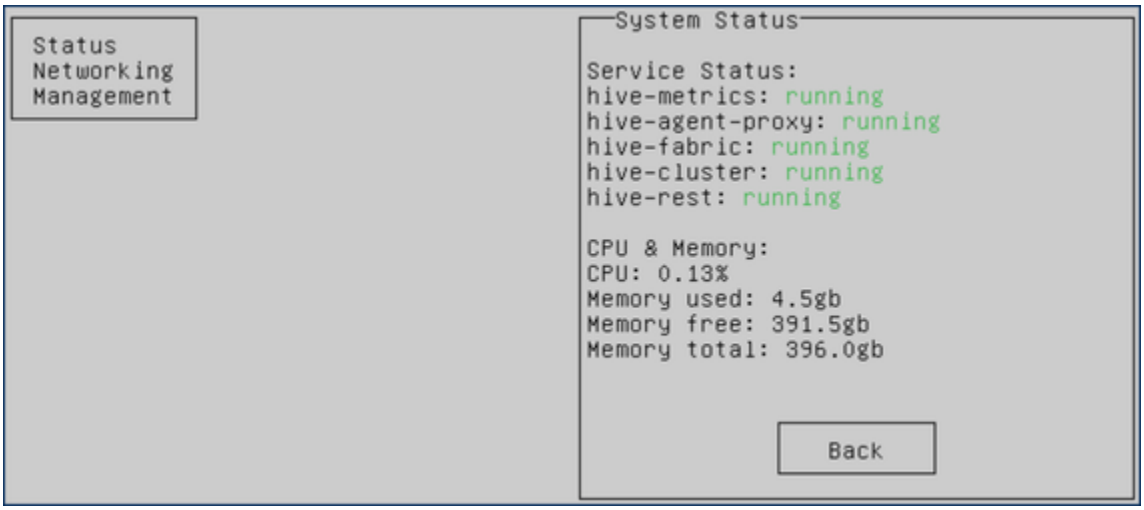
Status: This displays the status of the Hive Fabric services and the appliance in general.

Networking: See the current configuration and update any of the production network settings . Particulaly useful if you have lost remove connectivity to the appliance and need to correct a network setting.

Management: Manage the appliance such as Cluster membership, maintenance mode and power operations on the appliance itself.

Status

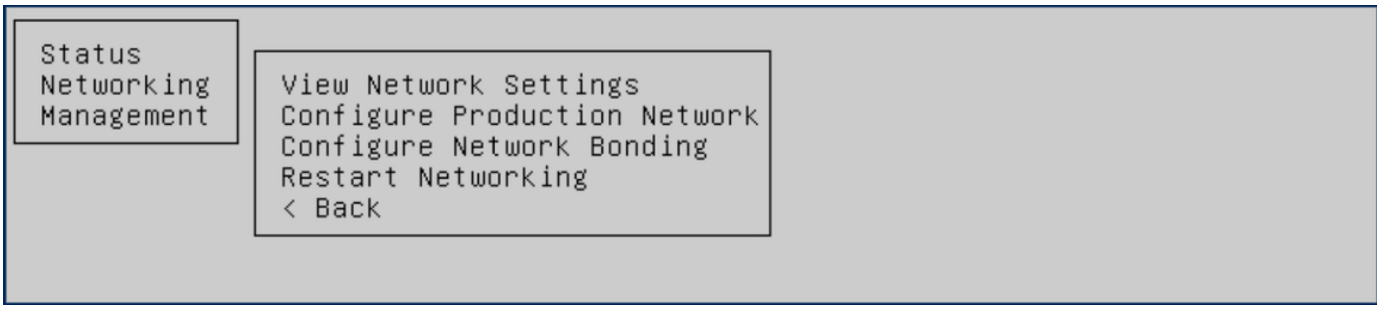
The **Status** menu displays the current health of the server and the Hive services. A Service Status list displays the current Hive services and their running state. A `running` status indicates that the service is running without issues.



CPU and Memory stats are displayed beneath the Service Status. These display the current metrics of the system. Here, the CPU usage can be monitored, as well as the current memory statistics.

Networking

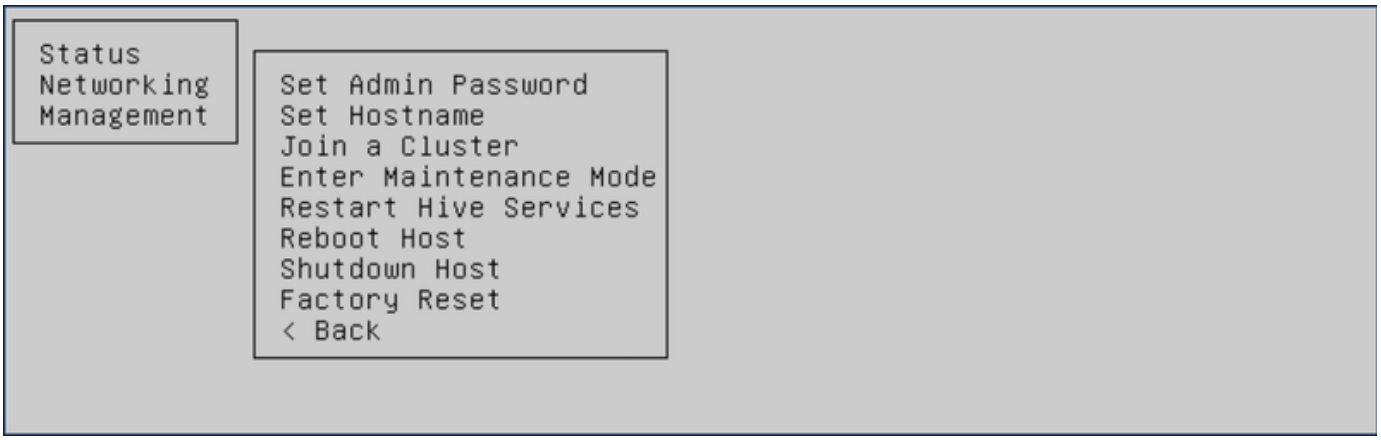
The **Networking** menu lets users reconfigure or even reset network configurations. Many of these options may also be set within the appliance's web interface.



- **View Network Settings** display the current network configuration for the Hive Fabric. The appliance's IP address, Subnet Mask, Default Gateway, and Network Interface are displayed here.
- **Configure Production Network** allows users to change the network interface configurations that were set during the initial run of the First Boot Wizard. DHCP and VLAN can both be enabled or disabled from this menu.
- **Configure Network Bonding** lets users set a Network Bond for the appliance.
- After any network settings has been edited, the applied changes must be saved via the **Restart Networking** option. A prompt will appear, confirming the server to proceed with the restart.

Management

The **Management** menu has a variety of options that are imperative to configuring and maintaining Hive Fabric. Many of these options may also be set within the appliance's web interface.



- **Set Admin Password** to enter a new Administrator password.
- **Set Hostname** sets a new hostname for the appliance.
- **Join a Cluster** joins the appliance to a cluster if it does not already have a membership. This option cannot be used to change cluster membership. The appliance must first detach itself from the cluster.
- **Enter/Exit Maintenance Mode** toggles the appliance to a maintenance state. It is necessary to enter Maintenance Mode in order to leave the host's cluster membership.

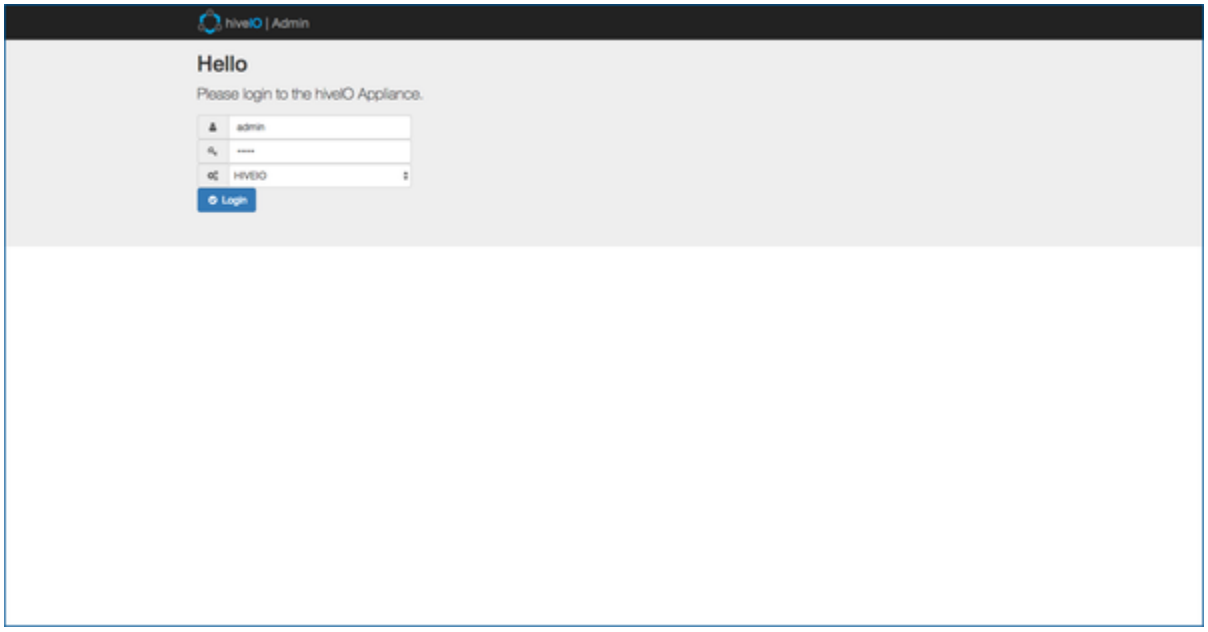
> **Clustering**
> This option only works while the appliance is a member of a cluster. Otherwise, an error will appear.

- **Restart Hive Services** restarts the Hive services after certain settings have been changed.
- **Reboot Host** restarts the host appliance. This action may be necessary to save applied settings or for troubleshooting purposes.
- **Shutdown Host** shuts down the host appliance.
- **Factory Reset** reboots the appliance to factory-default settings. Once this option is deployed, the First Boot Wizard must be run again.

> **Factory Resetting**
> Performing a Factory Reset will clear out all changes made to the server and restore the appliance to its initial settings. Any changes that were made to the server prior to factory resetting will be lost. This includes any software packages used to update Hive Fabric To perform a factory reset while retaining the latest version of Hive Fabric, perform a fresh install with the most current files.

Navigating the User Interface

The Hive Fabric user interface can be accessed by entering either the URL in the format of `https://<hive_fabric host IP>` or DNS name, if configured.



Default Credentials
The default credentials to login to the UI are:

Username: admin

Password: admin

A warning for the SSL connection may appear in the browser, a result of the self-signed certificate that is installed by default. This certificate can be replaced later with your own certificate. Refer to the Administration page for certificate configuration.

A series of options are available to the user on the left navigation bar once they login to administer the appliance. These options allow Users with the appropriate privileges to setup, configure and manage all aspects of Hive Fabric which consists of 6 main sections. Once configuration of each section is completed the appliance will be capable of hosting guests and securely brokering these to users. The configuration consists of:

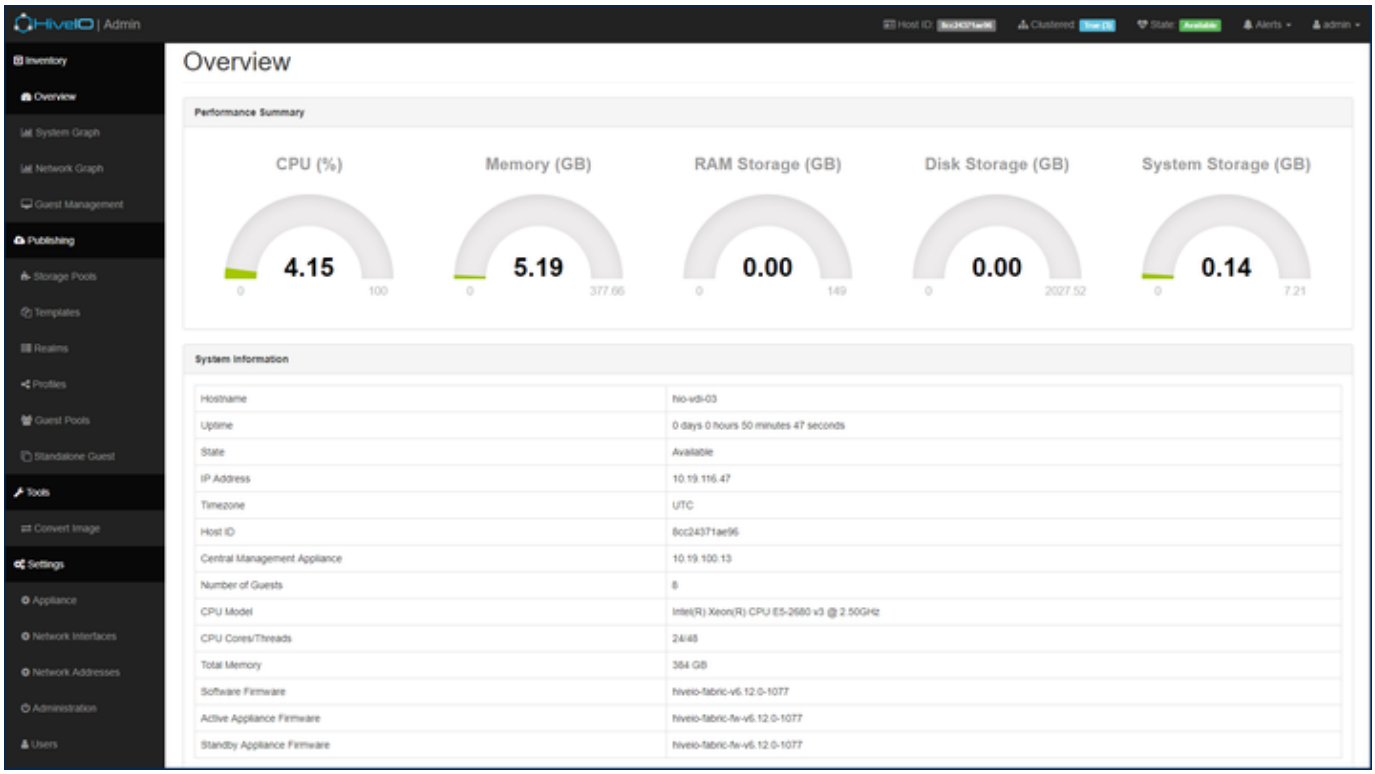
1. Appliance
2. Network Interfaces
3. Network Addresses
4. Templates
5. Realms
6. Guest Pools

Inventory

This section provides insight into the performance of the appliance and the management for Guests. The admin is able to view the basic health of the system including storage and networking for troubleshooting purposes. Administrators are able to monitor Guest Pools here, managing each individual guest.

Overview

This page provides key resource consumption metrics and detailed system information about the appliance.



Performance Summary

This panel provides a high level overview of the resource utilization across the appliance. The amount of CPU, memory and storage that is currently in use by the appliance is monitored and reported.

- CPU(%) : Display the %age of CPU resource currently in use across the appliance.
- Memory(GB): The memory installed in the appliance along with the current utilization. This is a summation of all system and guest utilization and includes RAM allocation to storage.
- RAM Storage (GB): The memory currently reserved for storage and the amount currently utilized.
- Disk Storage (GB): The available storage in the appliance and the amount currently being consumed by Guests.
- System Volume (GB): The storage reserved for the Hive Fabric OS. This should be monitored and should not be allowed to fill to 100%.

System Information

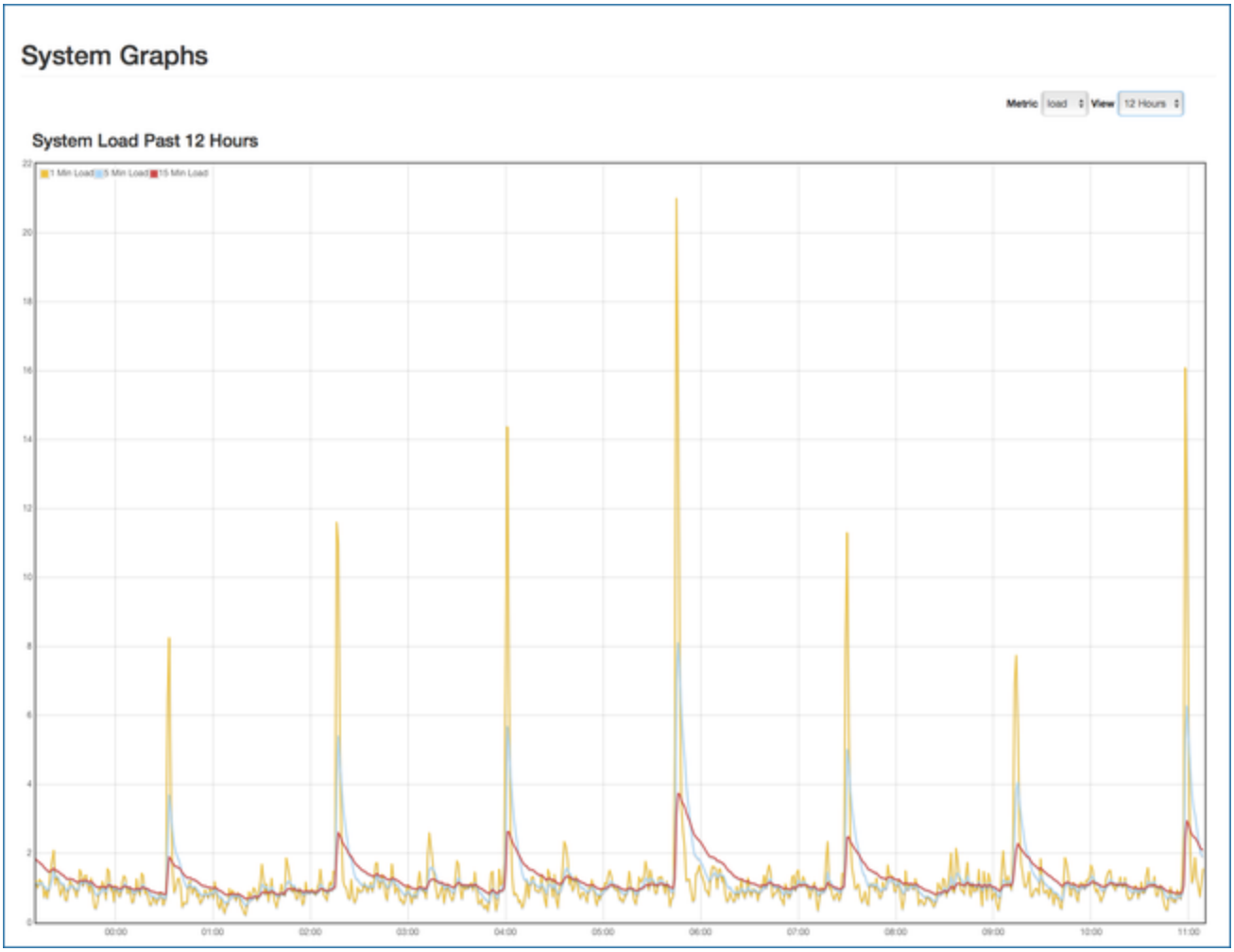
This page also displays key information about the appliance that may be useful for administration purposes. It also shows key information about the state of clustering, as well as the number of guests running hardware and software versions. Many of these settings are established during the First Boot Wizard and can be adjusted in the Appliance Settings page.

- **Hostname**: The current hostname of the appliance.
- **Uptime**: The amount of time that the appliance has been booted up and running.
- **State**: The current status of the appliance in the cluster.
- **IP Address**: The IP address of the appliance.
- **Timezone**: The timezone of the appliance.
- **Host ID**: The unique identifier assigned to the host. This is system generated and can't be changed by the admin.
- **Central Management Appliance**: The IP of the current Central Management Appliance in the cluster; The CMA is the appliance in the cluster responsible for join and union orchestration. If a cluster isn't configured this will be set to `localhost`.
- **Number of Guests**: The current number of active Guests on this appliance.

- **CPU Model**: The processor model and clock speed that the server is running on.
- **CPU Cores/Threads**: The total number of cores that the appliance has available to use across all CPUs. Threads will usually differ if hyper-threading is turned on in the BIOS and will usually be double the number of Cores.
- **Total Memory**: The total amount of memory available to the appliance.
- **Software Firmware**: The current version of the Hive Fabric firmware that is running.
- **Active Appliance Firmware**: The version of the active Hive Fabric firmware.
- **Standby Appliance Firmware**: The version of the standby Hive Fabric firmware.

Firmware
The appliance has active and standby firmware to allow for easy application of updates. In this architecture if an update adversely affects the appliance then it can be rolled out and replaced by the standby version.

System Graphs

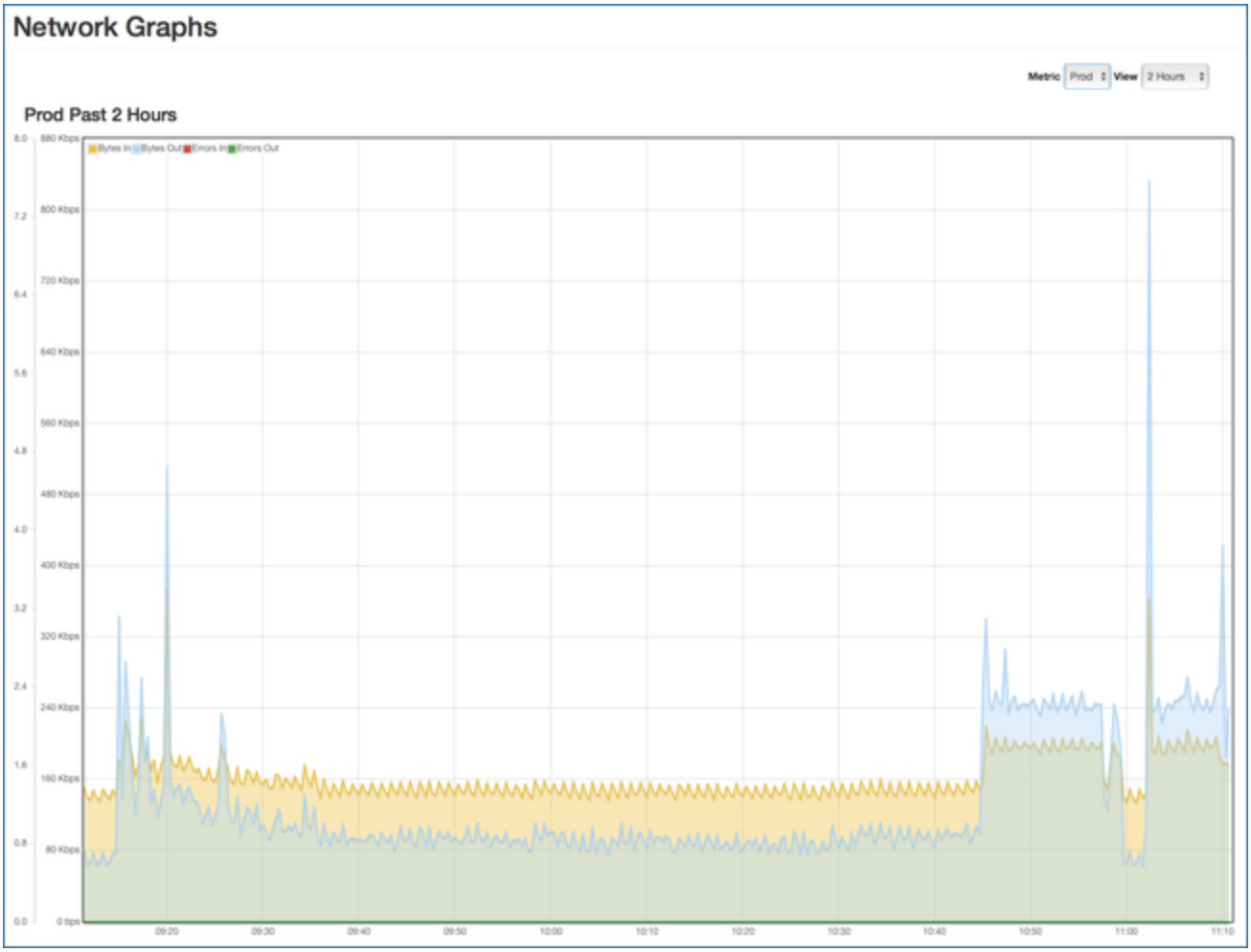


The health of the appliance can be monitored from this page. The System Graphs display graphs for various metrics within the appliance and can assist troubleshooting. The following metrics can be viewed:

- CPU
- System load
- System memory

The View dropdown menu can be used to select a specific period to review metrics for. The appliance tracks data occurring within the last 1 hour, 2 hours, 6 hours, 12 hours, 1 day, 1 week, or 1 month.

Network Graphs

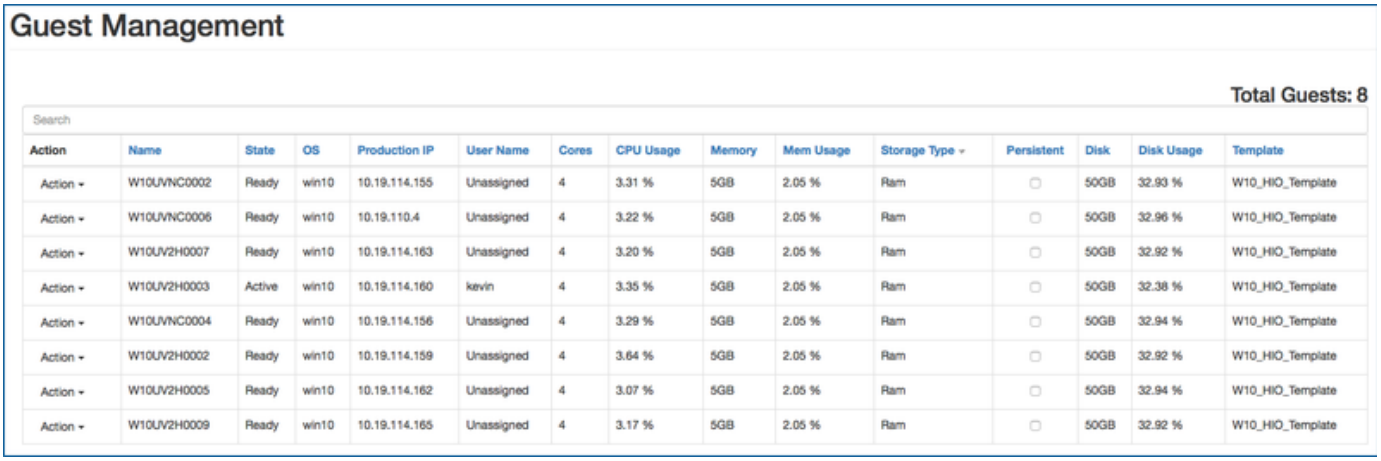


The network utilization across each physical network can be monitored from this page. The Network Graphs displays graphs for the following metrics:

- Bytes In
- Bytes Out
- Errors In
- Errors Out

The Metrics dropdown will allow users to view the health of any configured physical interface as well as the additional prod network that is automatically created for the management of the appliance. The View dropdown menu can be used to select a specific period to review metrics for. The appliance tracks data occurring within the last 1 hour, 2 hours, 6 hours, 12 hours, 1 day, 1 week, or 1 month.

Guest Management



This page displays the guests that are deployed on this appliance and allows the administrator to manage them. The guest table can be sorted by any of the columns, the default is Name. Users with administrative privileges have access to a series of actions that can be performed on the Guest.

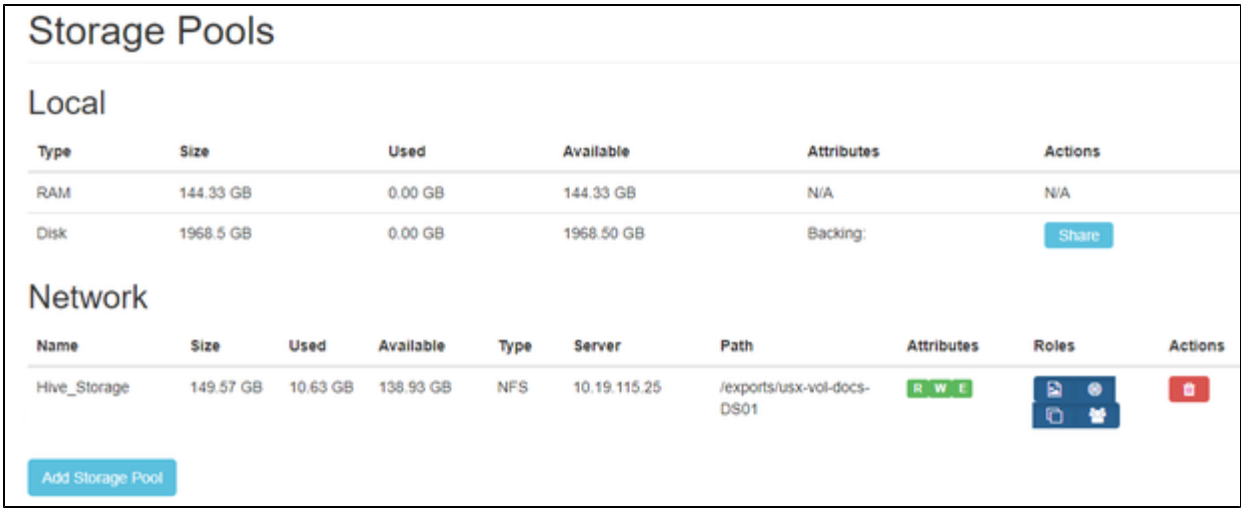
Below are the available actions that can be performed on the guest VM, accessible through the Action dropdown to the left of a guest entry in the table:

- **Power On**: Power on the Guest.
- **Shutdown**: Attempt to cleanly shutdown the Guest.
- **Reboot**: Reboot the Guest.
- **Power Off**: Force shutdown the Guest.
- **Reset**: Hard reset the Guest, equivalent to momentarily pressing the power button on a physical system.
- **Migrate**: Move this Guest to a different host in the cluster, when this option is selected a dialog box will appear giving a list of servers that are capable of running the selected guest.
- **Open Console**: Opens a console to the Guest, typically used for troubleshooting.

Publishing

These options focus on publishing options. Administrators can configure all the tools needed to run the guest pools for all users.

Storage Pools



Storage Pools are used throughout Hive Fabric for the setup and maintenance of virtual machines. The server's local storage, RAM storage, and any additional shared storage pools will be displayed here. Adding a Storage Pool to the appliance is the first step to creating or adding templates and Guest Pools. To add the appropriate files to the Storage Pool, follow the steps to Uploading files to a Storage Pool.

1. Click on **Storage Pools** on the left side Navigation Bar.
2. Click on the **Add Storage Pool** button and fill in the required field:

   - **Name**: The unique name used to identify the storage pool.
   - **Type**: The type of storage that will be used for the Storage Pool, supported systems are **NFS**, **CIFS**, and **Ceph (RBD)**.

     > **Known Issues**
     > There is a known issue where CIFS shares will be restricted to read-only permissions, regardless of permissions set on the system itself.

   - **Server**: Provide the server IP or FQDN of the external storage server.
   - **Path**: Enter the path of the export or share that will be mounted and used for the Storage Pool.
   - **Roles**: By default, a storage pool can fulfill a multiple of intended storage rolls. Selecting one of these options will disable that store's role within the appliance. That storage pool cannot be used for that purpose unless it is re-enabled. Storage roles can be adjusted at any time by clicking on the designated icon within the storage pool inventory. The available storage roles are:
     - **Template Storage**
     - **ISO Storage**
     - **Guest Storage**
     - **User Volume Storage**
3. Click **Add Storage Pool** to complete the process. If everything is correct, the storage pool will be added to the inventory. The appliance will display a list of *Attributes* that are applicable to the storage pool: **R**ead, **W**rite, and **E**xecute.

> A storage pool with read-only permissions will not have access to template creation and authoring. If

there are any issues regarding storage attributes, verify that the server permissions are set correctly.

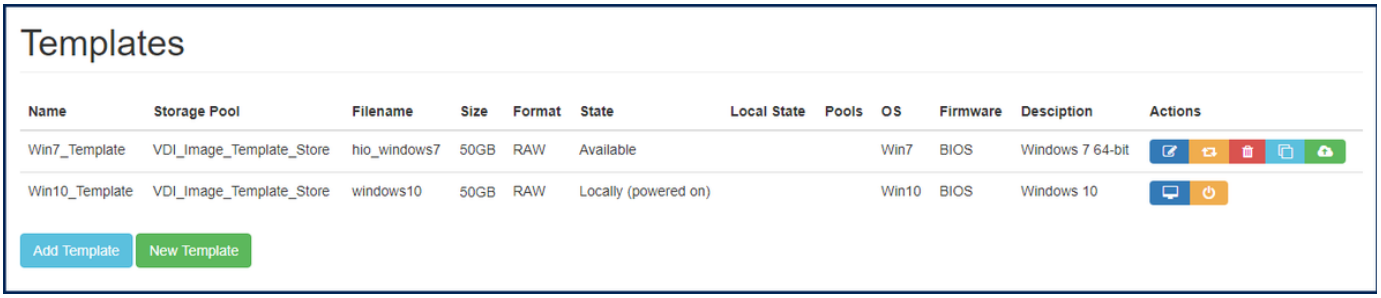
NFS Permissions
Server Administrators using an NFS share must consider the current user permissions of the server. The Storage Pool requires both the `root` user and the `libvert-qemu` user to have read and execute access. Aside from *Read-Write-Execute* permissions, the following settings must also be enabled for the NFS share: `insecure`, `no_subtree_check`, and `no_root_squash`.

If a local storage disk is available, administrators have the option to share the disk. This makes the local disk available to share as a storage pool. Click on the **Share** button next to the storage disk, located under **Actions**. A share link will be provided. To stop sharing, remove the share from the storage pool inventory first. Once the share disk is no longer active, click on the **Stop Sharing** button. The appliance will ask for confirmation before stopping the share.

Shared Local Storage
Local storage should not be shared and used in production. If the server fails then any appliance using this storage will be affected by the outage.

Uploading files to a Storage Pool

Templates



Templates are the foundation for deploying pools of virtual machines. A template is used to define the operating system, application set, and default settings that a virtual machine will initially build with, before being used to create a Guest Pool. Templates can be created from scratch through the Create a new Template wizard. Existing templates can be added to the cluster through the Add an existing Template process.

There is a balance between the number of templates that are created and the level of customization a template receives. Consider the ongoing template management and ensuring that users get all the applications they need to do their day to day job. The more generic a template is, the more guest pools can use the same template. However, this can complicate application delivery through the use of application virtualization to layer the applications a user requires into the guest.

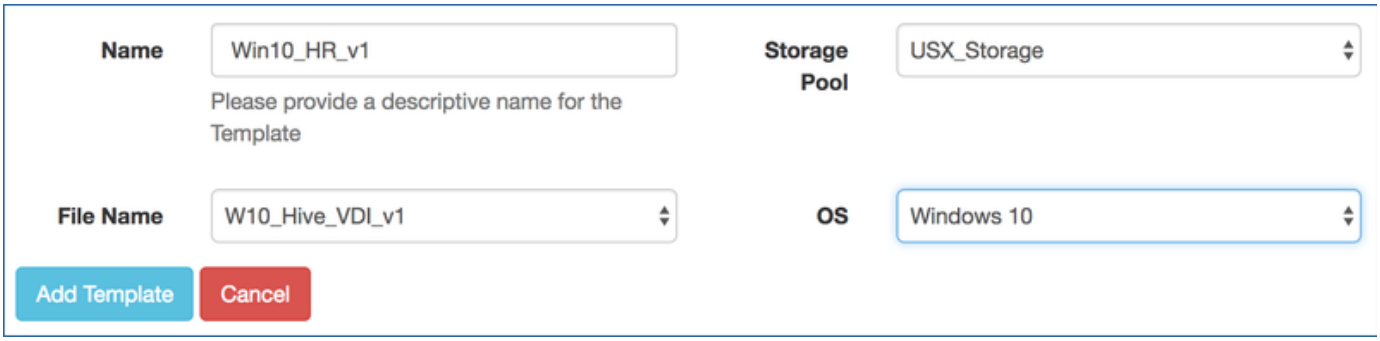
Consider
If a large number of templates are being managed for a small user group a persistent desktop maybe a better solution to deliver VDI to end-users.

This section guides through a number of key steps regarding templates:

Add an existing Template to the cluster in preparation for deploying a Guest Pool.
Create a New Template in preparation for deploying a Guest Pool.Authoring a Template
Template Management. Once a template has been created, it's life cycle is managed through a number of actions:

- plicate a Template
- Staging a Template
- Removing a Template
- Prepare a template with the Template Console
- Validate a Template for Guest Pool deployment
- Unload a Template

Add an existing Template



Hive Fabric can make use of an existing template. This template could have been previously utilized by Hive Fabric, copied over from another cluster, or been used with another virtualization platform. Hive Fabric is capable of using any QEMU/KVM-supported disk emulation, but the preferred emulation is either RAW or QCOW2. If an image has not been previously converted the Hive Fabric will convert the file upon upload, but it is faster and more ideal to perform the conversion beforehand. Supported disk images include:

- `raw`
- `qcow2` (KVM, Xen)
- `vmdk` (VMware)
- `vpc` (Hyper-V)
- `vhdx` (Hyper-V)
- `vdi` (Virtual Box)

> The system will automatically convert the template to RAW when the template is staged, if the template is stored on NFS shared storage RAW is the recommended format.

This template should have any 3rd party hypervisor agents (such as VMware tools) removed. The template should have the latest version of the VirtIO drivers installed. The template file must exist on a Storage Pool in the cluster and be in a supported format. To upload the template to a Storage Pool see uploading files to a Storage Pool.

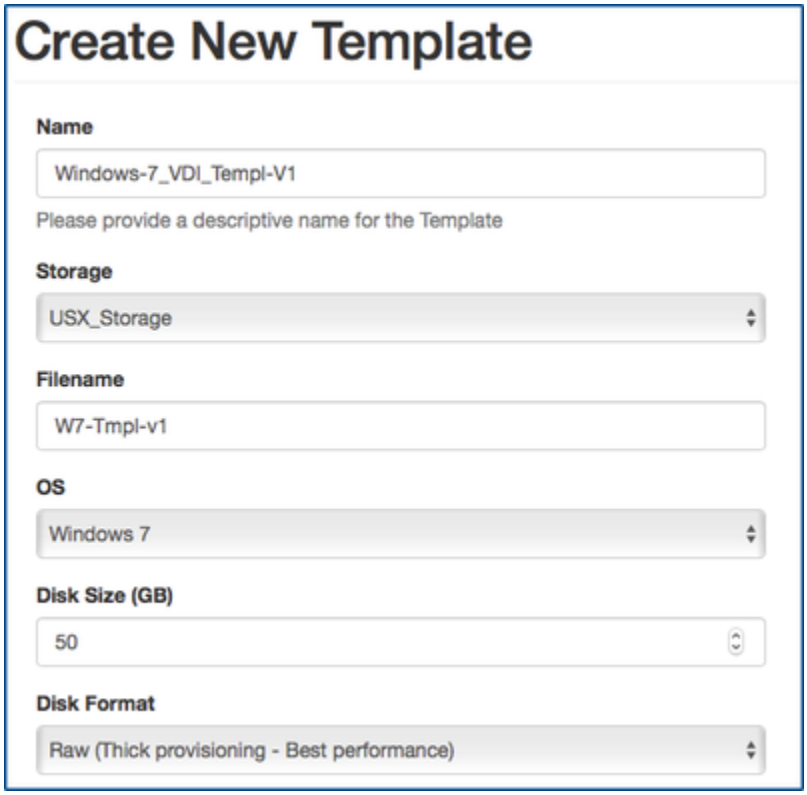
To add an existing template from a Storage Pool to Hive Fabric carry out the following steps:

1. Click on **Templates** on the left Navigation Bar.
2. Click on the **Add Template** button. Complete the following information:
   - **Name**: Assign a unique name to identify the template.
   - **Storage Pool**: Select the storage pool that the template resides on. Only stores that are meant to fulfill template storage roles will display here.
   - **File Name**: Select the template from the drop down list of files on the Storage Pool.

     > **Template Re-Use**
     > A template can only be added once to Hive Fabric. To re-use or add a template more than once, follow the steps on how to duplicate a template.

   - **OS**: Select the OS version of the template, this is used by the broker to display the appropriate version to the user. Select from **Windows 7**, **Windows 8**, **Windows 10**, **Windows 2012**, **Windows 2016**, or **Linux**.
   - **Description**: Enter a brief description for the template. This is optional, but may be preferred for organizational purposes.
3. Click **Add Template** to complete the process. The template will be validated and several actions become available depending on the current status of the template, see Template Management for more information.

Create a New Template

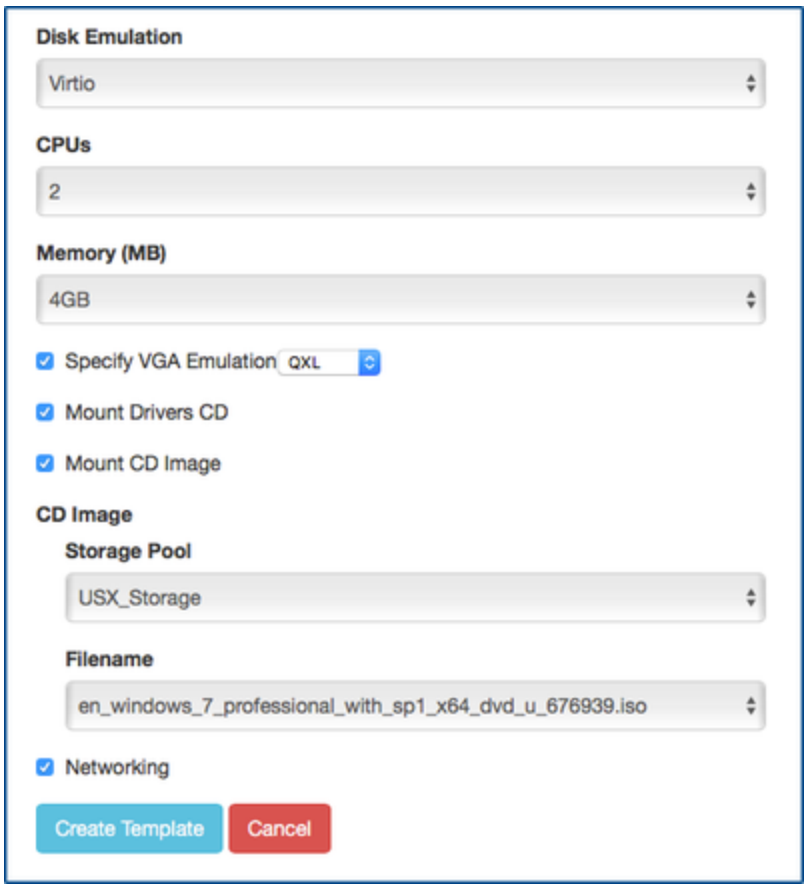


A new template is created through the Create Template wizard and is used to build a template from scratch, starting with the OS installation using an ISO file. The ISO file must first be uploaded to a Storage Pool. For more details, see Uploading files to a Storage Pool. Creating a new template will provide the best performance and a clean base to install applications and apply best practice configuration.

> **Golden Image**
> Templates are stored in a space efficient manner. When building a template from scratch it's a good idea to have a base install of the Operating System and some key optimizations (e.g. Drivers, performance optimization) and save this as a master template to create other templates from in the future. This is easily carried out by duplicating the template which gives a new standalone version that can then be further customize with applications and any settings specific to the Guest Pool intended to get delivered from the template.

To create a new template select the **New Template** button and complete the following information on the screen that appears:

- **Name**: Assign a unique name to identify the template.
- **Description**: Enter a brief description for the template. This is optional, but may be preferred for organizational purposes.
- **Storage**: The storage pool that will store the new template. Only stores that are meant to fulfill template storage roles will display here.
- **Filename**: Enter the name of the new file that will be created. A file extension does not need to be included.
- **OS**: The OS version that the broker will display when a user logs in. Select from **Windows 7**, **Windows 8**, **Windows 10**, **Windows 2012**, **Windows 2016**, or **Linux**.
- **Disk Size (GB)**: The disk capacity of the template. This size specified will be the same for the Guest machine.
- **Disk Format:** The appliance supports Raw and QCOW2 formats. Raw will give better performance. QCOW2 will be more space efficient. Where possible use RAW for the additional performance it provides.



- **Disk Emulation**: Specifies the disk emulation that the new template will use. Choose from **IDE**, **SATA**, **SCSI** , or **Virtio**. If a Linux OS is being installed the **VirtIO** option will be selected by default. **IDE** will be selected for a Windows OS.

> **Recomendation**
> The recommended disk emulation is **VirtIO**, using it will provide the best performance. VirtIO drivers are available as standard for most Linux OS. For any Microsoft Windows OS, the VirtIO disk driver will need to be installed by selecting the additional driver option during the install. The additional drivers and the VirtIO agent should be added once the OS is installed see VirtIO Device Driver Installation for more information.

- **CPUs**: The number of CPU cores to assign to the template during authoring. This is not the number of CPUs that a Guest Pool member will have.
- **Memory (MB)**: The amount of memory to assign to the template during authoring. This is not the amount of memory that a Guest Pool member will have.
- **Specify VGA Emulation**: Enabling this option sets the display emulation used in console mode. Choose from **VGA (Standard)**, **QXL**, **Cirrus**, **Xen**, or **VMVGA**. If left unchecked, this will be automatically set to **QXL**. This setting will not affect users accessing the virtual desktop.

> The default and recommended VGA emulation is **QXL**. If VGA emulation is selected for later versions of Microsoft Windows the resolution will default to 800 x 600.

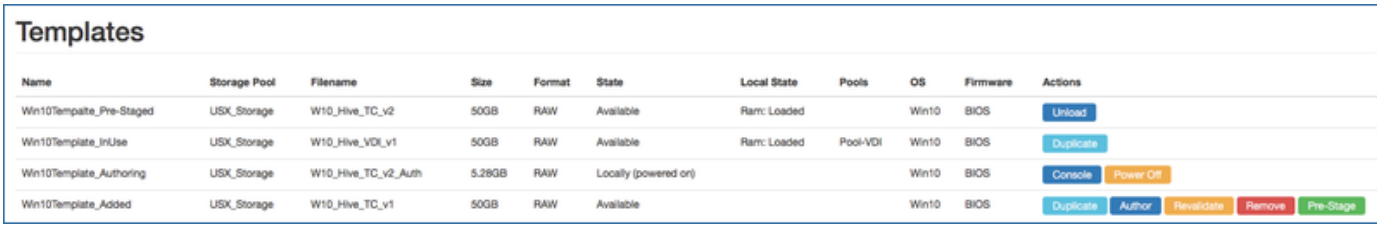
- **Mount Drivers CD**: Enabling this option will mount the included version of the VirtIO driver CD into the template to allow installation of optimized drivers for Hive Fabric.
- **Mount CD Image**: Enabling this option defines the ISO location or path of the installation ISO image.
- **Networking**: Select this to connect the template to the production network during authoring.

Click **Create Template** to complete the process.

This defines the parameters for the template and creates it. The template will automatically power-on. See Auth oring a Template and Template Administration for more information on how to connect to the console and

setup a template ensuring best practice is followed.

Template Management



Once a template has been created there are a number of different actions that form the lifecycle of a template:

Authoring a template is the most important of the template creation process and would typically include:

- Installing the Guest Operating System (OS).
- Installing the required applications.
- Applying HiveIO best practice configuration to the guest.

Staging a template for the creation of a Guest Pool.

- Users may also unload a staged template.

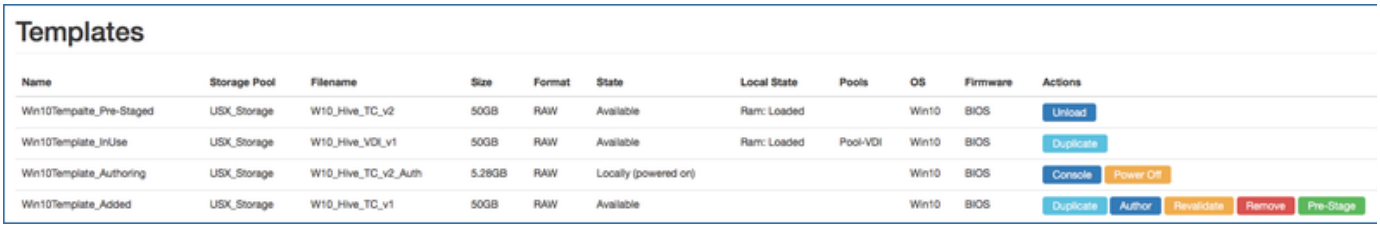
Duplicating a template to version or create a new template from a standard base.

Removing a template once it has been retired or is no longer needed.

Access the Console to install and configure the template's OS.

Revalidate a template for optimization and repairs.

Remove Template

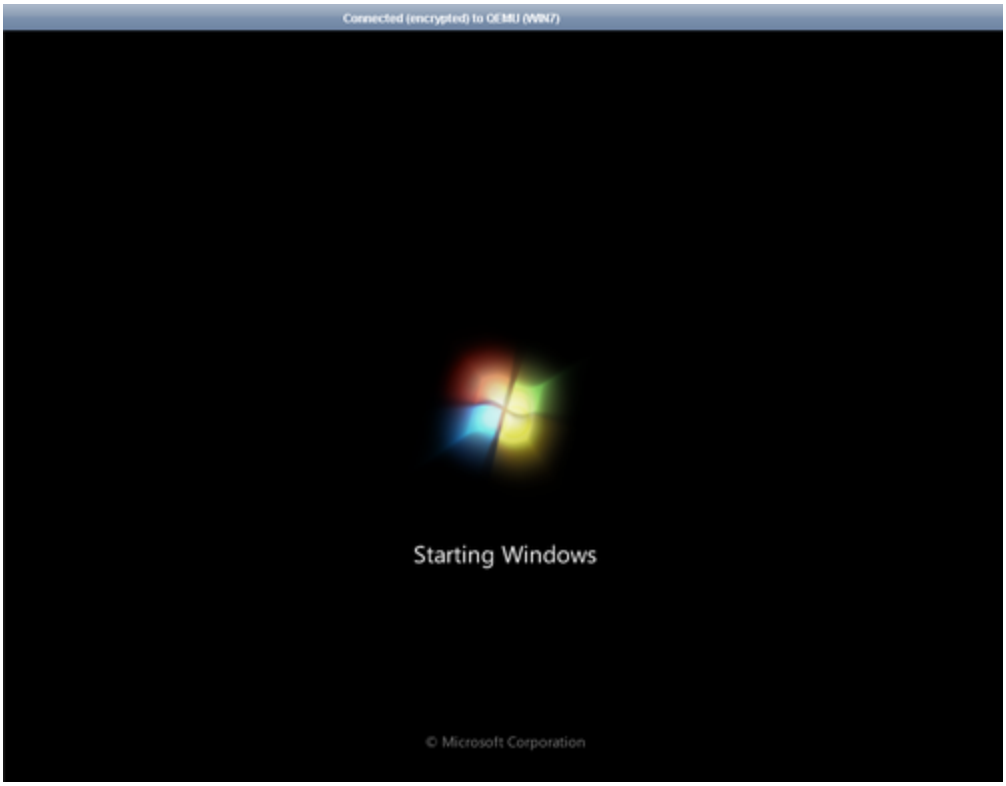


During the typical lifecycle of a deployment, a template may become outdated or no longer serve a purpose. The **Remove Template** option will remove an existing template from the template inventory. This will not delete the file from the Storage Pool. Delete obsolete template files directly off the storage.

Template Removal

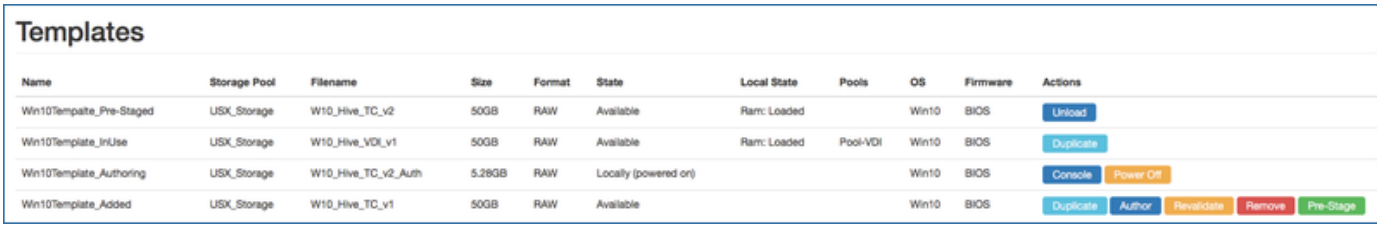
- A template can not be removed if it is in use or or staged for use across the cluster.

Template Console



This option opens a console session to the selected template, in a new browser tab. This allows for direct interaction with the template to install the Operating System, Applications or apply configurations and scripts.

Pre-Stage a Template

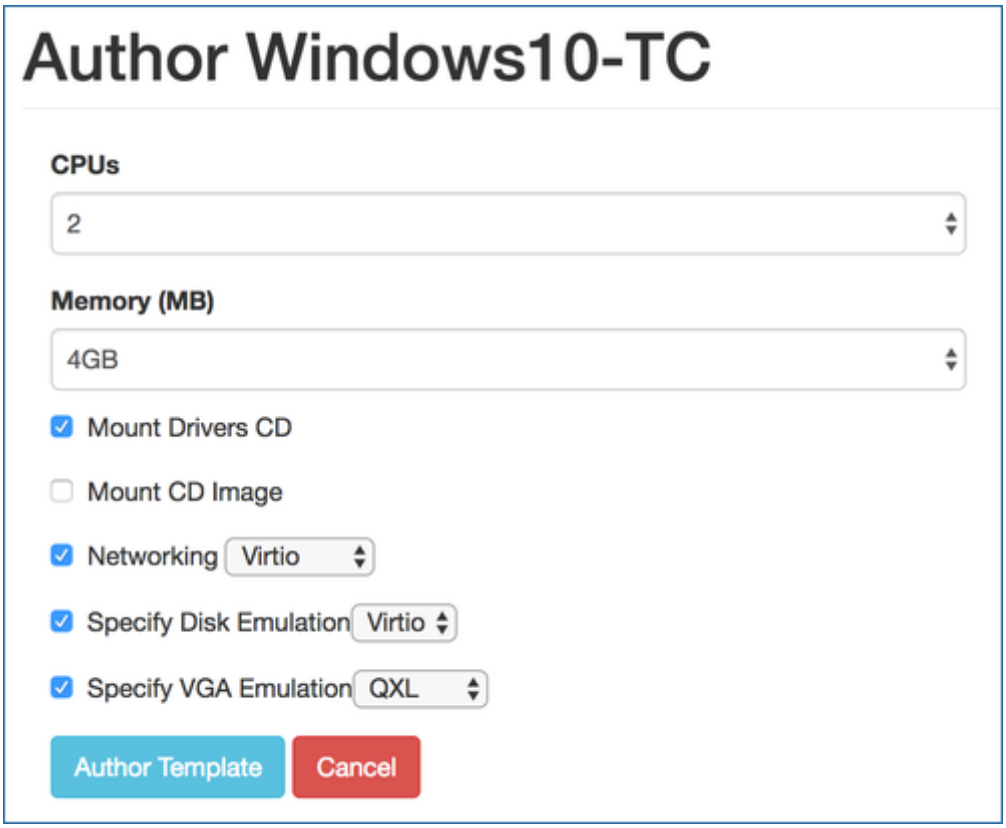


Template pre-staging copies the template to either local storage or the entire cluster, allowing for the template to be in the correct place ahead of Guest Pool creation. The option to stage cluster is only available once the appliance has joined a cluster. Once pre-staging has started, it may take a few moments for the load to complete. This will depend on the size of the template and the type of storage it is being copied to.

> Local RAM is typically the fastest pre-staging method, but will result in a template having to be re-staged in the event of a power-failure or host reboot.

To remove a template, refer to the instructions on how to Unload a Template.

Authoring a Template



Once a template has been added to the appliance or a new template created, it can be authored. Authoring allows the template to be booted up as if it were a guest VM to modify its install and configuration.

To author a template, click on the **Author** option under **Actions** for the template.

To allow the template to start, a number of settings must be specified. Note that these are specific for the template during authoring and are not used when deploying a Guest Pool. This allows for faster authoring through various means, such as temporarily assigning more memory. or CPU

> Templates kept within read-only Storage Pools will not have the authoring capability enabled.

- **CPU**: The number of cores to assign to the Template during authoring.
- **Memory**: The amount of memory to assign to the Template during authoring.
- **Mount Drivers CD**: This allows the Hive Fabric driver CD to be mounted inside the Template during authoring. This is required to install VirtIO version of drivers or update them to the latest version in the template.
- **Mount CD Image**: This allows for an ISO image to be mounted inside the template during authoring. This will behave like a standard CD, allowing for installation of update OS components or applications.
- **Networking**: Enables the network inside the template during authoring. Select the appropriate network driver type from the dropdown menu. The recommended option is **VirtIO**.
- **Specify Disk Emulation**: Specifies the method of disk emulation to be used during the authoring of a Template. The default will be automatically selected based on the OS selected. The recommended driver is VirtIO and this should be installed at the appropriate point.
- **Specify VGA Emulation**: Enabling this option sets the display emulation used in console mode. If left unchecked, this will be automatically set to QXL. Choose from **VGA (Standard)**, **QXL**, **Cirrus**, **Xen**, or **VMVGA**. This will not affect users accessing the virtual desktop.

> The default and recommended VGA emulation is **QXL**. If VGA emulation is selected for later versions of Microsoft Windows the resolution will default to 800 x 600.

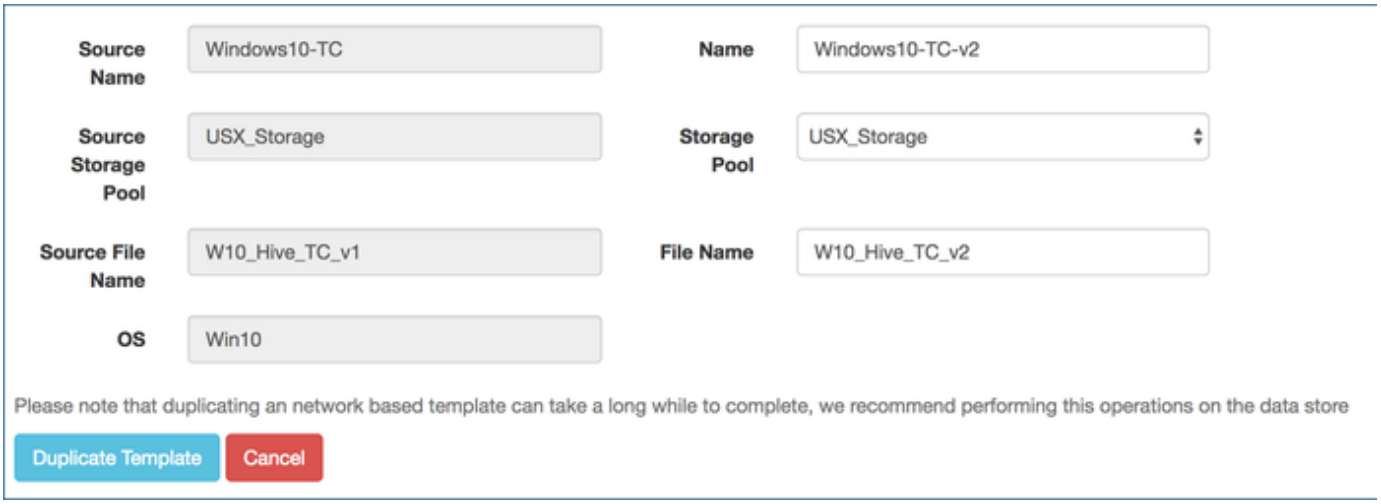
Click **Author Template** to set the resources and start the Template ready for interaction.

Microsoft Windows Requirements

- Windows templates require .Net 4.0 or higher to be installed for the Hive agent to work - https://www.microsoft.com/en-US/Download/confirmation.aspx?id=17718
- It is recommended to have the Visual C++ Redistributable package installed - https://www.microsoft.com/en-us/download/details.aspx?id=48145
- The Windows image must be 64-bit

Under the actions for the Template, click on Console to begin interacting with the Template through the console session. A new window will open, giving access to the console of the virtual machine so that changes can be made to the template.

Duplicate a Template



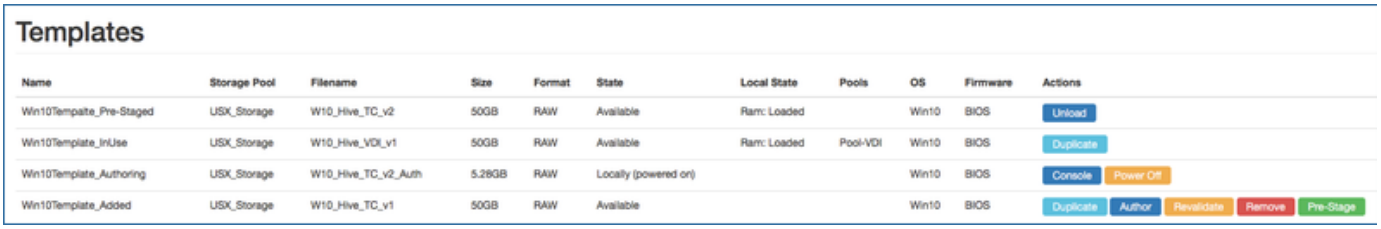
Duplicating a Template can be an efficient way to version a Template or have a base Template to build additional Templates from. This supports options such as the ability to build departmental templates that start from the same base OS template that has company-wide applications and settings applied. Each department template would then have specific applications installed and settings applied for their users.

The Duplicate Template option will copy an existing template creating a new standalone template.

1. Click on the **Duplicate** option under **Actions** and complete the required fields:
   - **Name**: The name of the duplicate template.
   - **Storage Pool**: Select the storage pool to store the new template.
   - **File Name**: The name that duplicate template image will be saved as on the Storage Pool.

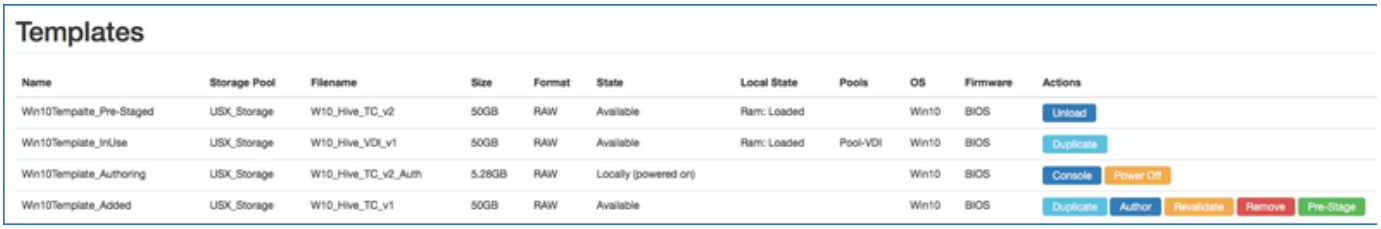
Click **Duplicate Template** to complete the process and start the template duplication.

Unload Template



Templates must be Unloaded before they can be removed from inventory. During the removal of a template it first has to be de-staged or 'unloaded' to ensure it has been removed from the cluster and can no longer be used. This is carried out by clicking the Unload button.

Template Validation

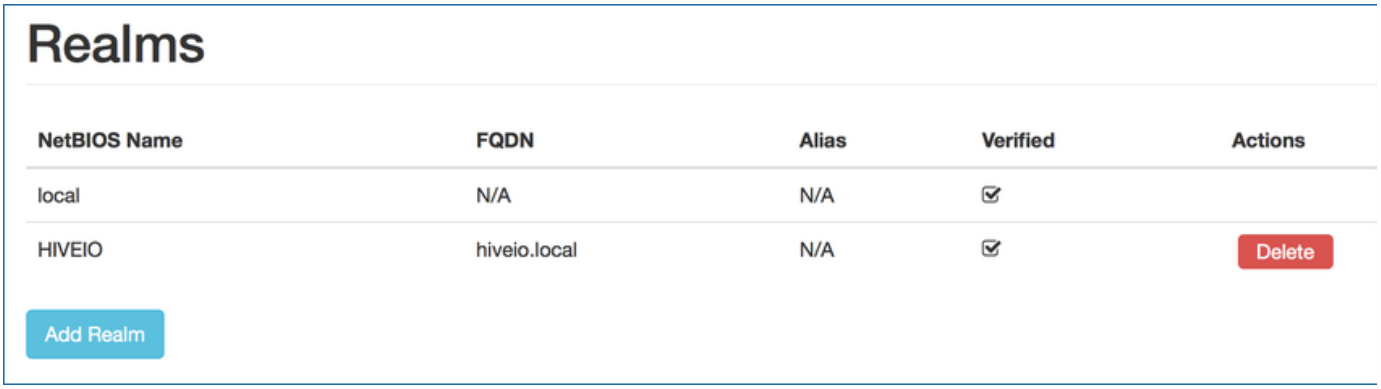


Occasionally, a template may need to be modified to add an application, apply an update or change a setting. This is carried out through the Authoring process. Following the shutdown of the template it must be re-validated to confirm that is in the correct state. During this process the re-validation process confirms:

- The template disk is partitioned properly.
- That the partitions are system readable and mountable.
- Checks that the appliance has read and write permissions on the template.
- That the filesystem on the template disk matches the OS that has been selected.
- Checks and where possible repairs any unclean filesystem (often caused by un-clean shutdowns).
- That the template is in the correct power-state (powered off).
- That hibernation has been disabled inside the template.

Should any of these fail the appropriate status will show in the UI and brief explanation will appear in the state's tooltip when the cursor is hovered over it.

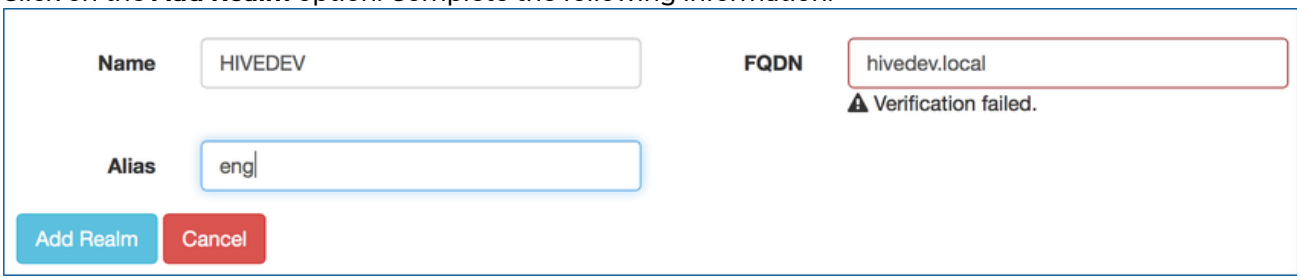
Realms



A Realm defines the link between the Cluster and an LDAP compliant authentication capability, e.g. Microsoft Active Directory. Authentication will happen under the umbrella of the Realm and will provide the building blocks to specify the users and groups that are allowed to authenticate against a Guest Pool. Multiple Realms can be specified to accommodate a wide variety of scenarios.

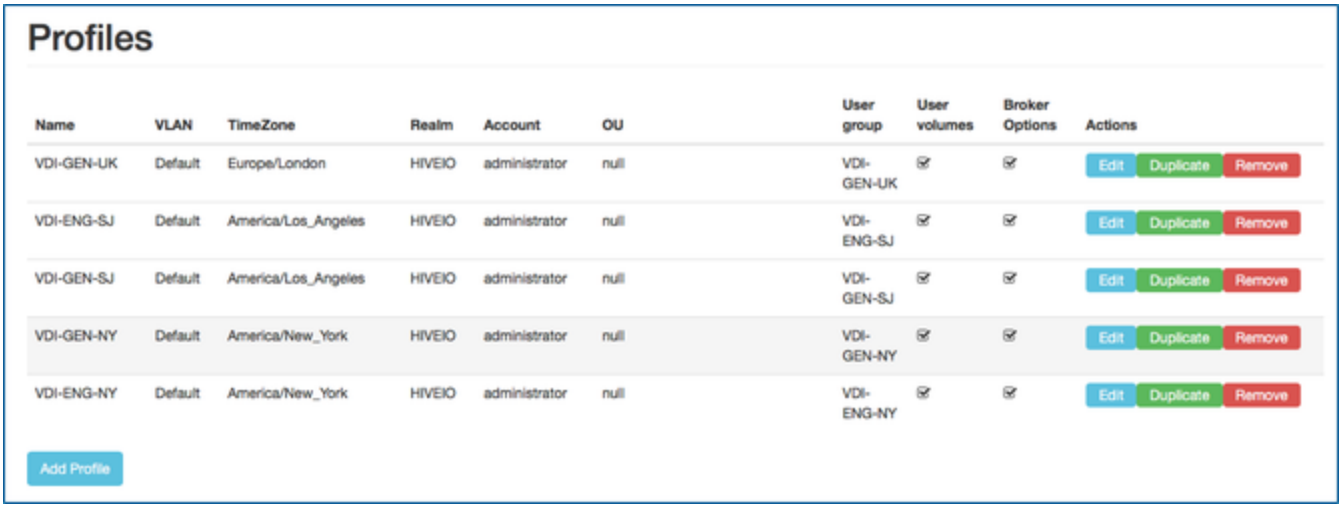
To define a Realm the following actions and information are required:

1. Click on **Realms** on the left side Navigation Bar.
2. Click on the **Add Realm** option. Complete the following information:



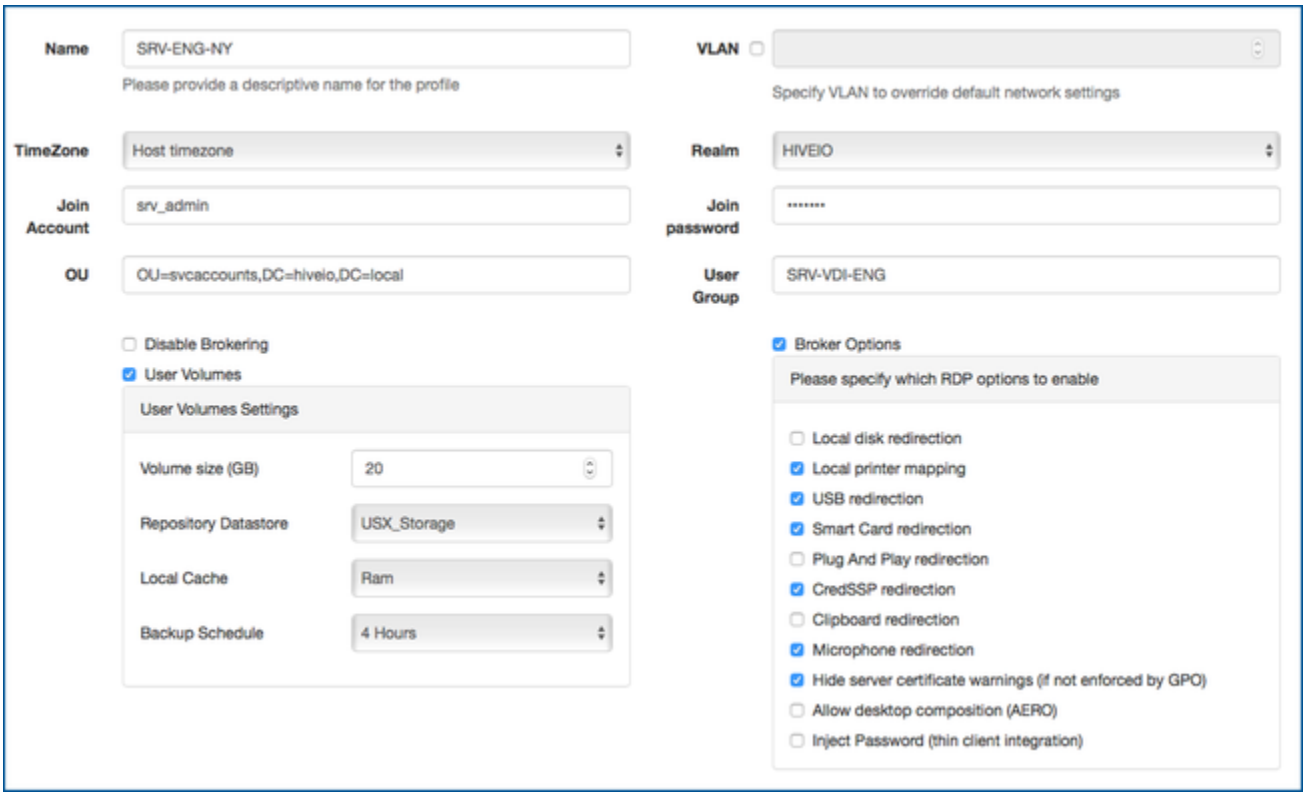
   - **NetBIOS Name**: The NetBIOS name of the domain being defined by the Realm.
   - **FQDN**: The Fully Qualified Domain Name of the domain. This field is automatically validated by the appliance and a success / failure message displayed for the administrator. If verification fails confirm that the information entered is correct, and that the FQDN can be resolved by the DNS server specified for the production network.
   - **Alias**: An alias can be set on a realm. It may be ideal to deploy this feature so users can login with their email domain rather than the actual domain name of the realm. `hivedev.local` could be the domain but the login uses `hivedev.com`. This is particularly useful in a multi-tenanted design.
3. Click **Add Realm** to save the Realm specification, once processed the Realm will be added to the list of Realms.

Profiles



Profiles are required to create a Guest Pool and allow Administrators to apply required settings to multiple guests with ease. The profile will dictate the functionality that the pool will provide to the end-user. These include access to a specific User Volume or the capability to connect to the user's Guest VM via the broker.

To Create a new Profile:



1. Click on **Profiles** on the left side Navigation Bar.
2. Click on the **Add Profile** option. A series of fields need to be completed:
   - **Name**: The name used to store the profile in Hive Fabric.
   - **VLAN**: Enter the VLAN ID if the default network settings will be over-ridden.
   - **TimeZone**: Select the time zone to apply to the profile. Leaving this at `Host timezone` will inject the current timezone set on the appliance.

> **UTC**
> For guests syncing with an AD, the timezone on the appliance and the AD must be set

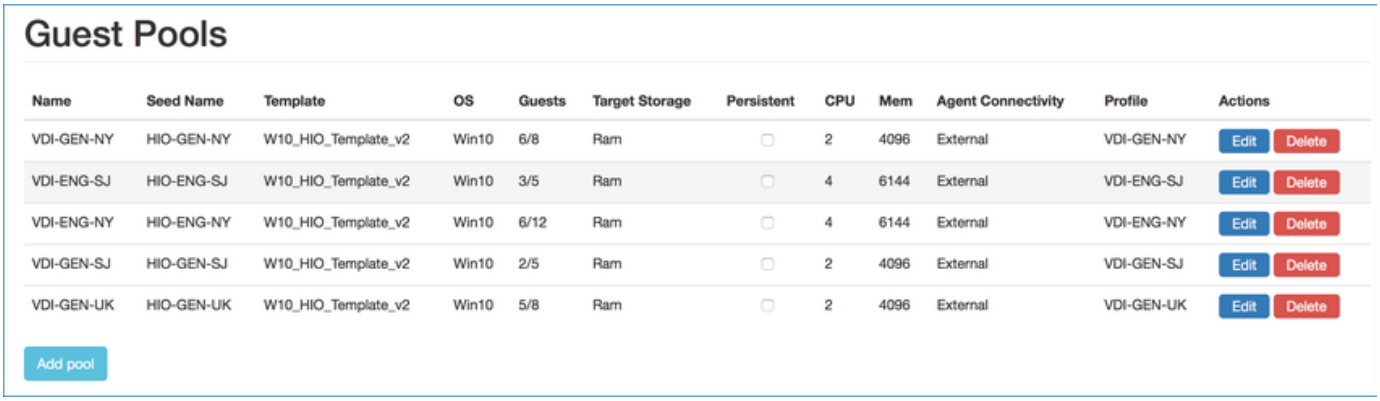
correctly. Using `UTC` as the timezone is recommended for proper timezone injection.

- **Realm**: Select the Realm to use for this Profile from the drop-down menu. The Realm specifies which authentication point will be used but the Guest Pool and should have already been created. Once the realm is selected, a new series of options will be present:
  - **Join Account**: Enter the account name of the user that has the appropriate privileges in AD to join Guests to the domain.
  - **Join Password**: Provide the password for the Join Account.
  - **OU**: Enter the Distinguished Name (DN) of the OU that contains the join account. If the administrator account is used then this does not need to be specified. This should be specified in the standard directory format, as shown here:
    ```
    <OU=service_accounts,DC=domain,DC=local>
    ```
  - **User Group**: The AD Group that contains the users that will log into the Guest Pool that this Profile is applied to.
  - **Disable Brokering**: Stops the Guest Pool from being accessed. This may be used to pre-stage Guest Pools. To enable access at a later date uncheck this option and set the appropriate settings for the Guest Pool. When brokering is disabled, **User Groups**, **User Volumes**, and **Br oker Options** can not be set.
  - **User Volumes**: Sets the appropriate settings for the User Volume.
    - **Volume Size (GB)**: The capacity for the User Volume allocated to each user.
    - **Repository Datastore**: The Storage Pool that will store the user volumes within this Profile. The recommendation is to use a shared storage Storage Pool for User Volumes.
    - **Local Cache**: Sets the cache for the user data, this copies the User Volume to the local appliance if the shared storage is slow for example this can provide a significant speed increase for the user. A RAM cache will be faster than a disk cache but consideration needs to be given for the available resources a good compromise is a local SSD.
    - **Backup Schedule**: Sets a schedule that the profile will follow for backing up user data from the local cache to the Storage Pool location. So long as a backup has been created, users will not lose data during a guest release. The schedule is typically dictated by the number of backups the Storage Pool can handle concurrently or the type of data stored in the profile and how often it is expected to change.
  - **Broker Options**: Select which options will be enabled when the user connects through the broker to their Guest.

3. Click **Add Profile** to complete the process. If all fields are validated correctly, the new profile will be added.

Once a profile has been created all of the settings can be modified or duplicated, using either the **Edit** or **Duplic ate** button, to remove a profile click the Remove button. Duplicating a profile can be useful for creating multiple profiles that share similar settings.

Guest Pools

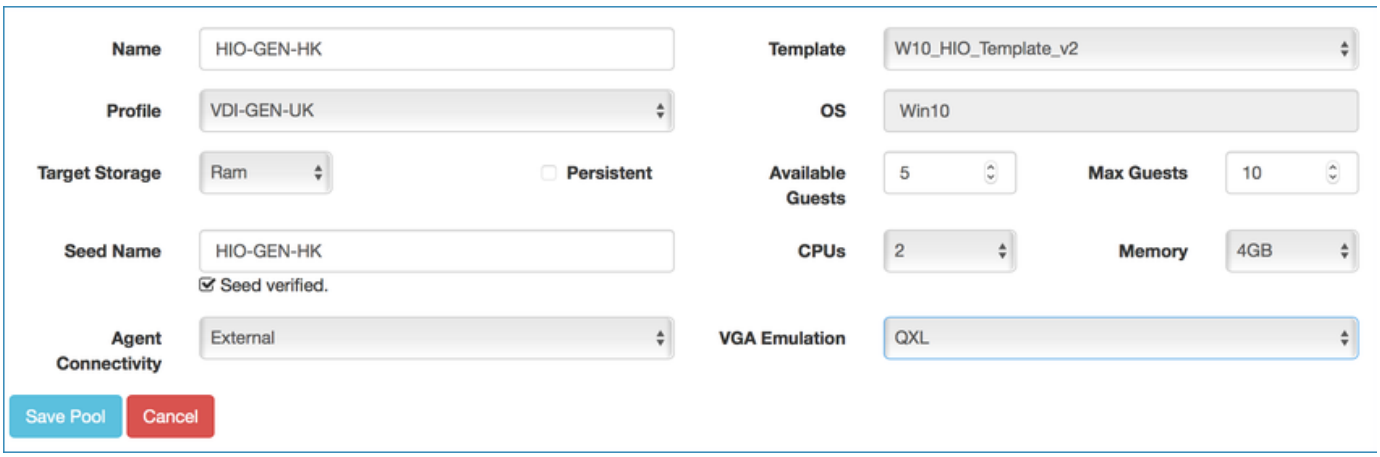


A Guest Pool is a set of Guest VMs that are grouped together to form a pool of resource that can be brokered to an end-user. The users that can access a Guest are defined in the Profile that is assigned to the Guest Pool. A user can login through the broker or gateway and have a single Guest VM assigned to them. A template must be created before a Guest Pool can be created. Multiple Guest Pools can be created to deliver multiple desktops to a single user or isolate one set of users from another. For example, if a small set of users need a specific application then a dedicated Template, Profile and Guest Pool can be created for them.

> Before proceeding, ensure that the Guest Template has the latest VirtIO drivers, optimizations applied, appropriate configuration, and the required set of applications installed.

To Create a Guest Pool carry out the following steps:

1. Click on **Guest Pools** on the left side Navigation Bar.
2. Click on the **Add Pool** option. A series of fields will need to be completed:



- **Name**: Assign a unique name to identify the Guest Pool.
- **Template**: Use the drop-down menu to select the template that will be used to create the Guest Pool.
- **VLAN Override**: Enter the VLAN ID. This will be set on the network interface of the Guests in the Pool.
- **OS**: Select the OS that is installed in the template. This will ensure the right icon is displayed in the broker for the end-user.
- **Storage Type**: Select the storage type that best fits the needs for the Guest Pool:
  - **RAM**: Memory based storage. This option is suitable for non-persistent or stateless Guests only. This storage type is deduplicated and compressed.
  - **Disk**: Local Disk based storage. This option can provide storage for hosting both persistent and non-persistent guests. If Persistent Guests are being deployed for production use the recommendation is to use shared storage. This storage type is deduplicated and compressed.
  - **Shared Storage**: Any shared storage pools that have been added to the cluster will be displayed in this list by their Name and can be used to host persistent guests. This option does not provide deduplication and compression natively but this may be delivered by the underlying storage for

example when using Hive USX. A Storage Pool has to be used if HA is required.

- **Persistent**: Determines whether the Guests being deployed are persistent. When enabled, VMs will persist across a reboot. Otherwise, each VM will start on a fresh state upon rebooting.
- **Min Density**: Sets the minimum number of Guest VMs that will always be available to be brokered from the pool. Once provisioned, this minimum number of Guests will be available at all times assuming there is enough resource in the cluster to create the Guests. The minimum number of Guests in a "Ready" state will be provisioned across the cluster until the maximum amount has been met, or the system runs out of resource.
- **Max Density**: Sets the maximum number of Guests that can be created in the Guest Pool. Once the maximum number of Guests has been achieved the appliance will stop accepting provisioning jobs from the cluster until a Guest slot frees up in the future.
- **Seed Name**: Assign a string that will be the prefix the the computer names of the Guests This must be a NetBIOS compliant hostname. The Seed Name will be appended with a 3 digit number starting from 000 and will increment by 1, ensuring Guest VM names are unique.
- **CPUs**: Select the number of cores to provide to each Guest.
- **Memory**: Select the amount of memory available to each Guest. The maximum that can be selected is 32GB as of this release.
- **Agent Connectivity**: Sets the method of connectivity to the Hive Agent. To live migrate Guests between hosts, set this option to **External**. Otherwise, this can remain at the default **Internal**.
- **VGA Emulation:** The VGA Emulation used by the Guest.

Click **Save Pool** to complete the process and start creating the Guests for the pool. When loading completes, the Guest Pools will spawn.

Once a Pool has been created then it can be edited or deleted using the appropriate buttons. When editing a Pool all of the fields mentioned above can be modified except for the Seed Name and the OS type. If the number of Available Guests or Max Guests is changed then this will only affect Guests that are not in use. For example if the max size of the pool is reduced but the number of Guests in use exceeds this, then they will remain until the user logs off. Afterwards, the Guest is destroyed and is not re-provisioned on the system.

Standalone Guest

A Standalone Guest can be created in lieu of a full Guest Pool. This is ideal for creating single instance servers with their own dedicated disks.

1. Click on **Standalone Guest** on the left side Navigation Bar. A series of fields will need to be completed:
   - **Name**: Assign a unique name to identify the Guest.
   - **Storage**: Select a storage option that has been established within the Storage Pool.
   - **File Name**: Select a Guest Image file from the dropdown menu. This image file must be contained within the selected storage option.
   - **OS**: The OS that the broker will display. Select from **Windows 7**, **Windows 8**, **Windows 10**, **Windows 2012**, **Windows 2016**, or **Linux**.
   - **Disk Emulation**: Select a storage disk emulation option. Choose from **IDE**, **SATA**, **SCSI**, or **Virtio**. If a **Linux** OS was selected above, the aappliance will automatically select the **Virtio** option.

     > The VGA (Standard) display displays at a low resolution.

   - **Firmware**: Select a firmware option. Choose from either **BIOS** or **UEFI**.
   - **CPUs**: Select the number of cores to allocate to the Guest. Larger images may require more cores.
   - **Memory (MB)**: Select the amount of memory to allocate to the Guest. Larger images may require more memory.
   - **VGA**: Select the display hardware to allocate to the Guest's console. Choose from **VGA (Standard)**, **Q XL**, **Cirrus**, **Xen**, or **VMVGA**. This will not affect users accessing the virtual desktop.
   - **Agent Connectivity**: Select the method that the Agent will connect. In most cases, this can be left at the default **Internal**.

     > **External** Agent Connectivity is a legacy option to support hardware that does not have the VirtIO drivers. For best results, install the VirtIO drivers before continuing.

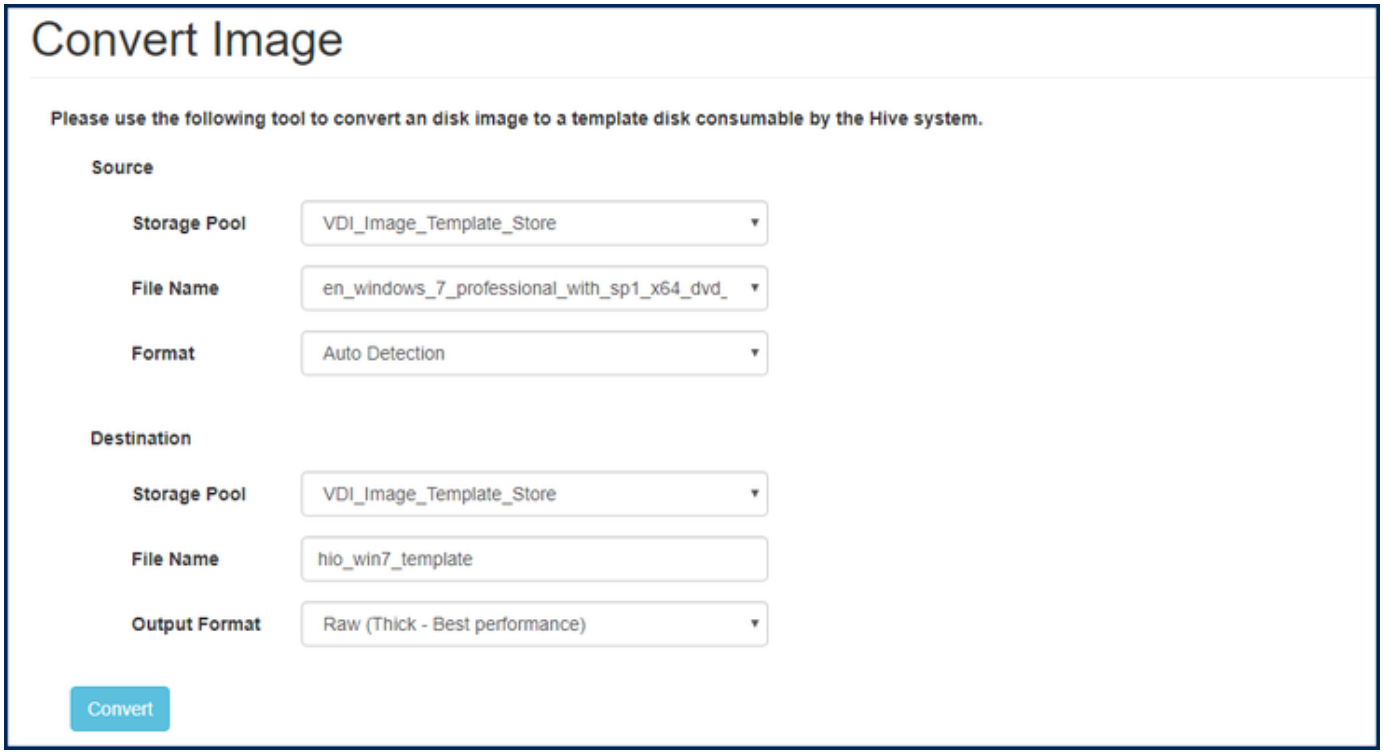
   - **TimeZone**: Select the time zone to apply to the profile. Leaving this at *Host timezone* will default to whichever time zone the host is currently using.
   - **Mount CD Image**: Enable this option if the Guest needs to mount a CD image. When selected, new options appear.
     - **Storage Pool**: The storage location of the CD image.
     - **Filename**: The name of the CD image within the storage location.
   - **Specify Network Device**: Enabling this option will allow a specific network device to be selected. Choose from **Virtio**, **e1000**, **ne2k_pci**, **pcnet**, or **rtl8139**.
   - **Specify VLAN**: Enable this option to specify a VLAN.
2. Click **Launch Guest** to complete the process. The Standalone Guest will be ready for use.

Tools

Extra tools are available to further assist with the usage of the Hive Fabric. The appliance offers users the ability to Convert an Image. With this tool, a disk image can be converted into ready-made template image. When the conversion is completed, follow the Add an existing Template wizard to begin preparing the new template image for Guest use.

Convert an Image

The Hive Fabric is compatible with any QEMU or KVM-supported disk emulation. Typically, the Hive Fabric will automatically convert images into a preferred usable format. The conversion tool reduces the need to constantly convert a template every time it is added to the Hive Fabric. This makes the process of adding a template quick, convenient, and easier to consume.



> VirtIO drivers must be installed and hypervisor tools must be remove first before an image is ready for conversion.

1. Click on **Standalone Guest** on the left side Navigation Bar. Complete the following information:
   - **Source**
     - **Storage Pool**: Select the storage location containing the disk image.
     - **File Name**: Select the image file from the dropdown menu. The image file must be contained within the selected Storage Pool.
   - **Format**: Select the format that will be used to convert the disk image.
   - **Destination**
     - **Storage Pool**: Select the storage location that the converted image will save to.
     - **File Name**: Enter a new file name for the converted disk image.
2. Click **Convert** the complete the process and begin the image conversion. The conversion may take a few moments to complete before the image becomes usable.

Return to Top

Settings

This segment contains all the setting and configuration options for the Hive system itself. Many of these settings may need to be adjusted before properly using the Hive appliance.

Appliance

Appliance configuration sets the general configuration of the host. The initial cluster configuration for an appliance is also done on this page.

1. On the left side Navigation Bar, under **Settings**, click on **Appliance**. The following fields may be set:
   - **Hostname**: Assigns a hostname to the appliance.
   - **Timezone**: The time zone of the host location/environment.

     > This needs to be set or Guests will not join the domain.

   - **NTP Server**: The NTP server IP address.

     > This needs to be set or Guests will not join the domain.

   - **Center Management Appliance**: Enter the IP address of the current Central Management Appliance (CMA) to join the appliance to an existing cluster. To set the current appliance as the Central Management Appliance, enter the name `localhost`. For more information on cluster management, refer to the Cluster Administration page.
   - **Max Clone Density**: The maximum number of Guest VMs permitted to this host. This will override all Pool density settings. The default amount shown is based on the server's system specs.
   - **Broker**: Enable and configure Guest VM brokering based on Realm and AD Group membership.
     - **Passthrough**: When set, authentication is performed a the Guest. Users will only need to enter a username.
     - **Hide Realms**: Disables the realm selection menu from the broker's login screen. Users are required to login with the UPN format `user@realm-fqdn`.
     - **Auto Connect**: When enabled, users will automatically connect to a Guest. Users that are members of more than one Guest Pool will connect to the first Pool.
     - **White Labeling**: Allows customization of the broker's login website.
       - **Theme**: Sets the color theme for the broker website.
       - **Logo**: Enter the external address of the logo image for the broker website.
       - **Favicon**: Enter the external address of the favicon image for the broker website.
       - **Company Name/Title**: Enter a name for the broker website to display in the welcome message of the login screen.
       - **HTTP Formatted Company Name/Title (Optional)**: Enter an HTTP-formatted name for the broker website to display in the welcome message of the login screen.
       - **HTTP Formatted Disclaimer (Optional)**: Enter an HTTP-formatted message for the broker to display on the login screen.
       - **Preview**: Pressing this button will display a preview of the broker's login page with the currently entered settings. If everything looks satisfactory, apply these settings by clicking on the **Submit** button.
   - **Gateway**: Enable and configure the remote connection broker.
     - **External Address (URI)**: Enter the gateway's URI. This will be used by the remote gateway for RDP connections.
     - **Start Port** and **End Port**: The range of firewall ports that the gateway will use.
     - **Deployment Type**: Determine if the broker will service **Local** guests from the appliance or **Global** guests from the cluster.
   - **Log Level**: Changes made are applied after restarting the Hive Services from the **Administration** page.
2. Click on **Submit** to complete the process.

Network Interfaces

This is the section used to configure the network settings that are specific to the environment. Administrators are about to create a Bond Interface. This allows for teaming multiple NICs to a single bond interface. This creates a network redundancy when each interface is connected to separate switches.

1. Click on **Network Interfaces** on the left side Navigation Bar.
2. To create a new Bond Interface, click on **Configure Bonding**. A series of options will be available:
   - **Members**: Select the networks that will be included as members of the Bond Interface. A minimum of two members are required to create a Bond.
   - **Mode**: Select the mode that the Bond will act in. Choose between **Active/Backup** or **802.3ad LACP**.
   - **Primary**: Select the network connection within the bond that will be set at the primary connection.
3. Click on **Submit** to complete the process. The Appliance will need to either **Reboot** or **Restart Network Services** to apply these changes.

Adminstrators can also configure port options for each network.

1. Click on **Hardcode Settings**, next to the network that will be configured. A seires of options will be avaialble:
   - **Speed**: Sets the speed for the network connection. Set this option to **Auto** detect, or select one of the speed options available.
   - **Duplex**: Sets the communication flow for the connection. Set this option to **Auto** detect, or select **fu ll** or **half**, based on the Ethernet connection.
   - **MTU**: Sets the maximum transmission units for the connection. Adjustments to this option are based on the connection.
2. Click on **Submit** to complete the process. The Appliance will need to either **Reboot** or **Restart Network Services** to apply these changes.

Network Addresses

This section will configure the network interface/VLAN that will be used as the guest VM's production network. Trunking and VLAN tagging are both supported. If a storage network is available for use, the appliance may also be enabled to access it. Using a storage network helps to segregate the management traffic and storage traffic within the network.

1. Click on **Network Addresses** on the left side Navigation Bar.
2. For **Production Network**, the following values may be set. Note that by default, these options are set to the values entered in the First Boot Wizard:
    - **Interface:** Select the network interface of the appliance.
    - **VLAN:** Specify the VLAN ID, if the server will be joining one.
    - **DHCP:** When enabled, an IP address is automatically assigned to the device. Disabling this option will allow entry of an IP Address, Netmask, and Gateway. If DHCP is to remain enabled, no further edits need to be made unless the DNS server being used is changing, or a DNS Search Path is being provided.
        - **IP Address:** Enter the static IP Address to assign to the server. This will change the IP Address used to access the web interface.
        - **Subnet Mask:** Enter the netmask for the network's host.
        - **Default Gateway:** Enter the default gateway for the network.
    - **DNS Server:** Enter an optional DNS server address. When using multiple DNS servers, separate the list with spaces.
    - **DNS Search Path**: Enter an optional DNS search path. When using multiple DNS search paths, separate the list with spaces.
3. For **Storage Network**, the following values may be set:
    - **Enable Storage Network:** When enabled, the storage area network becomes accessible after credentials are entered.
        - **Interface:** Enter the network interface of the storage area network.
        - **VLAN:** Enter the VLAN ID of the storage area network.
        - **IP Address:** Enter the IP Address of the storage area network.
        - **Subnet Mask:** Enter the netmask of the storage area network.
4. Click on **Submit** to complete the process. Once complete, the network must be restarted from **Administration** on the left side Navigation Bar. If the IP address has changed during this process, enter the new IP address into the Web Browser to regain access to the Web Interface.

Administration

Various maintenance and administrative options are available to ensure that the Hive Fabric runs efficiently. Regular maintenance is critical to the Appliance's health and should be performed regularly. Users must have administrative privileges in order to apply updates, power manage the appliance, or upload/download files.

Licensing

Users can view the current Appliance license and the amount of time remaining on that license. To add or extend the license, click on the **Upload License** option. Enter the **License Key** and click **Upload License** to add the new license.

Power Management

Administrators can manage the power of the Appliance.

- **Shutdown**: Shuts down the appliance. During a shutdown, no guest pools will be accessible.
- **Restart**: Restarts the Appliance. Guest Pools will not be accessible during the restart process. This option can be run whenever changes to the network or services have been applied.
- **Restart Network Services**: Restarts the Hive Appliance's network. This option is necessary whenever a change to the network has been applied.

  > This option should not be executed while there are users logged in to Guest Pools. Make sure that all users have logged out before performing a restart to network services.

- **Restart Hive Services**: Restarts Hive services without restarting the Appliance itself.

The following options will also be available once the Appliance has joined a cluster:

- **Unjoin Cluster**: Releases the appliance from its current cluster membership. This must be done before an appliance can join a new cluster. Do not use this option on appliances that have been designated as the CMA.
- **Enter/Exit Maintenance Mode**: The Appliance to enter or exit maintenance mode. The appliance must be in maintenance mode before it gets released from the cluster.

  > Do not interact with the database while the Appliance is in Maintenance Mode.

Software Firmware

This displays all software packages uploaded to the Appliance. Any package check-marked as **Current** is the version that is currently in use. Here, Administrators can easily upgrade the appliance without having to run through the installation process a second time. To upgrade the software package:

1. Download the latest `.pkg` file with the most current version of Hive Fabric.
2. Click on **Administration** on the left Navigation Bar.
3. Click on the **Upload Software** button. A Browse prompt will appear, where users can select the appropriate `.pkg` file.
4. Once the file has successfully uploaded, a few new actions will appear: **Stage** and **Delete**. Clicking on the **Stage** button prepares the appliance for package deployment. This process may take a few seconds.
5. When the package is staged and ready, click **Deploy** to install the update, or click **Cancel** to destage the package and cancel the update process.
6. Once the deployment begins, the package begins installation. This process may take a few moments to complete. During this time, the web interface and the server console will not be accessible.
7. When deployment completes, Hive will automatically restart and begin using the newly-deployed version.

Appliance Firmware Images

This displays all appliance firmware uploaded. Any version marked as **Current** is the version that is currently *Acti ve*. Inactive versions are marked as on *Standby*. The **Upload Appliance Firmware/Patch** option allows Administrators to upload a new version of the Appliance. When selected, a Browse prompt will appear, where users can select the appropriate `.tar` or `.gz` file. From there, newly uploaded images can be selected as the **Curr ent** version in use, and the previous version will be sent to *Standby*.

Support Files

This displays any files that have been created to give to Support for troubleshooting purposes. Clicking on **Creat e Support File** creates a compressed file that can be given to a HiveIO Support member. The file will be added to the Support Files inventory, along with the creation date and file size. Users may choose to **Download** the file for themselves or **Delete** the file if it is no longer needed.

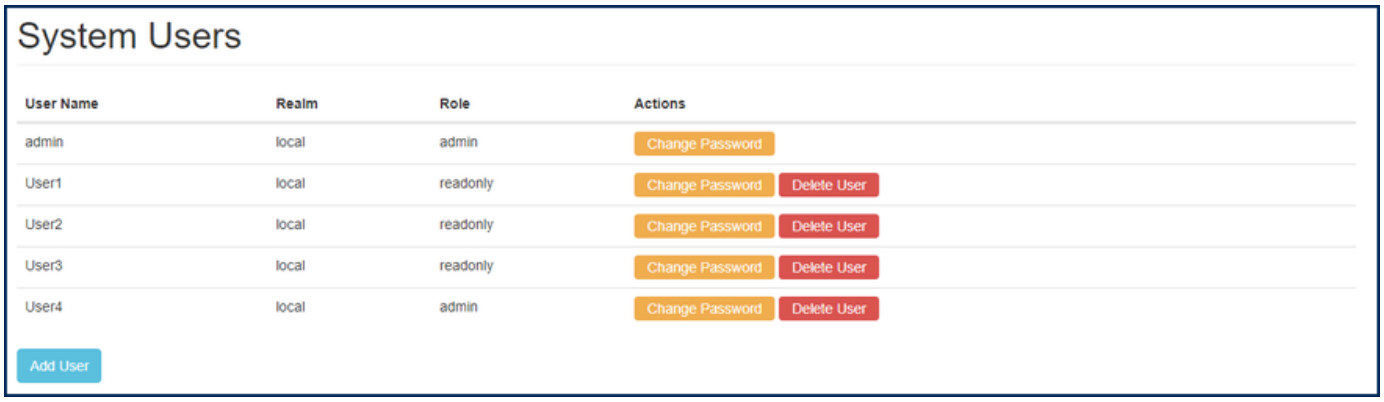
> **Timezones**
> Support logs print using UTC, regardless of the timezone set within the system.

Certificates

Displays any security certificates that have been applied to the Appliance. Users can view the **Status** of the certificate, the **Issuer** of the certificate, and the **Expiration** date of the certificate. The **Upload Certificate** option allows Administrators to upload a new Certificate to the Appliance. When selected, users can select to upload a new **Certificate** or **Key**. Clicking on either of these options will open a Browse prompt, where users can select the appropriate `.cer` file.

Users

This section is for Administrators looking to configure user accounts for the Hive Appliance. New users can be added to the system. These accounts are primarily for navigating the Fabric and cannot be used to access Guest desktops.



1. Click on **Users** on the left side Navigation Bar.
2. Click on the **Add User** option. A series of fields need to be completed:
    - **User Name**: The name of the user. This name must be unique.
    - **Realm**: The realm that the user has access to.
    - **Role**: The role of the user. *Admin* accounts have full privileges within the appliance. *Read only* accounts only have view privileges and cannot configure any settings or options within the appliance. It is important to determine which role the new user will fall under before creating the account. Once the role is set, it cannot be changed.
    - **Password**: Sets a password for the user. All accounts must have a password.
3. Click **Add User** to complete the process. The user account is immediately available for use.

Administrator accounts have the ability to **Change Password** for any account, or **Delete User** for existing accounts.

Template Administration

Templates will need updates during its life cycle. When the end user is ready to update, the procedure should be as follows:

1. First, duplicate the current template. This duplicate makes it easy to retain many of the templates settings during the update process. This also ensures that the current template does not get corrupted during the update process, should any errors or issues arise.
2. Author the duplicate template to apply the updates.
3. Modify the current guest pool for the new template, if the guest pool is not persistent.

> **Recommendation**
> It is ideal to set the "Available Guest" counter down to `0`. Then, once all unassigned guests have been destroyed, restore the available guest value.

Existing guests are not affected by the template update process, unless the "Available Guest" counter is set to `0`. Any new guests spawned will use the new template. Current users will receive the new guest templates upon logging off of their session.

> **Recommendation**
> When adding or creating a template, the recommended disk emulation is **VirtIO**. Use this whenever possible for the best performance. VirtIO drivers are native to most Linux systems. However, for any Microsoft Windows OS template, use IDE for install. The VirtIO drivers will need to be installed during the OS install or added to the template after installation for best performance and for network connectivity. For more information, view the process for installing VirtIO device drivers.

Before administrating a template, be sure to review:

- The best practices for proper desktop image management.
- The steps for installing VirtIO device drivers to a Windows OS image.

VirtIO Device Drivers Installation

VirtIO is a virtualization standard for network and disk device drivers where the guest's device driver understands it is running in a virtual environment, and cooperates with the hypervisor. This helps to ensure the guest gets the best possible performance for network and disk operations. HiveIO best practice also state to use these drivers for all applicable guests. Most Linux guests will come with VirtIO drivers pre-installed and will automatically use these.

There are two scenarios to consider:

1. Using an existing template and switching the current drivers installed in the guest over to VirtIO drivers. During the template authoring process, select the "Mount Drivers CD" option, under Networking. Select the `VirtIO` option, but ensure that Specify Disk Emulation matches the disk driver inside the guest. This is likely to be iSCSI on most modern templates. The following process will switch to the VirtIO drivers:
    a. Author the template and login to the guest with administrator privileges.
    b. Open the Start menu and search for Device Manager.
    c. Locate the Ethernet Controller. Right-click on this option and select "Update Driver Software".
    d. Follow the update wizard's prompts when they appear. When asked how to search for driver software, select "Browse my Computer for Driver Software". Enter the path to the CD drive and specific folder for the Guest OS. e.g: `d:\NetKVM\w7\amd64`.
    e. Follow the prompts to complete the driver installation process.
    f. Repeat this process for the SCSI Controller and PCI standard RAM Controller.
    g. Any unknown devices may also have VirtIO device drivers that can be updated by following this same procedure.
2. Creating a new Template. Select the "Mount Drivers CD" option, under Networking. Enable "Specify Disk Emulation" and select the `VirtIO` option.
    a. During the installation of Windows use the "Specify Additional Driver" option to navigate to the appropriate OS folder on the VirtIO driver CD for the SCSI controller. Add this so that Windows can recognize the disk for installation.
    b. Once the Windows installation has completed, the additional devices can be updated or installed. Login with a user that has administrative privileges
    c. Open the Start menu and search for Device Manager.
    d. Locate the Ethernet Controller. Right-click on this option and select "Update Driver Software".
    e. Follow the update wizard's prompts when they appear. When asked how to search for driver software, select "Browse my Computer for Driver Software". Enter the path to the CD drive and specific folder for the Guest OS. e.g: `d:\NetKVM\w7\amd64`.
    f. Follow the prompts to complete the driver installation process.
    g. Repeat this process for the SCSI Controller and PCI standard RAM Controller.
    h. Any unknown devices may also have VirtIO device drivers that can be updated by following this same procedure.

Desktop Image Management

Repository

An external NFS, CIFS, or Ceph volume is required as a desktop image repository. These shares store OS images and template images for Hive Fabric use.

> **Permissions**
> Any storage with read-only permissions can add existing templates, but will not have access to template creation and authoring.

Delivery

New desktop image deployment is achieved by updating the template used within the Guest Pool configuration. Once a new desktop image is pushed to the repository, a new template can be created in the HiveIO Administration portal. After the template is created, it can then be assigned to any existing Guest Pool or during Guest Pool creation. For more information, review Templates.

Guest Session Scripts

The Hive Fabric supports the use of hook scripts for advanced users who want to automate certain agent processes within their Windows deployments. These scripts are executable string files that are placed within a designated folder, typically `C:\Program Files\HiveIO\Scripts`, of the Guest OS template. Because these scripts must run within the template, they will have to be baked into the Windows template before deployment. This can be done from within the Console during the Template Authoring process.

A script starts running whenever a specific session change event occurs. The supported values are:

- Onlogin
- Onlogoff
- Onremoteconnect
- Onremotedisconnect

In the example given below, the script will set a name for the Citrix ICA client to use by forwarding the hostname of the device to the remote desktop.

set_citrix_clientname

```
$key = (get-itempropertyvalue -Path "HKLM:\SOFTWARE\HiveAgent" -Name
"ClientName")
set-itemproperty -Path "HKLM:\SOFTWARE\Wow6432Node\Citrix\ICA Client" -Name
"ClientName" -Value $key
```

To run a script from a template:

1. Author the template and access the template console.
2. Place the script into the Windows image's `C:\Program Files\HiveIO\Scripts` folder.
3. Open the Windows Registry Editor and edit the following registry path “HKLM\SOFTWARE\HiveAgentActions”. Add an SZ value to reflect one of the supported session event values above, depending on when the script will run. The contents of that value must be the full filepath for the script. Based on the sample script above, this would be `C:\Program Files\HiveIO\Scripts\set_citrix_clientname.ps1`.

Session scripts are non-interactive, so no further user input will be required upon running. The executable file executes the strings and starts the process as written in the script. After the script runs, logs are generated.

Cluster Administration

Hive Fabric supports the grouping of multiple Appliances in a Cluster. This allows for cross-server administration, resource load balancing and simple administration of a large number of appliance. A cluster requires a minimum of two appliances. However, the recommendation is to have at least three appliances. This provides further resilience and ensures a quorum is available to handle a "split-brain" scenario. The cluster is maintained by the Central Management Appliance, or CMA role. This role is assigned to the first server that forms the cluster. The CMA gets replicated across the other members of the cluster. These members becomes proxies and get cached.

The first three appliances to join the cluster automatically become Cluster Managers. All manager appliances run the database service within the cluster and replicate changes between each other. Once the Cluster Manager roles are assigned, appliances that join the cluster after this point become Cluster Members. The cluster will always attempt to have three managers. If the CMA ever experiences an issue, the cluster can cast a majority vote and promote a member to a Cluster Manager role.

Further details on joining and managing the cluster :

- Joining an appliance to a Cluster.
- Removing an appliance from a Cluster.
- The Cluster Dashboard monitors and maintains the entire cluster.
- Follow these Best Practices when building out clusters.

Cluster Dashboard

The dashboard portal will provide monitoring functions to the entire HiveIO cluster. To access the Dashboard portal, enter the URL as: `https://<HiveIO-Host-IP>/dashboard`.

Overview

The **Overview** tab provides an overall monitoring view of the entire cluster. It displays Key Performance Indicator graphs for each fabric in the cluster. KPI status includes:

- Guest Density
- Active user Count
- CPU Usage
- Memory Usage
- Storage Usage

In addition, a side bar will display the KPI summary index of the entire cluster.

Hardware

Hardware view provides the general information and specifications of the hardware of each of the fabric hosts. Information includes:

- Manufacturer and Model
- BIOS Version
- System Board Model
- Processor Type and Speed
- Memory Size and Type
- Core Temperature

Guests

The **Guest** section provides guest orchestration functions for the cluster. This is similar to guest management in the Administration portal. However, the view will cover the entire cluster instead of just an individual fabric. For more information on guest management, please review Guest Management.

Service Bus: Broker

The **Broker** tab displays the configuration and overall statistics of the HiveIO internal message bus.

Service Bus: Exchanges

The **Exchanges** tab provides the list of topics available within the HiveIO internal message bus. In addition, the user can select any item listed in exchanges and enable the *Listen* feature. This will allow the user to create a hook to the item and monitor the messages that are being transmitted on the bus.

Service Bus: Queues

The **Queues** tab provides a list of available queues in the HiveIO message bus.

Cluster Best Practice

Join a Cluster

Joining Hive Fabric to an existing cluster is a simple process. If a cluster does not yet exist, then two appliances can join together to create a new cluster.

1. On the left side Navigation Bar, under **Settings**, click on **Appliance**.
2. Enter a hostname for the appliance. This must be set or the appliance will not successfully join the cluster.
3. For the **Central Management Appliance** field, enter an IP address for an appliance within the cluster. This IP does not have to point the the designated Central Management Appliance, as it will be located through the cluster.
    - If the cluster does not exist, enter the IP address of the other appliance that will unite to establish a cluster. The IP entered will promote that appliance to a Central Management Appliance. The Central Management Appliance will list itself as the `localhost` on its appliance.
4. Set the appliance broker and gateway information as needed. Once all the required information has been completed, click on **Submit** to join the cluster.

Once the appliance successfully joins the cluster, then the **Clustered** status at the top of the window will be `True`. The number of members within the cluster will display in parenthesis.

> This process can not be replicated to join an appliance to another cluster while it is already a member of a cluster. The appliance must first be removed from its current cluster before it can establish a membership with new one.

Remove Appliance from a Cluster

During the typical life cycle, an appliance may become an unwanted member of the cluster and necessitate removal. It is also possible that an appliance needs to switch its cluster membership. However, appliances must first be removed from its current cluster membership before it can join a new cluster. This is integral to advanced cluster management, such as partitioning for multiple clusters.

Data migration is automatic, but the handling may vary based on the status of workload persistence. For non-persistent servers, other appliances will pick up the data. Persistent workloads perform a live migration from the existing cluster.

> Do not decouple the Central Management Appliance from the cluster.

The following steps remove the appliance from the cluster:

1. On the left side Navigation Bar, under **Settings**, click on **Administration**.
2. Set the appliance to **Enter Maintenance Mode**. This must be done before removing the Appliance from the cluster.
3. Click on the **Unjoin Cluster** button. A confirmation prompt will appear, stating that this action cannot be undone. Click on **OK** to advance and begin the release.

The removal process erases the local database. It also erases local entries from the Central Management Appliance. The removal process may take a few moments, depending on the size of the server. The appliance will reboot when everything is complete. For appliances that will be joining a new cluster, return to the Join a Cluster process.

> **Known Issue**
> If the appliance fails to restart automatically, a manual reboot must be performed to apply the cluster status change. Wait at least five minutes before applying the manual reboot to ensure that the cluster membership information updates correctly.

VM Broker

Once a guest is successfully deployed, users are ready to log in. The Hive Fabric provides access to the guest OS through either the broker or the gateway. Before users can begin to login and use their desktops, these brokering services must be established first. The Guest Connection Broker and Port Accessible Gateway portals are configured from the Appliance settings.

Any workstation that is on the same network as the guest pool will access guest desktops through the Broker. Remote users will access virtual desktops through the Gateway.

Broker

HiveIO includes a built-in guest brokering function. This feature can be enabled via the **Appliance Settings** secti on of the Administration portal. Once enabled, the Guest Connection Broker can be accessed by entering the URL as `https://<HiveIO-Host-IP>/broker`.

To login, simply enter the *UserName* and *Password*. Access role is based on the user's AD Group membership and the AD Group defined in the Guest Pool definition of the specified realm.

Once logged in, a list of available desktop resources will be presented to the user for each Guest Pool.

Accessing the Guest

1. In a web browser, type the server IP/broker address. Typically, this will resemble `https://<address here>/broker`.
2. Login with the user's AD username and password. Once access is granted, the user's guest assignments will display.
3. Select a guest and click on **Assign & Connect**. An RDP file will begin downloading. When the download finishes, the file is ready to launch. This will connect the user to the Guest Image.

Gateway

An RDP access gateway function is available in the HiveIO appliance. This feature can be enabled via the **Appliance Settings** section of the Administration portal. Once enabled, users will be able to access the guest VM through the internal port addressable gateway instead of connecting via the IP address guest. Brokering for the gateway will be accessed via the URL `https://<HioveIO-Host-IP>/remote`.

Accessing the Guest

1. In a web browser, type the server IP/broker address. Typically, this will resemble `https://<address here>/remote`.
2. Login with the user's AD username and password. Once access is granted, the user's guest assignments will display.
3. Select a guest and click on **Assign & Connect**. An RDP file will begin downloading. When the download finishes, the file is ready to launch. This will connect the user to the Guest Image.

> **Connectivity**
> Users who lose connectivity during VDI access through the gateway must log back in to the gateway to regain access to their desktop.