UNISYS

ClearPath Forward

Installation and Getting Started Guide

Release 4.0 and Higher

April 2017 8231 0913-005

Contents

Section 4. Configuring InfiniBand-Ethernet Gateway Switch

Section 5. Creating a Partition with a Unisys-Supplied OS

Section 7. Creating a Partition with a Customer-Supplied OS on a NEPP

Section 8. Integrating VMware Virtual Machines into the Fabric

Section 14. Backing Up and Restoring Fabric Management Platform, Fabric Manager, and Application Operating Environments on PEPPs

Section 15. Handling Events

Figures

Tables

Section 1
Introduction

1.1. Documentation Updates

This document contains all the information that was available at the time of publication. Changes identified after release of this document are included in problem list entry (PLE) 19168964. To obtain a copy of the PLE, contact your Unisys representative or access the current PLE from the Unisys Product Support website:

http://www.support.unisys.com/all/ple/19168964

Note: *If you are not logged into the Product Support site, you will be asked to do so.*

1.2. Audience

This document is intended for all users of the ClearPath Forward fabric, including

- System administrators
- Network administrators
- System operators
- Unisys service representatives

1.3. Purpose

This document

- Describes the architecture and various Fabric Manager user interface elements.
- Provides operational instructions to do the following:
  - Completing initial installation and configuration
  - Creating partitions
  - Configuring partition images
  - Starting and stopping partitions and platforms
  - Viewing, adding, and deleting platforms
  - Launching the platform management card (PMC) virtual console and partition image console
  - Hardening and unhardening application operating environments

- Backing up and restoring the Fabric Manager and enterprise partition platforms (EPPs)
- Handling events

1.4. Media and Documentation

The following documents are required or referenced in this document.

- ClearPath Forward Product Documentation website
- ClearPath Forward Information Center
- *ClearPath Forward Overview and Planning Guide* (8222 4528)
- *ClearPath Forward Administration and Operations Guide* (8222 4544)
- *ClearPath Forward Glossary* (8222 4502)

1.5. Understanding the Relationship Between System and Fabric

With ClearPath Forward™ technology, a "system" and a "fabric" are synonymous. A fabric is a computing environment in which applications can run in multiple operating environments or on multiple enterprise partition platforms or on both simultaneously. All platforms are interconnected by a high-speed InfiniBand Interconnect and Ethernet. All the devices and environments in the fabric function as a single entity and are managed by the Fabric Manager. In this way, all of the components in the fabric appear as a single system.

Contrarily, "system" is not synonymous with "platform" (nor with its synonyms "Intel platform" and "enterprise partition platform"). A platform is a single physical computer. A system (fabric) almost always consists of at least two platforms.

To understand more about the ClearPath Forward fabric, see the 1.6 Summary of the Fabric Architecture section.

1.6. Summary of the Fabric Architecture

The following figure shows the major components of the ClearPath Forward fabric, which are defined in the table that follows:

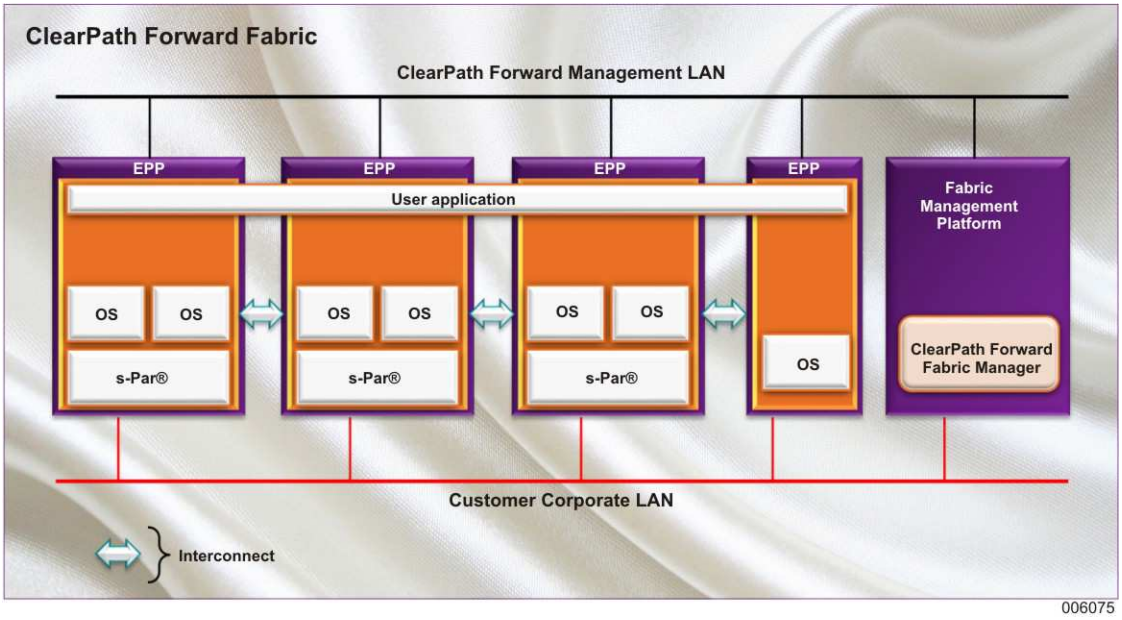


Table 1–1. Definitions of Components in the Fabric

Component	Definition
ClearPath Forward fabric	A fabric computing environment from Unisys Corporation in which applications can run in multiple operating environments and/or on multiple Intel computers (referred to as enterprise partition platforms), all interconnected by a high-speed Interconnect. All devices and environments in the fabric are managed by a single user interface (called the Fabric Manager) and can function as a single entity. ***Note:*** *A ClearPath Forward fabric is also referred to as a "ClearPath Forward system."*
ClearPath Forward Management LAN	An Ethernet LAN for managing the enterprise partition platforms and partitions within the fabric. It enables the Fabric Management Platform to communicate with the enterprise partition platforms and partitions.
Customer corporate LAN	Your enterprise's Ethernet intranet. It allows your enterprise to communicate with each enterprise partition platform, with the Fabric Management Platform, and with other computers in your enterprise.

Table 1–1. Definitions of Components in the Fabric (cont.)

Component	Definition
EPP Enterprise partition platform	The computer that is the basic building block of a ClearPath Forward fabric. An EPP includes the Intel-based hardware, all partition images running on the hardware, platform services, and all of the software. EPPs can be partitionable or nonpartitionable. In the case of partitionable enterprise partition platforms, the EPP also includes s-Par® firmware. ***Notes:*** • *If the partitionable enterprise partition platform includes the optional DVD drive, it is for Unisys maintenance use only; customers should not use it.* • *The optional DVD drive in the nonpartitionable enterprise partition platform is available for customer use.*
Fabric Management Platform	A computer equipped with Intel Xeon instruction processors that runs the Linux operating system and communicates with the enterprise partition platforms over the ClearPath Forward Management LAN. It provides the web browser-based management user interface to the fabric, called the Fabric Manager.
Fabric Manager	Management software running on the Fabric Management Platform. It provides monitoring information and manages all of the components in the fabric. It enables you to alter the configuration of platforms in the fabric with ease, resizing operating environments and even reprovisioning an entire server with alternate operating environments and software stacks, based on preexisting partition templates called blueprints.
Interconnect	The hardware, software, and firmware that enable enterprise partition platforms to communicate with one another and support applications that span multiple partitions, platforms, and operating systems. The primary components of the Interconnect include • High-speed switched fabric communications hardware • TCP/IP communications protocols • Unisys Secure Partitioning (s-Par®) firmware • Unisys Interconnect firmware and fabric management software for installation and runtime deployment
Operating systems	The operating systems providing the partition operating environments. The following operating systems are supported in the fabric: Windows Server, SUSE Linux, RedHat Linux.
Partitions	A portion of a computer that is supported by its own dedicated hardware resources (such as processors, memory, and input/output) and runs its own operating environment (operating system and software stack). Unisys Secure Partitioning (s-Par®) provides the capability to support multiple partitions on a single hardware platform. In the figure, each operating system (OS) represents a partition.

Table 1–1. Definitions of Components in the Fabric (cont.)

Component	Definition
s-Par® Unisys Secure Partitioning	Unisys firmware that provides the capability to run multiple operating environments (operating systems) concurrently on the same Intel platform. Each operating environment has dedicated hardware resources (processors, memory, and I/O) that isolate one operating environment from another and ensure that a failure of one environment does not affect another.
User application	All of the software that, together, solves a particular problem or accomplishes a particular task that the enterprise wishes to solve or accomplish. With the ClearPath Forward fabric, an application can span operating system and hardware platform boundaries. Such an application is sometimes referred to as a hybrid application, consolidated application, enterprise application, or distributed application.

1.7. List of Fabric Manager Actions

The following list describes actions you are able to perform while using the Fabric Manager user interface. For complete information on these Fabric Manager capabilities, see the *ClearPath Forward Administration and Operations Guide*.

- Getting started with the user interface
  - Fabric Manager
    - Logging into the Fabric Manager
    - Selecting a preferred language in the Fabric Manager
  - Viewing software update information
  - Fabric Management Platform
    - Logging into the Fabric Management Platform
    - Changing a user's password
    - Viewing Fabric Manager server health
    - Viewing Fabric Manager high availability status
- Managing Fabric Manager users and roles
  - Migrating a user to LDAP
  - Creating a user
  - Creating a group
  - Adding a user to a group
  - Creating a role
  - Modifying permissions to a role
  - Mapping a group to a role
  - Resetting a user's password

  - Changing a user's password
  - Setting-up a user's password lockout preferences
  - Unlocking a user
  - Enabling a user
  - Disabling a user
  - Deleting a user from a group
  - Deleting a user and a group
  - Connecting to the customer-deployed LDAP service
- Managing the fabric as a whole
  - Editing the system attributes
  - Setting the fabric under maintenance mode
  - Setting up Call Home
    - Viewing the Call Home configuration
    - Configuring Call Home
    - Setting up the Call Home schedule
    - Verifying the Call Home configuration
    - Managing Call Home email notifications
  - Adding a platform to the fabric
- Managing a secure fabric
  - Adding a secure fabric
  - Associating a PEPP partition with a secure fabric during commissioning
  - Associating a PEPP partition with a secure fabric after commissioning
    - Associating a partition image to a secure fabric
    - Associating a Windows operating environment with a secure fabric
    - Associating a SUSE LINUX operating environment with a secure fabric
    - Associating a Red Hat Enterprise Linux operating environment with a secure fabric
  - Associating a NEPP partition with a secure fabric
    - Associating a Windows operating environment with a secure fabric
    - Associating a SUSE LINUX operating environment with a secure fabric
    - Associating a Red Hat Enterprise Linux operating environment with a secure fabric
    - Associating a VMware operating environment with a secure fabric
  - Choosing from predefined secure fabrics for a NEPP-only fabric environment

  - Disassociating an operating environment from a secure fabric
    - Removing a virtual IP over InfiniBand (IPoIB) interface
    - Disassociating a partition image from a secure fabric
    - Determining mapping of a Subnet Tag (PKEY) to a virtual IPoIB interface
    - Determining mapping of a virtual IPoIB interface to a physical port
  - Viewing a secure fabric summary
  - Editing a secure fabric
  - Deleting a secure fabric
- Managing power for each platform
  - Powering-on a platform
  - Performing a soft shutdown on a platform
  - Powering-off a platform
  - Performing a hard restart on a platform
  - Performing a soft restart on a platform
  - Performing a power cycle on platform
  - Performing a force dump on a platform
  - Shutting down the entire fabric
  - Restarting the fabric
- Managing platforms
  - Viewing the platform summary
  - Viewing configuration information of a platform
  - Editing a platform's name and description
  - Launching the Platform Management Card (PMC) virtual console
  - Deleting a partitionable EPP
  - Deleting a nonpartitionable EPP
  - Configuring attributes on physical and logical NIC ports
    - Enabling NIC port sharing on a platform
    - Disabling NIC port sharing on a platform
- Managing s-Par firmware
  - Viewing s-Par firmware details
  - Uploading s-Par firmware
  - Upgrading s-Par firmware
  - Deleting s-Par firmware from the platform
  - Deleting s-Par firmware from the Fabric Management Platform

- Managing blueprints and gold images
  - Managing blueprints
    - Viewing blueprint details
    - Adding a blueprint
    - Deleting a blueprint
    - Filtering blueprints
  - Managing gold images
    - Viewing gold image details
    - Adding a gold image
    - Deleting a gold image
    - Filtering gold images
- Managing partitions
  - Commissioning a partition image
    - Selecting a blueprint
    - Setting up basic partition information
    - Providing configuration details
    - Selecting I/O ports
    - Associating secure fabrics with a partition image
    - Selecting boot LUN and data LUNs
    - Viewing the summary
  - Viewing the partition summary
  - Accessing the partition image console (Partition Desktop)
  - Changing the user/password of the partition image console
  - Deleting the user/password of the partition image console
  - Starting and shutting down the partition images
    - Starting a partition image
    - Performing a soft restart of a partition image
    - Performing a hard restart of a partition image
    - Gracefully shutting down a partition image
    - Shutting down multiple partition images
    - Performing a force halt of a partition image
    - Performing force dump on a partition image
  - Enabling a partition image
  - Disabling a partition image

  - Adding multiple operating system images to a partition chassis
  - Editing a partition image
  - Resizing a partition image
  - Decommissioning a partition image
- Managing switches
  - Adding a switch
  - Viewing switch details
  - Editing switch details
  - Launching the switch console
  - Deleting a switch
- Managing events
  - Viewing events
  - Filtering events
  - Accepting events
  - Closing events
  - Re-opening events
  - Re-sending failed Call Home events
  - Editing the event log retention period
- Managing high availability for the Fabric Manager
  - Accessing the Fabric Manager cluster
  - Managing the Fabric Manager cluster
    - Connecting to a specific Fabric Management Platform
    - Identifying all access points to a cluster
    - Managing the cluster service
    - Monitoring data replication status
    - Managing synchronization of files
    - Connecting to the active Fabric Management Platform and monitoring the cluster node status
    - Performing routine maintenance and updates
    - Viewing current failure status and limits for the Fabric Manager resources
    - Cleaning up and manually resetting a resource failcount
    - Manually migrating the Fabric Manager workload

- Managing security
  - Using the Unisys Stealth solution
- Managing time on all platforms in the fabric
  - Setting time for your platform
- Managing Fabric Management Platform and enterprise partition platform dumps
  - Managing Fabric Management Platform dumps
    - Generating Fabric Management Platform dumps
    - Downloading a Fabric Management Platform dump file
    - Deleting a Fabric Management Platform dump file
  - Managing enterprise partition platform dumps
    - Generating enterprise partition platform dumps
    - Downloading an enterprise partition platform dump file
    - Deleting an enterprise partition platform dump file
- Troubleshooting
  - Fabric Management Platform and Partition Desktop problems
  - Fabric Manager user problems
  - Partition image problems
  - Commissioning failures
  - Dump file problems
  - Info pane problems
  - Fabric Manager service problems
  - Fabric Manager high availability configurations
  - Reporting problems to Unisys

1.8. List of ClearPath Forward Fabric Management Platform Manager Actions

The following list describes actions you are able to perform while using the ClearPath Forward Fabric Management Platform Manager web-based user interface (FMP Manager user interface). For complete information on these ClearPath Forward Fabric Management Platform Manager capabilities, see the associated help.

- Getting started with the user interface
  - Logging into the Fabric Management Platform Manager
  - Changing a user's password
  - Selecting a preferred language in the FMP Manager

- Configuring Cluster
  - Providing cluster details
  - Providing fencing details
  - Providing access point details
  - Reviewing the summary
- Managing Cluster Nodes and Services
  - Viewing cluster summary
  - Managing nodes and resources
  - Managing cluster services
- Managing Fencing
  - Viewing fencing details
  - Editing fencing details
- Managing File Synchronization
  - Enabling file synchronization service
  - Disabling file synchronization service
  - Adding or removing files for synchronization
- Managing Storage
  - Viewing file system utilization summary
  - Increasing file system size
- Managing Logs
  - Searching and viewing critical FFM system logs
  - Downloading the system logs
  - Viewing cluster audit logs
  - Viewing and fixing replication alert issues
- Managing backups and upgrading FMP
  - Backup FFM database information
  - Backup and upgrade FMP system information
- Managing Users
  - Adding a user
  - Deleting a user
  - Modifying a user
- Managing Access to FMP Manager
  - Enabling access to ClearPath Forward FMP Manager through Corporate LAN
  - Disabling access to ClearPath Forward FMP Manager through Corporate LAN

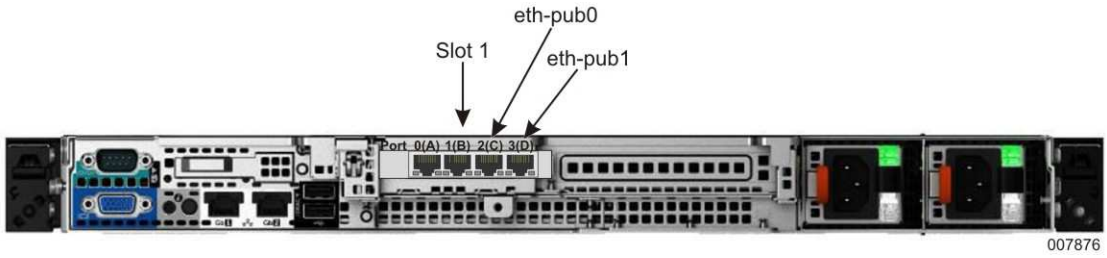
Section 2

Completing Initial Installation and Configuration

When the Unisys representative completes initial hardware installation and software configuration, the customer performs the following tasks to complete installation and configuration.

2.1. Cabling the Fabric Management Platform to Your Network

At the rear of the Fabric Management Platform (FMP), locate port C and port D on the quad port NIC (PCIe slot 1), and cable the FMP to your network.



Note: *PCIe slot 1 port C on is named* eth-pub0*, and PCIe slot 1 port D is named* eth-pub1*.*

2.2. Cabling Enterprise Partition Platforms to Your Network

For nonpartitionable enterprise partition platforms (EPPs), connect any of the NIC ports to your network and any of the fibre channel HBA ports to your storage subsystem.

For a partitionable EPP,

1. Using the Fabric Manager user interface, view the partition summary of a particular partition on the partitionable EPP.
2. Click **View Port Info** to display a logical diagram of the NIC and HBA ports allocated to the partition.
3. Identify the physical location of the ports, and then connect the ports appropriately to your network.

   Note: *If multiple ports are allocated to your partition, be sure to cable all described ports to your network.*

The following sample configurations show various mixes of ports and, based on orientation of the installed card, the relationship of the ports to the installed location.

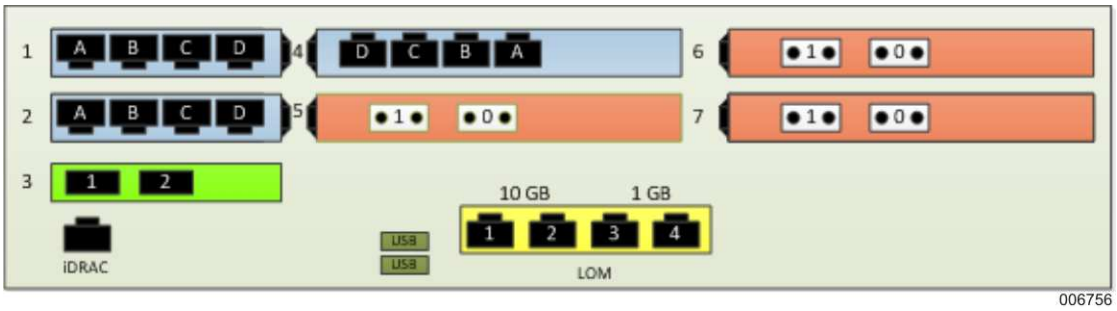


Figure 2–1. Example of Physical Location of Ports for 2-Socket EPP with 3 Quad-Port 1GbE NICs and 3 Dual-Port 8Gb Fibre Channel HBAs

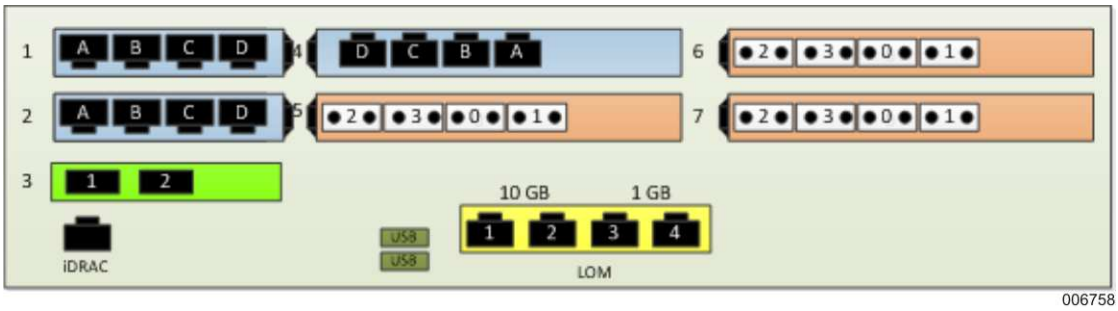


Figure 2–2. Example of Physical Location of Ports for 2-Socket EPP with 3 Quad-Port 1GbE NICs and 3 Quad-Port 8Gb Fibre Channel HBAs

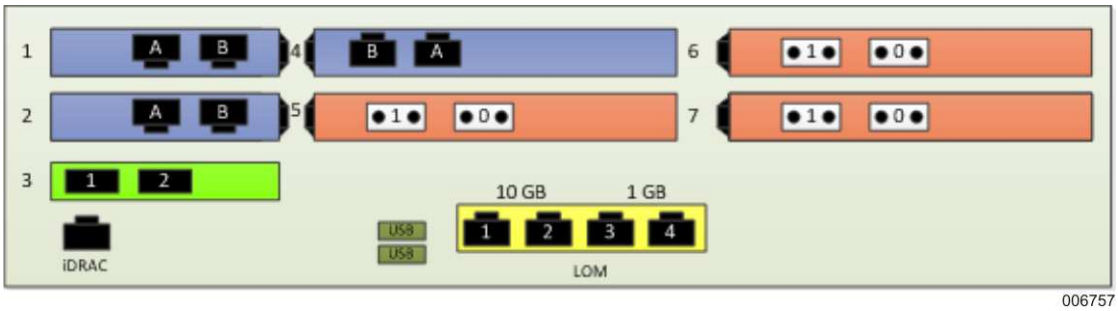


Figure 2–3. Example of Physical Location of Ports for 2-Socket EPP with 3 Dual-Port 10GbE NICs and 3 Dual-Port 8Gb Fibre Channel HBAs

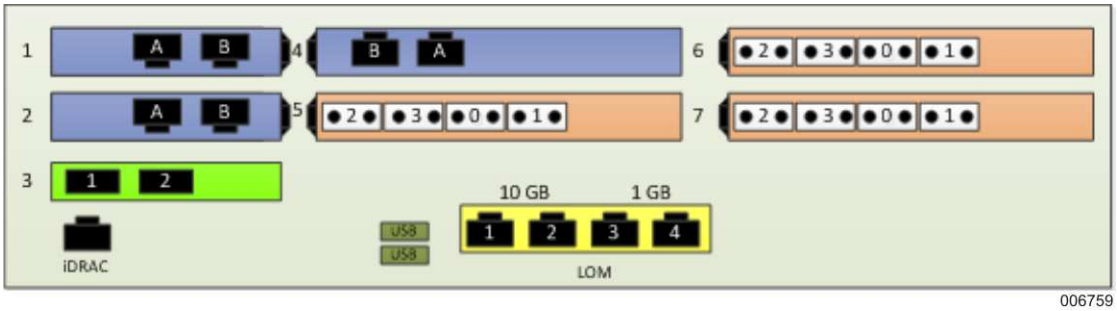


Figure 2–4. Example of Physical Location of Ports for 2-Socket EPP with 3 Dual-Port 10GbE NICs and 3 Quad-Port 8Gb Fibre Channel HBAs

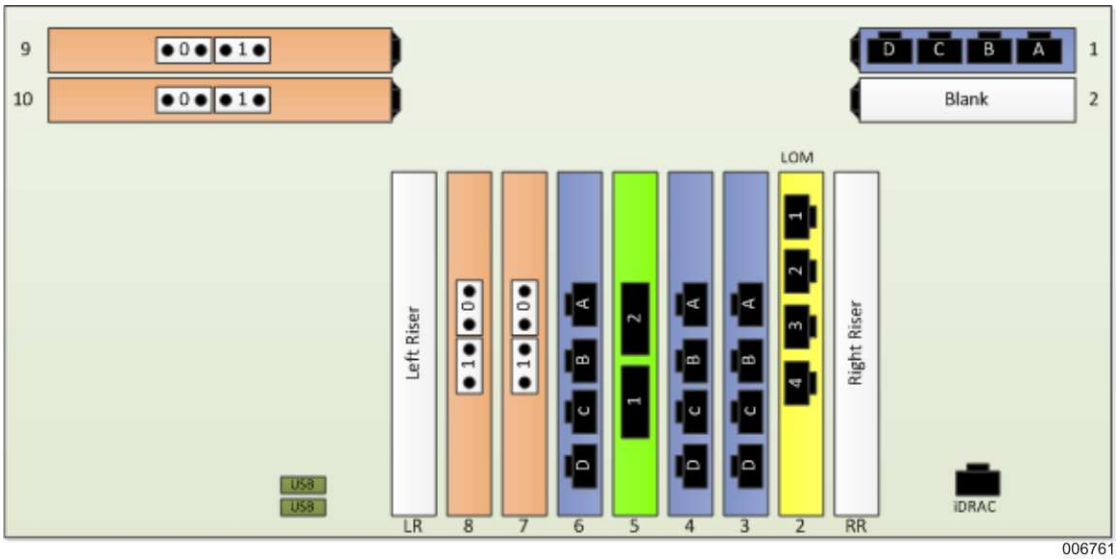


Figure 2–5. Example of Physical Location of Ports for 4-Socket EPP with 4 Quad-Port 1GbE NICs and 4 Dual-Port 8Gb Fibre Channel HBAs

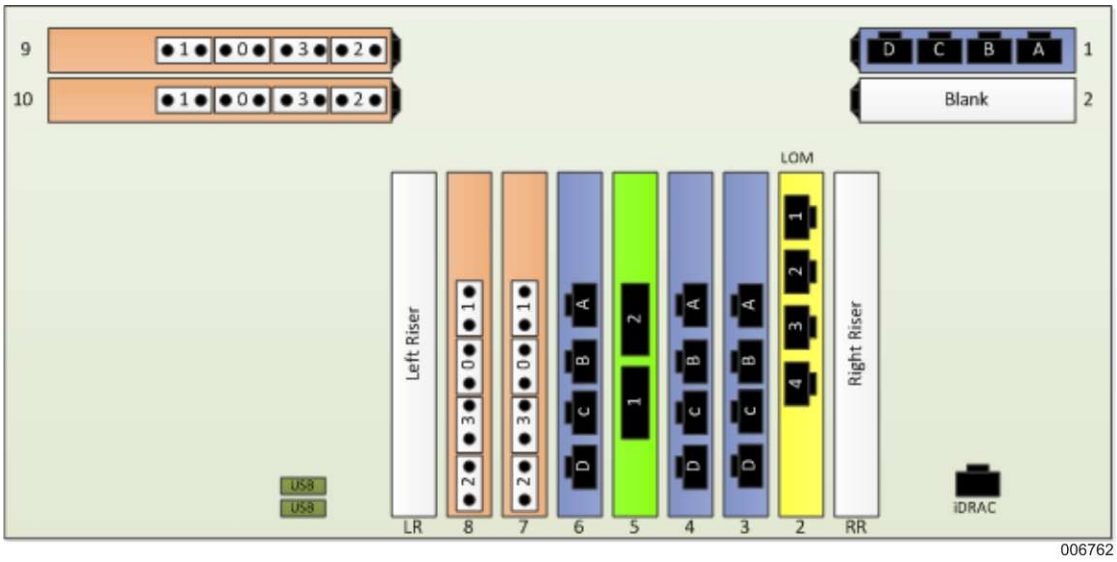


Figure 2–6. Example of Physical Location of Ports for 4-Socket EPP with 4 Quad-Port 1GbE NICs and 4 Quad-Port 8Gb Fibre Channel HBAs

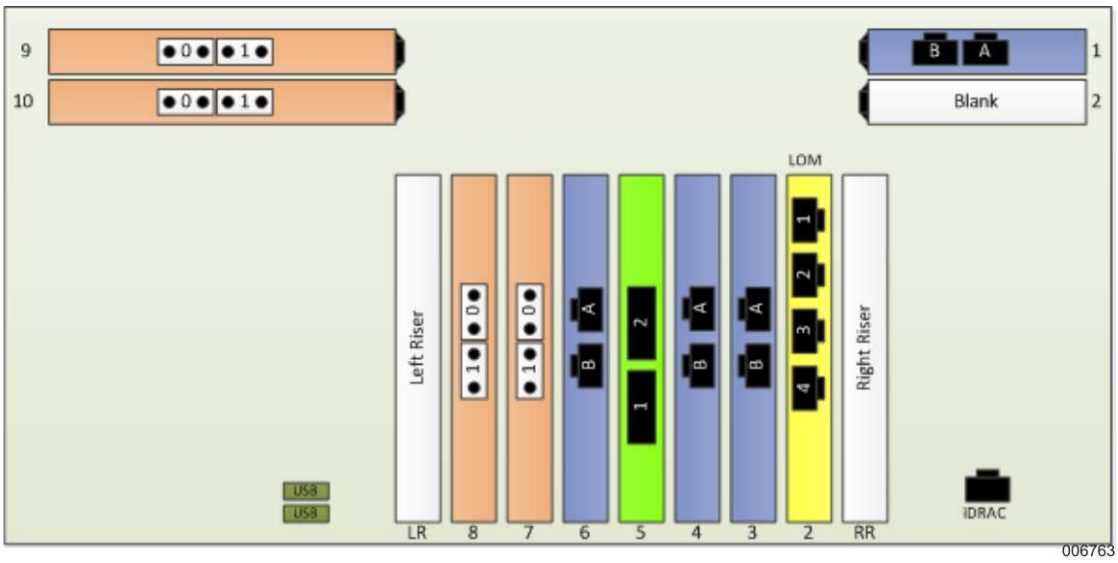


Figure 2–7. Example of Physical Location of Ports for 4-Socket EPP with 4 Dual-Port 10GbE NICs and 4 Dual-Port 8Gb Fibre Channel HBAs

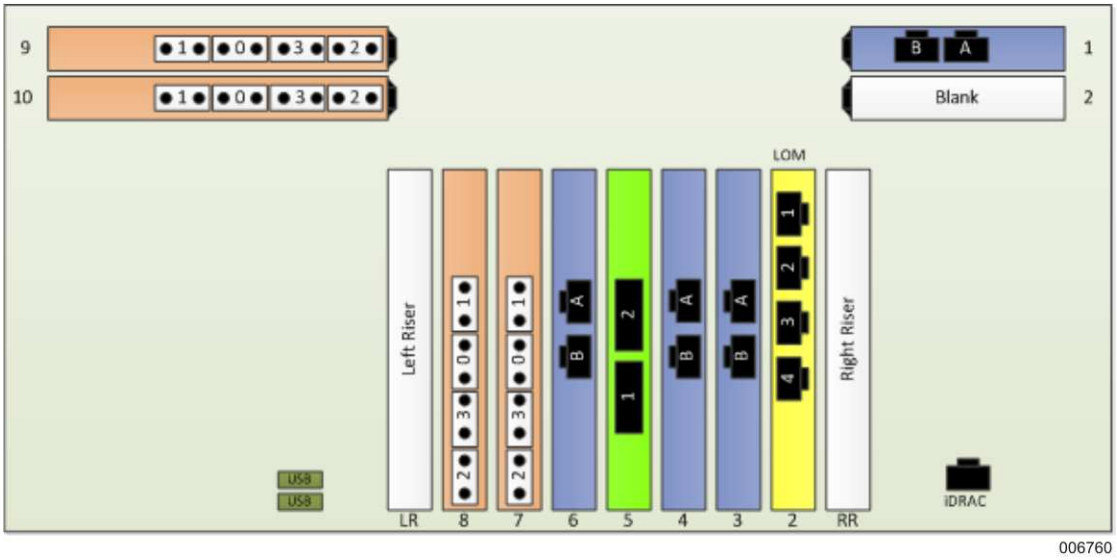


Figure 2–8. Example of Physical Location of Ports for 4-Socket EPP with 4 Dual-Port 10GbE NICs and 4 Quad-Port 8Gb Fibre Channel HBAs

2.3. Updating the Fabric Manager Certificate

> **Caution**
>
> The Fabric Manager user interface needs a valid certificate in order to start. You must complete the entire procedure before restarting the Fabric Manager.

The Fabric Management Platform is shipped with a default RSA keypair and self-signed certificate in order for initial operations to be secured by Secure Sockets Layer (SSL)/Transport Layer Security (TLS). For best security practices, Unisys recommends that you generate a new RSA keypair and request and install a Certificate Authority (CA) signed certificate to replace the defaults that are shipped with the platform.

Note: *In the following procedures, # represents a command prompt. You do not need to type it.*

Generating a New RSA Keypair and Certificate Authority-Signed Certificate

To update Fabric Manager with a new RSA keypair and Certificate Authority-signed certificate, refer to the following instructions:

1. Launch a virtual console from the Fabric Management Platform console and log in as root.
2. Navigate to the "ssl" directory by entering the following command:

   ```
   # cd /usr/local/ffm/apache2/conf/ssl
   ```

3. Enter the following command to set the environment variable to set the Domain Name System (DNS) name in the certificate.

   Note: *Angular brackets (< >) are used to represent variable data. Do not include them in the following command.*

```
# export ALTNAME=DNS:<hostname>,IP:<FMP_IP>,DNS:localhost,IP:127.0.0.1
```

   where <hostname> is the fully qualified host name of the Fabric Management Platform and <FMP_IP> is the IP address of the Fabric Management Platform.

   The IP address of the Fabric Management Platform depends on what IP address is used to access the Fabric Management Platform remotely. See Table 2–1 for the available options.

Table 2–1. Fabric Management Platform IP Addresses

Component	IP Address
Customer corporate LAN (public LAN)	**Static:** • For FMP1 and FMP2, the two IP addresses you previously chose for connection to your management network environment. ***Note:*** *In a high-availability (HA) environment, both FMPs have respective unique static IP addresses.* **Floating:** • For FMP1 and FMP2, the single IP address you previously chose for when a high-availability (HA) cluster is created.

Table 2–1. Fabric Management Platform IP Addresses (cont.)

Component	IP Address
ClearPath Forward Management LAN (FM LAN)	**Static:** • FMP1: 172.29.254.252 • FMP2: 172.29.253.252 **Floating:** • FMP1 and FMP2: 172.29.254.60 ***Note:*** *The FM LAN IP address subnet (172.29) can be modified by the Fabric Manager administrator, however, the second octet (254.252, 253.252 and 254.60) remains constant. For example, if the FM LAN IP address subnet would change from 172.29 to 172.80, then the static and floating FM LAN IP addresses would change to 172.80.254.252, 172.80.253.252 and 172.80.254.60.*

4. Enter the following command to create the key (localhost.key) and a certificate request (localhost.pem):

```
# openssl req -newkey rsa:2048 -keyout localhost.key -out localhost.pem -config /etc/ssl/
ffm_openssl.cnf -extensions v3_req
```

   The two files "localhost.key" and "localhost.pem" are created.

   Notes:

   - *If this step required the entry of a passphrase, the passphrase must be removed in order for the key to be used by an autostarted service. To remove the passphrase, continue to step 5.*
   - *If this step did not require the entry of a passphrase, continue to step 6.*
   - *If you need to regenerate the public and private keys, use the above command. If you wish to only renew the certificate, use the following command and then continue to step 6:*

   ```
   # openssl x509 -x509toreq -in localhost.crt -out localhost.pem -signkey localhost.key
   ```

5. Enter the following commands to remove the passphrase from the key:

   - `# mv localhost.key localhost.key.org`
   - `# openssl rsa -in localhost.key.org -out localhost.key`

   Note: *Enter the passphrase from step 4 when prompted.*

6. Submit the localhost.pem file to an appropriate Certificate Authority, which will then return a localhost.crt file (that is, a certificate).

Note: *The certificate must be in PEM format in order for step 7 and step 10 to work. If the certificate is not in PEM format, use the openssl x509 command to convert the certificate to PEM format.*

7. To create the certificate store for local access, enter the following command to export the certificate received from the Certificate Authority created in step 6 to PKCS12 format:

```
# openssl pkcs12 -export -out localhost.pfx -inkey localhost.key -in localhost.crt
```

   The localhost.pfx file is created.

   Note: *Do not enter an export password when prompted.*

8. Enter the following command to verify whether the files have been created:

```
# ls –l
```

   The three files "localhost.key", "localhost.crt", and "localhost.pfx" are displayed with the date and time of that particular day.

9. To create the certificate store for remote web services, enter the following command to export the certificate received from the Certificate Authority created in step 6 to PKCS12 format:

```
# openssl pkcs12 -export -out ffm_fmws.pfx -inkey localhost.key -in localhost.crt
```

   The ffm_fmws.pfx file is created.

   Note: *Ensure that an export password is entered when prompted. This is required in step 10.*

10. Import the PKCS12 file (ffm_fmws.pfx) to the jetty keystore as follows:

```
# keytool -importkeystore -srckeystore ffm_fmws.pfx -srcstoretype PKCS12 -destkeystore ffm_fmws_keystore.jks
```

   Notes:

   - *You will be asked to enter a keystore password. Please use the same password in step 14.*
   - *If this is for a redundant FMP configuration (HA), ensure that this certificate is installed in both FMPs in the same directory. You may need to copy the file manually to both FMPs and perform steps 11 through 15 before restarting Fabric Manager services.*

11. Navigate to the "etc" directory by entering the following command:

```
# cd /usr/local/ffm/jetty/etc
```

12. Move the keystore file to /usr/local/ffm/jetty/etc as follows:

```
# mv /usr/local/ffm/apache2/conf/ssl/ffm_fmws_keystore.jks ffm_fmws_keystore.jks
```

13. Navigate to the "lib" directory by entering the following command:

```
# cd /usr/local/ffm/jetty/lib
```

14. Generate the OBF password for the password provided in step 10 for jetty keystore.

   Note: *Angular brackets (< >) are used to represent variable data. Do not include them in the following command.*

```
# java -cp jetty-util-7.6.8.v20121106.jar
org.eclipse.jetty.util.security.Password me <keystore password>
```

where <keystore password> is the same keystore password entered in step 10.

The output of the command displays the password in OBF, MD5, and CRYPT format as follows:

- `OBF:19iy19j019j219j419j619j8`
- `MD5:e10adc3949ba59abbe56e057f20f883e`
- `CRYPT:meYmEekhPnz3w`

Note: *This procedure is currently making use of the OBF format. Fabric Manager uses the OBF format only for SSL certificates in a jetty configuration.*

15. Copy and paste the OBF format into the jetty-ssl.xml file (/usr/local/ffm/jetty/etc/jetty-ssl.xml) for the ssl context factory configuration with ID "sslContextFactoryClientAuth" as follows.

    Note: *For this particular case, include the angular brackets (<>) in each command line.*

```
<New id="sslContextFactoryClientAuth" class="org.eclipse.jetty.http.ssl.SslContextFactory">
<Set name="KeyStorePassword"> OBF:19iy19j019j219j419j619j8</Set>
<Set name="KeyManagerPassword"> OBF:19iy19j019j219j419j619j8</Set>
<Set name="TrustStore"><Property name="jetty.home" default="." />/etc/
ffm_fmws_keystore.jks/etc/ffm_fmws_keystore.jks</Set>
<Set name="TrustStorePassword"> OBF:19iy19j019j219j419j619j8</Set>
```

16. If you are configuring mutual authentication for web services at this time, do not restart Fabric Manager services yet—proceed to the "Adding Certificate Authorities for Mutual Authentication" subsection, and then restart Fabric Manager services at the end of that subsection.

17. Enter the following command to restart the Fabric Manager services:

    ```
    # rcffmservices restart
    ```

    The Fabric Manager services are restarted.

Generating a New RSA Keypair and Self-Signed Certificate for Internal Deployment and Testing

> **Caution**
>
> The Fabric Manager user interface needs a valid certificate in order to start. You must complete the entire procedure before restarting the Fabric Manager.

For best security practices, Unisys recommends that you generate a new RSA keypair and request and install a Certificate Authority (CA) signed certificate to replace the defaults that are shipped with the platform. However, you may request and install a self-signed certificate for internal deployment and testing. The self-signed certificate should be

replaced with a Certificate Authority-signed certificate before any production deployment occurs. See "Generating a New RSA Keypair and Certificate Authority-Signed Certificate" at the beginning of this section to replace the certificate.

To update Fabric Manager with a new RSA keypair and self-signed certificate, refer to the following instructions:

1. Launch a virtual console from the Fabric Management Platform console and log in as root.
2. Navigate to the "ssl" directory by entering the following command:

   ```
   # cd /usr/local/ffm/apache2/conf/ssl
   ```

3. Enter the following command to set the environment variable to set the DNS name in the certificate.

   Note: *Angular brackets (< >) are used to represent variable data. Do not include them in the following command.*

   ```
   # export ALTNAME=DNS:<hostname>,IP:<FMP_IP>,DNS:localhost,IP:127.0.0.1
   ```

   where <hostname> is the fully qualified host name of the Fabric Management Platform and <FMP_IP> is the IP address of the Fabric Management Platform.

   The IP address of the Fabric Management Platform depends on what IP address is used to access the Fabric Management Platform remotely. See Table 2–1 for the available options.

4. Enter the following command to create the key (localhost.key) and a certificate request (localhost.crt):

   ```
   # openssl req -x509 -sha512 -newkey rsa:2048 -keyout localhost.key -out localhost.crt -config /etc/
   ssl/ffm_openssl.cnf -extensions v3_req
   ```

   The two files "localhost.key" and "localhost.crt" are created.

   Notes:

   - *If this step required the entry of a passphrase, the passphrase must be removed in order for the key to be used by an autostarted service. To remove the passphrase, continue to step 5.*
   - *If this step did not require the entry of a passphrase, continue to step 6.*

5. Enter the following commands to remove the passphrase from the key:

   - `# mv localhost.key localhost.key.org`
   - `# openssl rsa -in localhost.key.org -out localhost.key`

   Note: *Enter the passphrase from step 4 when prompted.*

6. To create the certificate store for remote web services, enter the following command to export the certificate received from the self-signed certificate to PKCS12 format:

   ```
   # openssl pkcs12 -export -out ffm_fmws.pfx -inkey localhost.key -in localhost.crt
   ```

   The ffm_fmws.pfx file is created.

   Note: *Ensure that an export password is entered when prompted. This is required in step 8.*

7. Import the source keystore to a keystore of type PKCS12:

```
# keytool -importkeystore -srckeystore ffm_fmws.pfx -srcstoretype PKCS12
```

8. Import the PKCS12 file (ffm_fmws.pfx) to the jetty keystore as follows:

```
# keytool -importkeystore -srckeystore ffm_fmws.pfx -srcstoretype PKCS12 -destkeystore ffm_fmws_keystore.jks
```

Notes:

- *You will be asked to enter a keystore password. Please use the same password in step 12.*
- *If this is for a redundant FMP configuration (HA), ensure that this certificate is installed in both FMPs in the same directory. You may need to copy the file manually to both FMPs and perform steps 9 through 13 before restarting Fabric Manager services.*

9. Navigate to the "etc" directory by entering the following command:

```
# cd /usr/local/ffm/jetty/etc
```

10. Move the keystore file to /usr/local/ffm/jetty/lib as follows:

```
# cp /usr/local/ffm/apache2/conf/ssl/ffm_fmws_keystore.jks .
```

11. Navigate to the "lib" directory by entering the following command:

```
# cd /usr/local/ffm/jetty/lib
```

12. Generate the OBF password for the password provided in step 8 for jetty keystore.

Note: *Angular brackets (< >) are used to represent variable data. Do not include them in the following command.*

```
# java -cp jetty-util-7.6.8.v20121106.jar
org.eclipse.jetty.util.security.Password me <keystore password>
```

where <keystore password> is the same keystore password entered in step 8.

The output of the command displays the password in OBF format as follows:

```
OBF:1x7w1ta81vup1vul1ta61x8y
```

Note: *Fabric Manager uses the OBF format only for SSL certificates in a jetty configuration.*

13. Copy and paste the OBF format into the jetty-ssl.xml file (/usr/local/ffm/jetty/etc/jetty-ssl.xml) for the ssl context factory configuration with ID "sslContextFactoryClientAuth" as follows.

Note: *For this particular case, include the angular brackets (<>) in each command line.*

```
<New id="sslContextFactoryClientAuth" class="org.eclipse.jetty.http.ssl.SslContextFactory">
<Set name="KeyStorePassword"> OBF:1x7w1ta81vup1vul1ta61x8y</Set>
<Set name="KeyManagerPassword"> OBF:1x7w1ta81vup1vul1ta61x8y</Set>
<Set name="TrustStore"><Property name="jetty.home" default="." />/etc/
ffm_fmws_keystore.jks/etc/ffm_fmws_keystore.jks</Set>
<Set name="TrustStorePassword"> OBF:1x7w1ta81vup1vul1ta61x8y</Set>
```

14. If you are configuring mutual authentication for web services at this time, do not restart Fabric Manager services yet—proceed to the "Adding Certificate Authorities for Mutual Authentication" subsection, and then restart Fabric Manager services at the end of that subsection.
15. Enter the following command to restart the Fabric Manager services:

    ```
    # rcffmservices restart
    ```

    The Fabric Manager services are restarted.

2.4. Mutual Authentication for Web Services Security

ClearPath Forward Management Web Services Security Model

The client software that integrates programmatically with the ClearPath Forward Management Web Services (FMWS) through its Application Programming Interface (API), must be authenticated for each individual request. The authentication is achieved using the Hypertext Transfer Protocol (HTTP) basic authentication and mutual authentication (two-way authentication) using certificates. The communications protocol between the client and FMWS is Hypertext Transfer Protocol Secure (HTTPS) using Secure Sockets Layer (SSL) encryption. This is supported by two-way certificates for the Fabric Manager user interface and client software sides of communication. To configure the Fabric Manager server to accept requests from a client machine or application, the following information is required:

- The client's DNS server
- Any certificates from Certificate Authorities that were used in generating client certificates

Authentication

The Base64–encoded string that contains a user name and password needs to be sent in the "Authorization" HTTP header.

Mutual Authentication

Mutual authentication or two-way authentication (sometimes written as 2WAY authentication) refers to two parties authenticating each other at the same time. When mutual authentication using certificates is used, the server requests the client to provide a certificate in addition to the server certificate issued to the client.

Adding Certificate Authorities for Mutual Authentication

The Fabric Manager administrator should import the Certificate Authority (CA) certificates to be trusted into the server trust store. Refer to the following instructions to do this process:

1. Launch a virtual console from the Fabric Management Platform console and log in as root.
2. Copy the CA certificates from the Fabric Management Platform to the following directory:

   ```
   /usr/local/ffm/jetty/etc
   ```

3. Import each of the root and intermediate CA certificates to the Java keystore by entering the following command.

   Note: *Angular brackets (< >) are used to represent variable data. Do not include them in the following command.*

   ```
   # keytool -import -trustcacerts -alias <alias_name> -file <certificate_name> -keystore ffm_fmws_keystore.jks
   ```

   where <alias_name> is the name used to differentiate between two certificates (for example, fmws, CHRFWD, FwdInt, etc.) and <certificate_name> is the name of the certificate file (for example, localhost.cer, keystore.crt, or ffm_fmws.pfx).

   Note: *Repeat this step for all of the intermediate CA certificates for the primary certificate.*

4. The Fabric Manager services have to be restarted after all the CA certificates are imported. Enter the following command to restart the Fabric Manager services:

   ```
   # rcffmservices restart
   ```

   The Fabric Manager services are restarted.

2.5. Implementing Security Best Practices

The ClearPath Forward fabric adopts a multi-faceted approach to security, and ClearPath Forward architecture implements an increased level of security in multiple ways. For more information, refer to the *ClearPath Forward Product Documentation Web Site* or the *ClearPath Forward Overview and Planning Guide* (8222 4528).

Unisys recommends that you also review the *ClearPath Forward Security Guide* (8230 6614) which describes the best practices Unisys recommends for fabric environments. Review these best practices and implement them according to your site security policies.

2.6. What To Do Next

If desired, create one or more secure fabrics. For more information, see Section 3, Creating a Secure Fabric.

If you want bare metal servers and virtual machines (VMs) in your Ethernet customer corporate LAN environment to participate as members of a secure fabric, configure the optional InfiniBand-Ethernet gateway switch. For more information, see

Section 4, Configuring InfiniBand-Ethernet Gateway Switch.

For partitionable enterprise partition platforms, install operating systems to a partition on the partitionable enterprise partition platform. Depending on the source for your operating system images, see Section 5, Creating a Partition with a Unisys-Supplied OS, or Section 6, Creating a Partition with a Customer-Supplied OS on a PEPP.

For nonpartitionable enterprise partition platforms, install one of the supported customer-supplied operating systems. For more information, see Section 7, Creating a Partition with a Customer-Supplied OS on a NEPP.

The Fabric Manager database and configuration files should be backed up after completing initial configuration and whenever the configuration is changed. For more information, see 14.2 Fabric Manager Backup.

Section 3
Creating a Secure Fabric

This section provides information about how to get started creating a secure fabric.

3.1. Secure Fabrics

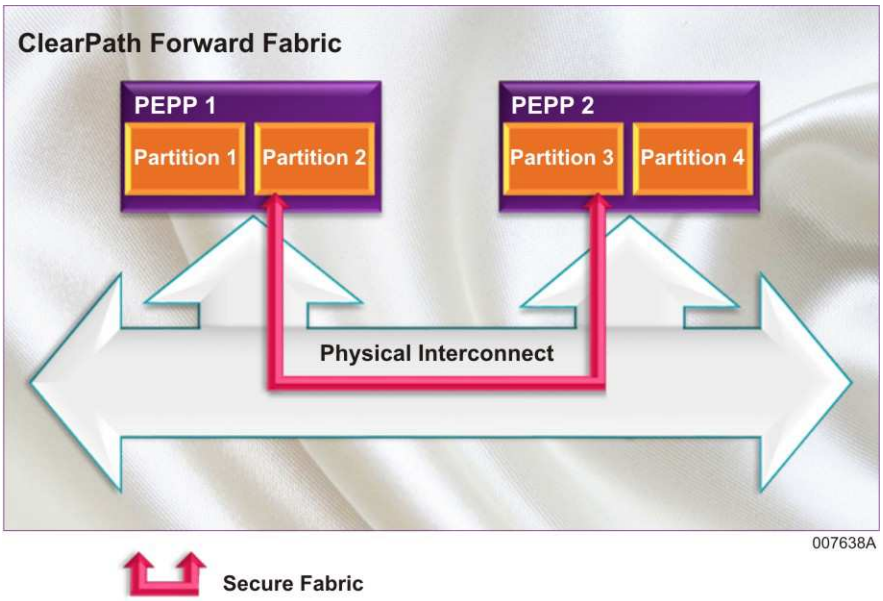
The InfiniBand-based Interconnect includes the ability to define logical subsets of the physical Interconnect called *secure fabrics*. A secure fabric enables you to define a set of partition images that can communicate with each other, but they ***cannot*** communicate with other partition images; and other partition images that ***are not*** part of the secure fabric ***cannot*** communicate with partition images that ***are*** part of the secure fabric. In essence, secure fabrics divide the physical Interconnect into multiple independent fabrics. Secure fabrics are similar to Ethernet virtual LANs (VLANs).

A given partition image can be associated with zero, one, or many secure fabrics. The partition's operating system can interact with each secure fabric that the partition is associated with.

3.2. Example of How to Create a Secure Fabric

You can use the Fabric Manager to create additional secure fabrics, and then associate partitionable enterprise partition platform (PEPP) partitions or nonpartitionable enterprise partition platforms (NEPPs) with a given secure fabric.

In the following example, Partition 2 on PEPP 1 and Partition 3 on PEPP 2 participate in a secure fabric.



To establish such a secure fabric, do the following:

1. Access the Secure Fabric screens in the Fabric Manager user interface.

   3.2.1 Step 1: Navigating to the Fabric Manager Secure Fabrics Screens

2. Add a new secure fabric, filling in the required information.

   3.2.2 Step 2: Adding a Secure Fabric

3. Use the Fabric Manager to commission partition images on PEPP 1 (Partition 2) and PEPP 2 (Partition 3), making sure to select the new secure fabric during commissioning so that the partitions are automatically associated with the secure fabric.

   3.2.3 Step 3: Specifying the Secure Fabric During Commissioning

Since Partition 2 and Partition 3 are associated with the new secure fabric, they can communicate with each other via the new secure fabric. Partition 1 on PEPP 1 and Partition 4 on PEPP 2 are not associated with the new secure fabric and thus cannot communicate with the other two.

3.2.1. Step 1: Navigating to the Fabric Manager Secure Fabrics Screens

To access the Secure Fabric screens in the Fabric Manager user interface, log in to the Fabric Manager, point to **System Administration**, and then click **Secure Fabrics**. The **Manage Secure Fabric** screen appears on the left pane and the **Details: Physical Fabric** screen appears on the right pane.

For more information on using the Fabric Manager user interface, see the help associated with the Fabric Manager or the *ClearPath Forward Administration and Operations Guide*.

3.2.2. Step 2: Adding a Secure Fabric

To add a new secure fabric named **Secure Fabric 1**, do the following:

1. In the right-hand **Details: Physical Fabric** pane, click **Add**.

   The **Add Secure Fabric** window appears.

2. In the **Secure Fabric Name** field, type **Secure Fabric 1** as a name for the new secure fabric.

   Note: *The following is a list of names that you cannot use to name a secure fabric:*

0	forward-system	forwardsystem	localhost
FMP-1	FMP-2	secure-fabric	securefabric
secure-fabrics	securefabrics	ip-lan	iplan
fmlan	fm-lan	hdlan	hd-lan
physical-fabric	physicalfabric	physicalfabrics	physical-fabrics
switch	switches	forwardsystems	cpf-system

3. In the **Description** field, type a description for the new secure fabric. For example, "Secure fabric for a partition on PEPP 1 and a partition on PEPP 2."
4. In the **IPv4 Subnet Details** section, fill in the following:
   - **Subnet IP**: Type the IP address of the subnet that you want the secure fabric associated with. Unisys recommends the use of private IPv4 address spaces.

     Note: *The IP addresses should meet the following requirements:*

     - *Class 'A': First Octet should be between 1 and 126*
     - *Class 'B': First Octet should be between 128 and 191*
     - *Class 'C': First Octet should be between 192 and 223*

   - **QoS**: Depending on anticipated bandwidth usage, select the Quality of Service (QoS) you want associated with the secure fabric.

     For more information on Quality of Service and service levels, see the *ClearPath Forward Overview and Planning Guide*.

   - **Subnet Tag**: Select the desired subnet tag.

     The subnet tags are the unique preexisting identifiers for secure fabrics. (Subnet tags are known in InfiniBand as PKEYs).

5. Click **Add**.

   A confirmation message appears.

6. Click **OK**.

   The new secure fabric named **Secure Fabric 1** appears in the right-hand **Details: Phyiscal Fabric** pane.

For more information on adding secure fabrics, see the help associated with the Fabric Manager or the *ClearPath Forward Administration and Operations Guide*.

3.2.3. Step 3: Specifying the Secure Fabric During Commissioning

When you commission Partition 2 on PEPP 1 and Partition 3 on PEPP 2 respectively, be sure to select the secure fabric Secure Fabric 1.

Note: *For more information on commissioning, see the help associated with the Fabric Manager or the* ClearPath Forward Administration and Operations Guide.

To commission a partition image on PEPP 1, do the following:

1. On the Fabric Manager user interface, point to **System Administration**, and then click **CPF System**.
2. Click **Platforms and Partitions**.

   The **Details: Platforms and Partitions** screen appears.
3. Select the platform named PEPP 1.
4. Click **Commission**.

   Alternatively, double-click the platform row, and then on the **Summary** tab of the platform, click **Commission**.

   A message informing that the system is discovering the resources for the commissioning appears. After discovering the required resources to commission a partition image, the Commission window appears.
5. In the Commission window, fill in the required information and selections on the following tabs, clicking **Next** to move to the next tab.
   - **Blueprint**
   - **Partition Attributes**

     In this example, the partition image name is Partition 2.
   - **Cores and Memory**

     Be sure to assign sufficient memory to the partition image because secure fabrics consume more memory. For more information about the memory usage by secure fabrics see the *ClearPath Forward Administration and Operations Guide*.
   - **I/O Ports**
6. On the **Secure Fabric** tab, select the **Secure Fabric 1** secure fabric, select a logical port from the **Logical Ports (BDF)** list, and then click **Next**.

Notes:

- *Fabric Manager allows you to associate a partition image to more than one secure fabric.*
- *The Bus Device Function (BDF), also called as logical port, identifies the logical port.*
- *You can assign the same logical port for multiple secure fabrics.*

7. On the **Storage** tab, fill in the required information and selections, and then click **Next**.
8. On the **Summary** tab, review the settings for the partition image, and then click **Submit**.

Similarly, commission a partition image on PEPP 2, named Partition 3.

Since Partition 2 on PEPP 1 and Partition 3 on PEPP 2 are associated with the secure fabric Secure Fabric 1, they can communicate with each other via the secure fabric.

3.3. Associating an Operating Environment with a Secure Fabric

The most convenient way to configure a partitionable enterprise partition platform (PEPP) partition for participating in a given secure fabric is to associate the partition image with the secure fabric during commissioning. For more information, see 5.3 Commissioning a Partition Image.

If you did not associate a partition image with a secure fabric during commissioning, and wish to associate a PEPP partition after the partition image has been commissioned, you will need to configure the PEPP partition so that it can participate in a given secure fabric. For more information, refer to the *ClearPath Forward Administration and Operations Guide*.

If you wish to configure a nonpartitionable enterprise partition platform (NEPP) for participating in a given secure fabric, refer to the *ClearPath Forward Administration and Operations Guide* after installing and configuring a supported operating system on your NEPP (see Section 7, Creating a Partition with a Customer-Supplied OS on a NEPP).

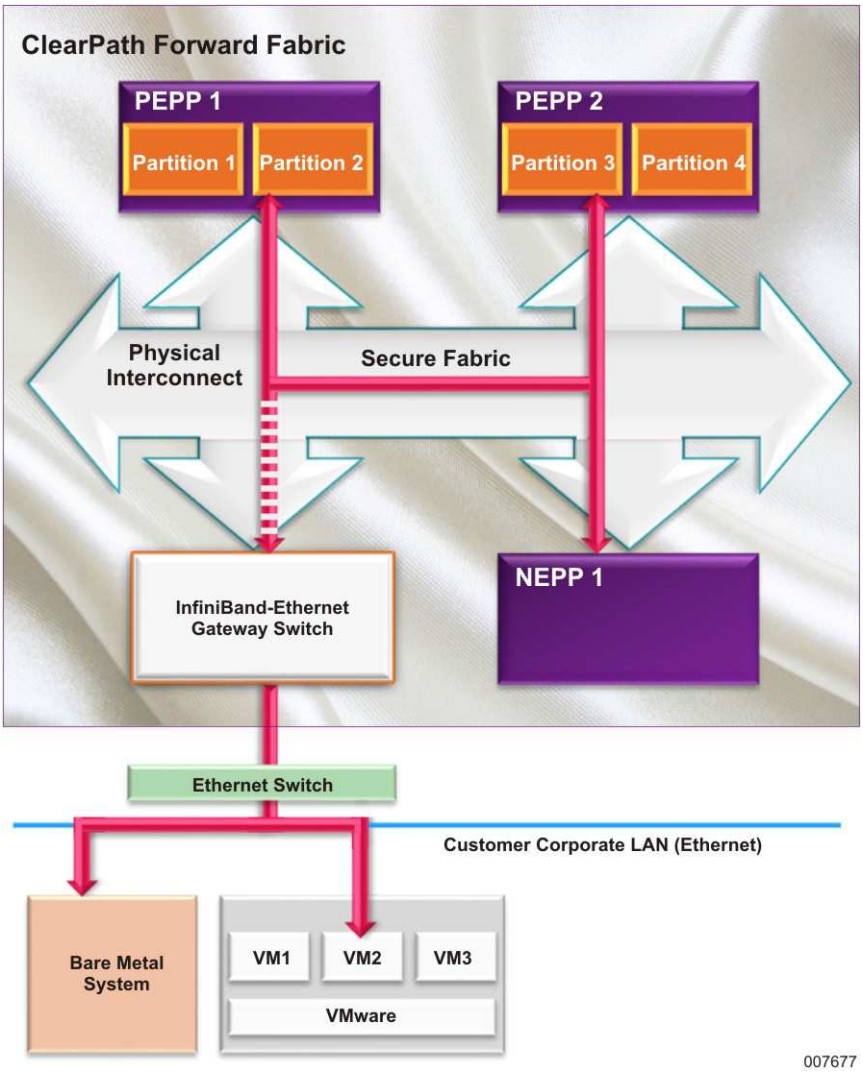
3.4. Managing Your Secure Fabric

For more information on managing your secure fabrics—including detailed procedures for adding, editing, and deleting secure fabrics, as well as disassociating partitionable enterprise partition platform (PEPP) partitions and nonpartitionable enterprise partition platforms (NEPPs) from a secure fabric—refer to the *ClearPath Forward Administration and Operations Guide*.

Section 4
Configuring InfiniBand-Ethernet Gateway Switch

You may want bare metal servers and virtual machines (VMs) in your Ethernet customer corporate LAN environment to participate as members of a secure fabric. However, IP addresses within the ClearPath Forward fabric will likely have a different subnet address from your Ethernet customer corporate LAN. To include your bare metal servers and virtual machines in a secure fabric, you may optionally purchase one or more 12-port InfiniBand-Ethernet gateway switches. You can order the switch at the same time that you order your fabric, or you can order the switch separately as a field upgrade.

The InfiniBand-Ethernet gateway switch includes a gateway license. The switch and license allow communication between the ClearPath Forward fabric and your Ethernet customer corporate LAN. Within the fabric, network traffic uses the high-speed InfiniBand Interconnect.



In the preceding example, Partition 2 on PEPP 1, Partition 3 on PEPP 2, NEPP 1, Bare Metal System, and VM2 participate in a secure fabric.

The Unisys service representative can set up the InfiniBand-Ethernet gateway switch when the fabric is installed or when the switch field upgrade is performed.

Note: *During configuration of the InfiniBand-Ethernet gateway switch, you will need the subnet tag (PKEY) values for each secure fabric. For more information on secure fabrics, refer to Section 3, Creating a Secure Fabric.*

The following topics describe how to set up the factory-prepared InfiniBand-Ethernet gateway switch, as well as some tasks that you might need to perform.

4.1. Overview of Configuring InfiniBand-Ethernet Gateway Switch

For an InfiniBand switch to be configured as an InfiniBand-Ethernet gateway switch, the switch requires a gateway license. A gateway license is specific to the serial number of a particular InfiniBand switch, and is not transferable. If you select the optional package of an InfiniBand-Ethernet gateway switch, the gateway license is pre-installed at the factory.

With the gateway license installed and applied, the InfiniBand switch can run in gateway mode, and you can choose which switch ports operate in InfiniBand mode and which operate in Ethernet mode (see 4.3 Configuring InfiniBand-Ethernet Gateway Switch Port Type). This enables InfiniBand and Ethernet traffic to coexist in the switch, effectively splitting the hardware into two separate switches—an InfiniBand switch and an Ethernet switch—and network traffic does not pass between these two switches unless deliberately enabled through a Proxy ARP communication path.

With a switch configured in gateway mode, the network interfaces are split into two groups:

- The InfiniBand set of ports that are connected to the InfiniBand hosts or other switches
- The Ethernet set of ports that are connected to the customer corporate LAN Ethernet switch

While operating in this configuration, gateway capabilities can be configured to enable passing traffic between the InfiniBand and Ethernet hosts as follows:

1. Define one or more Ethernet Virtual Local Area Networks (VLANs) within the InfiniBand-Ethernet gateway switch; and for each Ethernet port of the InfiniBand-Ethernet gateway switch that will be communicating with a secure fabric, configure the port to allow VLANs to go through it.

   For more information, see 4.4 Configuring Ethernet VLANs.

2. Create a mapping of Ethernet VLANs to secure fabric Subnet Tags (referred to as *pkeys* in InfiniBand terminology).

   For more information, see 4.5 Associating Ethernet VLAN with Subnet Tag.

3. If desired, verify that communication between InfiniBand and Ethernet ports is allowed by issuing a ping command from a host to another.

   For more information, see 4.6 Verifying Communication Between Ports on InfiniBand-Ethernet Gateway Switch.

Note: *In a ClearPath Forward fabric, an InfiniBand switch functions as a fabric switch, and is configured to run Subnet Manager (SM) by default. When an InfiniBand switch is configured as an InfiniBand-Ethernet gateway switch (that is, its gateway function is active), the switch is no longer able to run Subnet Manager. InfiniBand switches that continue their function as fabric switches are not affected, and continue to run Subnet Manager.*

4.2. Accessing InfiniBand-Ethernet Gateway Switch

To access the InfiniBand-Ethernet gateway switch for configuration purposes, do one of the following:

- Web management interface

  On the desktop or laptop PC, use a web browser to open a session to the switch address. When the switch management console appears, log on with the administrative credentials (default credentials from factory is admin/admin).

- Command line interface (CLI)

  On the desktop or laptop PC, start a remote connection session to the switch address. When the switch prompt appears, log on with the administrative credentials (default credentials from factory is admin/admin).

Table 4–1. Default ClearPath Forward Management LAN (FM LAN) IP Addresses for InfiniBand-Ethernet Gateway Switches

Component	Endpoint	IP Address	Comments
InfiniBand-Ethernet Gateway Switch 1	Management Port 1	172.29.254.127	InfiniBand-Ethernet gateway switch management port 1 (mgmt0) on InfiniBand Switch 1.
InfiniBand-Ethernet Gateway Switch 2	Management Port 1	172.29.253.127	InfiniBand-Ethernet gateway switch management port 1 (mgmt0) on InfiniBand Switch 2.

4.3. Configuring InfiniBand-Ethernet Gateway Switch Port Type

From the factory, ports on the InfiniBand-Ethernet gateway switch are configured as follows:

- Ethernet: Ports 1 through 10
- InfiniBand: Ports 11 and 12

If desired, change the configuration.

Considerations When Configuring Port Type

- To maintain a connection to the ClearPath Forward fabric, there must be at least one port configured as an InfiniBand port.
- For redundancy purposes and higher throughput, Unisys recommends two or more ports be configured as InfiniBand ports.

Using Web Management Interface

1. Access the switch. For more information, see 4.2 Accessing InfiniBand-Ethernet Gateway Switch.
2. On the **Ports** tab of the management console, in the left-hand navigation, click **Protocol Type**.

   The Port Protocol Config page appears.
3. Under the **Port Type Info** section, review which ports are configured as InfiniBand or Ethernet.
4. To change the protocol (port type) of a port, under the **Port Protocol Config** section, enter the port number, select the desired type of port, and then click **Apply**.
5. When you complete all desired configuration, click **Save** in the upper right area of the management console to save all changes.

Using Command Line Interface (CLI)

1. Access the switch. For more information, see 4.2 Accessing InfiniBand-Ethernet Gateway Switch.
2. At the prompt, execute the following command to view the port type configuration of all switch ports.

   ```
   show ports type
   ```
3. To change the port type of a port, be sure to shut down the port before reconfiguring it. In the following example, port 10 is originally an InfiniBand port and is reconfigured as an Ethernet port.

```
Switch-1 [standalone: master] > enable
Switch-1 [standalone: master] > configure terminal
Switch-1 [standalone: master] (config) # interface ib 1/10
Switch-1 [standalone: master] (config interface ib 1/10) # shutdown
Switch-1 [standalone: master] (config interface ib 1/10) # exit
Switch-1 [standalone: master] (config) # port 1/10 type Ethernet
Switch-1 [standalone: master] (config) # interface ethernet 1/10
Switch-1 [standalone: master] (config interface ethernet 1/
10) # no shutdown
```

4. Repeat the configuration commands as needed to reconfigure the port type of a port.

4.4. Configuring Ethernet VLANs

Define one or more Ethernet Virtual Local Area Networks (VLANs) within the InfiniBand-Ethernet gateway switch. Each Ethernet switch port that will be communicating with a ClearPath Forward fabric must be configured to allow VLANs to go through it.

Creating Ethernet VLANs

Define the set of Virtual Local Area Networks (VLANs) to enable within the InfiniBand-Ethernet gateway switch:

1. If needed, access the command line interface (CLI) for the switch. For more information, see 4.2 Accessing InfiniBand-Ethernet Gateway Switch.
2. At the prompt, execute the CLI **configure terminal** command to enter the configuration mode.

```
enable
configure terminal
```

3. Define and enable one or more VLANs.

   For example, if you wish to define four VLANs, named (tagged) as 10, 4000, 193, and 27 respectively, do the following:

```
Switch-1 [standalone: master] (config) # vlan 10
Switch-1 [standalone: master] (config vlan 10) # exit
Switch-1 [standalone: master] (config) # vlan 4000
Switch-1 [standalone: master] (config vlan 4000) # exit
Switch-1 [standalone: master] (config) # vlan 193
Switch-1 [standalone: master] (config vlan 193) # exit
Switch-1 [standalone: master] (config) # vlan 27
Switch-1 [standalone: master] (config vlan 27) # exit
```

Configuring Allowed Traffic for Ethernet Port

Each Ethernet port on the InfiniBand-Ethernet gateway switch can be configured to allow tagged packets, untagged packets, or both, as well as whether traffic from a particular VLAN is allowed.

1. While in configuration mode, specify the particular Ethernet port you wish to configure.

   In the following example, Ethernet port 1/28 is specified.

```
Switch-1 [standalone: master] (config) # interface ethernet 1/28
```

2. Configure the Ethernet port to allow type of VLAN traffic (tagged packets, untagged packets, or both), as well as traffic from multiple VLANs. Valid port switch modes are:

   - Trunk: This mode configures the port for only tagged packets.
   - Access: This mode configures the port to allow only untagged packets on the ingress Ethernet ports.
   - Hybrid: This mode configures the port to allow both tagged and untagged packets on the ingress Ethernet ports.

   In the following example, Ethernet port 1/28 is configured to only allow tagged packets, that is, trunk mode is used. It is also configured to allow the four VLANs 10, 4000, 193, and 27.

```
Switch-1 [standalone: master] (config interface Ethernet 1/28) # switchport mode trunk
Switch-1 [standalone: master] (config interface Ethernet 1/
```

```
28) # switchport trunk allowed-vlan add 10
Switch-1 [standalone: master] (config interface Ethernet 1/
28) # switchport trunk allowed-vlan add 4000
Switch-1 [standalone: master] (config interface Ethernet 1/
28) # switchport trunk allowed-vlan add 193
Switch-1 [standalone: master] (config interface Ethernet 1/
28) # switchport trunk allowed-vlan add 27
Switch-1 [standalone: master] (config interface Ethernet 1/
28) # exit
```

Repeat as necessary for all Ethernet ports on the InfiniBand-Ethernet gateway switch.

Verifying Ethernet VLAN Configuration

While in configuration mode, execute the **show vlan** command to verify that the VLANs are set up as expected. For example,

```
Switch-1 [standalone: master] (config) # show vlan
VLAN    Name        Ports----    ----------  ----------------------
1       default     Eth1/18, Eth1/19, Eth1/20, Eth1/21, Eth1/22,
                    Eth1/23, Eth1/24, Eth1/25, Eth1/26, Eth1/27
10, 27, 193, 4000   Eth1/28
```

4.5. Associating Ethernet VLAN with Subnet Tag

To create a mapping of Ethernet VLANs to secure fabric subnet tags (referred to as PKEYS in InfiniBand terminology) and transmit IPv4 packets between the Ethernet and InfiniBand networks, set up Proxy ARP logical interfaces on the InfiniBand-Ethernet gateway switch to act as bridges for forwarding IP over Ethernet (IPoE) packets to the IP over InfiniBand (IPoIB) interfaces, and IPoIB packets to the IPoE interfaces.

A Proxy ARP logical interface owns an IP address, VLAN tag, and InfiniBand PKEY value of the subnet it belongs to. (InfiniBand PKEYs are identified as subnet tags on the Fabric Manager user interface.) An InfiniBand-Ethernet gateway switch supports up to 32 Proxy ARP logical interfaces, and each interface must have a unique pairing of VLAN with subnet tag (PKEY).

Obtaining Secure Fabric Subnet Tags

Using the Fabric Manager user interface, add the desired secure fabrics, and then note down the subnet tag (PKEY) values for each secure fabric. For more information on adding secure fabrics, refer to the *ClearPath Forward Administration and Operations Guide*.

Setting Up Proxy ARP Logical Interface

While in configuration mode, enable Proxy ARP, create a Proxy ARP interface, set up an IP address and network mask to the interface, add a VLAN and a subnet tag (PKEY) to the interface, and then enable the interface.

In the following example, the **ip proxy-arp** command is executed to enable Proxy ARP, and the logical interface Proxy-ARP 2 is created. The interface is set up with the IP address 172.31.100.1 and network mask 16, and then VLAN 10 and subnet tag (PKEY) 0x0001 are added. Finally, the interface is enabled.

```
Switch-1 [standalone: master] (config) # ip proxy-arp
Switch-1 [standalone: master] (config) # interface proxy-arp 2
Switch-1 [standalone: master] (config interface proxy-
arp 2) # ip address 172.10.100.1
Switch-1 [standalone: master] (config interface proxy-
arp 2) # ip netmask /16
Switch-1 [standalone: master] (config interface proxy-arp 2) # ip vlan 10
Switch-1 [standalone: master] (config interface proxy-
arp 2) # ip pkey 0x0001
Switch-1 [standalone: master] (config interface proxy-arp 2) # no shutdown
Switch-1 [standalone: master] (config interface proxy-arp 2) # exit
```

Repeat as needed to create enough Proxy ARP logical interfaces to map all Ethernet VLANs to secure fabric subnet tags.

Verifying Proxy ARP Logical Interface Setup

After creating all desired Proxy ARP logical interfaces and mapping all Ethernet VLANs to secure fabric subnet tags, execute the **show interfaces proxy-arp brief** command to verify that the interfaces are set up as expect. For example,

```
Switch-1 [standalone: master] (config) # show interfaces proxy-arp brief
Interface    Description   State   Bridged interfaces
-----------------------------------------------------------
proxy-arp 1  N/A           Up      vlan 1, pkey 0x7fff
proxy-arp 2  N/A           Up      vlan 10, pkey 0x1
proxy-arp 3  N/A           Up      vlan 4000, pkey 0xfa0
```

4.6. Verifying Communication Between Ports on InfiniBand-Ethernet Gateway Switch

Use a ping command to verify that communication is allowed over a Proxy ARP path linking a subnet tag (PKEY) and an Ethernet VLAN.

In the following example, a ping is issued from the SLES 11 partition connected to the IPoIB port with subnet tag (PKEY) 0x8fa0 to a non-partitionable enterprise partition (NEPP) connected to the Ethernet VLAN 4000 port of the InfiniBand-Ethernet gateway switch:

```
sles11sp3-vm1:~ # ping -c 4 172.40.0.31
PING 172.40.0.31 (172.40.0.31) 56(84) bytes of data.
64 bytes from 172.40.0.31: icmp_seq=1 ttl=127 time=1004 ms
64 bytes from 172.40.0.31: icmp_seq=2 ttl=127 time=0.066 ms
64 bytes from 172.40.0.31: icmp_seq=3 ttl=127 time=0.093 ms
64 bytes from 172.40.0.31: icmp_seq=4 ttl=127 time=0.135 ms
--- 172.40.0.31 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 0.066/251.211/1004.550/434.940 ms
```

4.7. Configuring the InfiniBand-Ethernet Gateway Switch for Health Monitoring

To verify or set up the InfiniBand-Ethernet gateway switch for health monitoring by the Fabric Manager, do the following:

1. Access the web management interface for the switch. For more information, see 4.2 Accessing InfiniBand-Ethernet Gateway Switch.
2. On the **Setup** tab of the management console, in the left-hand navigation, click **SNMP**.

   The SNMP configuration page appears.
3. Under the **SNMP v3 Users** section, locate the user **admin**, and then click **Edit**.

   The Edit SNMP v3 User page appears.
4. Ensure the **Enable user** checkbox is selected.
5. Verify or set the authentication password to **authauth**.
6. Verify or set the privacy password to **passpass**.
7. Click **Apply**, and then click **OK**.
8. Click **Save** in the upper right area of the management console to save all changes.

The InfiniBand-Ethernet gateway switch is now ready for health monitoring by the Fabric Manager.

If necessary, use the Fabric Manager user interface to add the InfiniBand-Ethernet gateway switch to the fabric. For more information, see the help associated with the Fabric Manager or the *ClearPath Forward Administration and Operations Guide*.

4.8. Backing up InfiniBand-Ethernet Gateway Switch License Key

Unisys recommends making a backup of the InfiniBand-Ethernet gateway switch license key so it can be restored if the license is lost.

To back up the InfiniBand-Ethernet gateway switch license key, do the following:

1. Access the Web management interface of the switch.

   For more information, see 4.2 Accessing InfiniBand-Ethernet Gateway Switch.
2. On the **Setup** tab of the management console, in the left-hand navigation, click **Licensing**.

   The Licensing page appears.
3. Using your preferred software, make a screen capture of the license key. Be sure the area outlined in red in Figure 4–1 is captured.

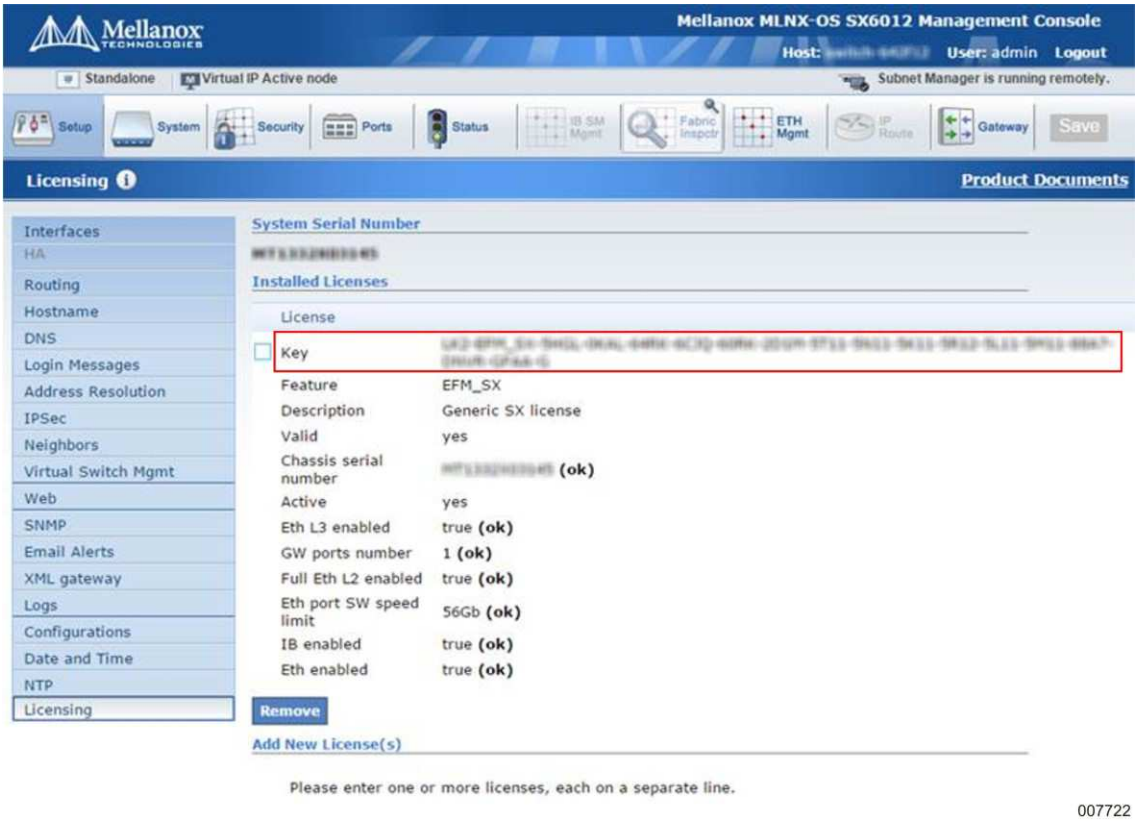


Figure 4–1. InfiniBand-Ethernet Gateway Switch Licensing Page

4. Save the .png or .jpg file to a safe location designated by the customer.

4.9. Connecting InfiniBand-Ethernet Gateway Switch to Your Network

You can connect the InfiniBand-Ethernet gateway switch directly to a 40 Gb Ethernet switch in your datacenter. Alternatively, you can use a 40 Gb-to-10 Gb x 4 fan-out cable to provide four 10 Gb connections from a single switch port. Note that the connectors on the 4 x 10 Gb fan-out cable are direct attach twinaxial connections, and the datacenter LAN switch must support that type of connector.

4.10. Resetting InfiniBand-Ethernet Gateway Switch to Factory Default

Note: *Pressing the physical reset button on the InfiniBand-Ethernet gateway switch reboots the switch but does not reset it to factory default configuration.*

If you need to reset the InfiniBand-Ethernet gateway switch to the default configuration from the factory, execute the following CLI command:

```
reset factory keep-basic
```

The command resets the switch while maintaining the gateway license and management port IP addresses that were configured at the factory.

After the reset, execute the following CLI commands to set the switch into gateway mode:

```
system profile vpi-single-switch
no ip routing
ip proxy-arp
```

Note that after a reset to the factory default configuration, ports 1 through 10 are once again configured as Ethernet ports, and ports 11 and 12 are once again configured as InfiniBand ports. If desired, change the configuration; see 4.3 Configuring InfiniBand-Ethernet Gateway Switch Port Type for more information.

4.11. Replacing the InfiniBand-Ethernet Gateway Switch

The gateway license for an InfiniBand-Ethernet gateway switch is specific to the switch's serial number and can only be used for that particular switch. Unisys Product Support maintains a record of the InfiniBand-Ethernet gateway switches by serial number and their associated licenses.

If an InfiniBand-Ethernet gateway switch fails, report the serial number to Unisys Product Support at **GW-SWITCH@unisys.com** so Unisys can appropriately process the retired gateway license on the failed switch.

4.12. Configuring NTP Settings on the InfiniBand-Ethernet Gateway Switch

After replacing the InfiniBand-Ethernet gateway switch, the NTP time source must be configured using the following procedure:

1. Using a web browser on your workstation, enter **172.29.254.127** in the browser address bar to connect to the InfiniBand-Ethernet gateway switch. If a second InfiniBand-Ethernet gateway switch is present, enter **172.29.253.127**.
2. On the **Setup** tab, select the **Date and Time** option from the left column of the management console.
3. Adjust the Time Zone field as appropriate.

   If the date and time is off by days, months, or years, adjust the values to the current date and time. If these fields are read-only, temporarily disable NTP so that you can adjust them. To temporarily disable NTP, do the following:

   a. Select the **NTP** option from the left column of the management console.

   b. Uncheck the Enable NTP Time Synchronization check box and click **Apply**.

c. Select the **Date and Time** option from the left column of the management console.

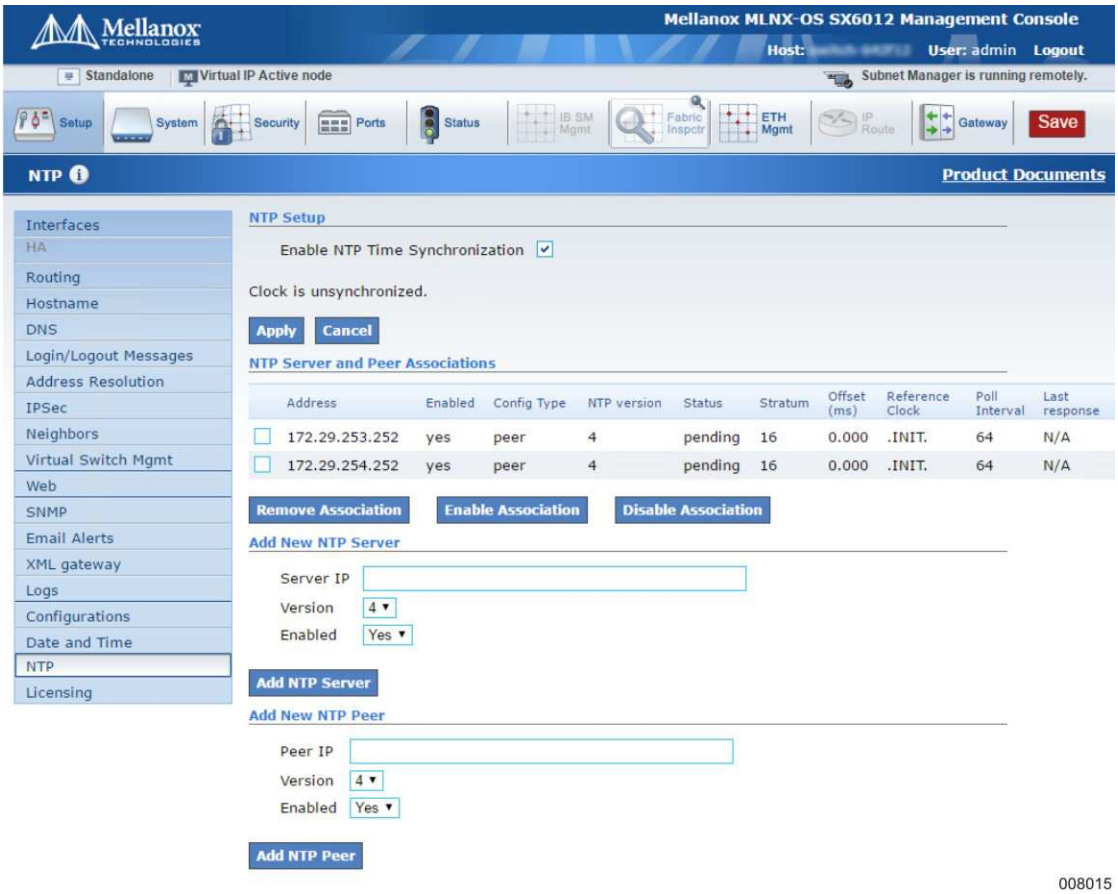
d. Adjust the Date and Time Zone fields as appropriate and click **Apply**.

4. Select the **NTP** option from the left column of the management console.

5. In the NTP Server and Peer Associations section, the first two nodes of each address should be the subnet of the FM LAN. By default this is 172.29, so if the client has not modified the FM LAN subnet, the two IP addresses should be **172.29.254.252** and **172.29.253.252** (if a second FMP is present). If a different subnet is being used for the FM LAN, use that instead of 172.29. If the IP addresses are not correct, perform the following steps:

   a. In the Add New NTP Server section, enter the following:

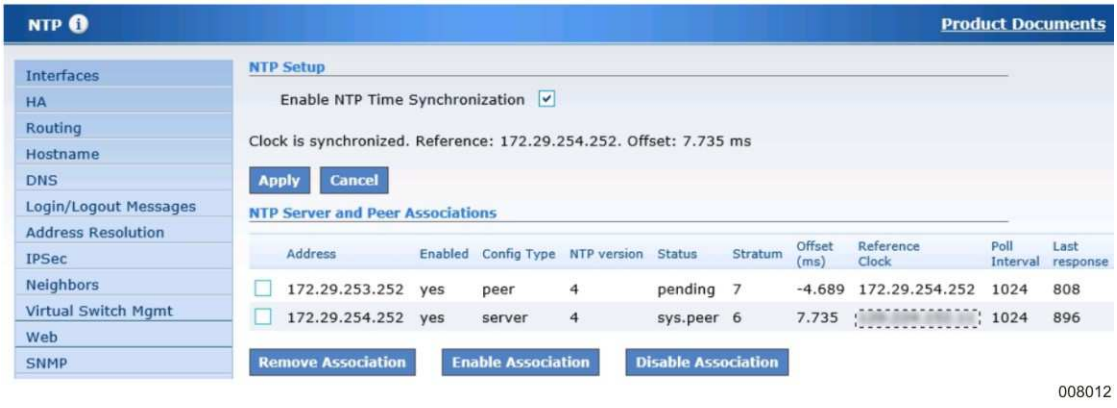
      - Server IP address: **172.29.254.252** (or ***x.y*.254.252**, where ***x.y*** is the customized subnet).
      - Version: **4** (default)
      - Enabled: **Yes** (default)



6. Click **Add NTP Server**.

7. If there is a second FMP in the system, in the Add New NTP Peer section, enter the following:
   - Server IP address: **172.29.253.252** (or ***x.y*.253.252**, where ***x.y*** is the customized subnet).
   - Version: **4** (default)
   - Enabled: **Yes** (default)
8. Click **Add NTP Peer**.
9. Check that the NTP Server and Peer Associations section contains the added NTP server and peer IP addresses.
10. If incorrect IP addresses were configured, select the two check boxes to the left of those IP addresses and then click the **Remove Association** button.
11. Select the Enable NTP Time Synchronization check box (if it's not already enabled) and then click **Apply**.

    Note: *There might be a delay from the time NTP synchronization is enabled and the correct IP addresses are defined for the switch to synchronize with the NTP server, but eventually the InfiniBand-Ethernet gateway switch (in the Date and Time view) will show the same date and time as FMP1. If FMP1 is getting its clock from an NTP server, then the Reference Clock field will display the IP address of FMP1s' source NTP server. Likewise, the FMP2 IP address will show FMP1 as its NTP source.*
12. Click the **Save** button in the top right corner. The final display should appear as follows.



13. Repeat this procedure on the second InfiniBand-Ethernet gateway switch (if a second one is present).

Section 5
Creating a Partition with a Unisys-Supplied OS

This section provides information on creating partitions with Unisys-supplied operating systems.

5.1. Overview of Installing a Unisys-Supplied OS on a Partitionable Enterprise Partition Platform

To install one of the Unisys-supplied operating systems to a partition on a partitionable enterprise partition platform (PEPP),

1. Use the Fabric Manager user interface to commission a partition image with the desired operating system. For more information, see 5.2 Overview of Commissioning a Partition and 5.3 Commissioning a Partition Image.

   Note: *For more information on creating secure fabrics, refer to Section 3, Creating a Secure Fabric.*

2. Complete initial configuration of the operating system. For more information, see 5.4 Completing Installation and Configuration of a Unisys-supplied Windows Partition Image or 5.5 Completing Installation and Configuration of a Unisys-supplied Linux Partition Image.

3. After configuring and customizing the operating system and application operating environment, be sure to back up your partition. For more information, see 5.6 Backing Up Application Operating Environments on Partitionable Enterprise Partition Platforms.

   Notes:

   - *When configuring a software firewall on a partition image, ensure that you configure the firewall to allow incoming ping requests through the ClearPath Forward Management LAN (FM LAN). The Fabric Manager monitors the health status of a partition image through ping checks; if the ping requests on the FM LAN to the partition image are blocked by a firewall, the Fabric Manager displays a warning state for the partition image's health (but does not generate an event).*
   - *Do not use the YaST firewall module to configure software firewalls on a partition created using a Unisys-supplied SUSE Linux Enterprise Server (SLES) image. As Unisys uses a custom firewall zone, the YaST firewall module will report errors.*

5.2. Overview of Commissioning a Partition

Commissioning is the process of creating a partition image by using the Fabric Manager user interface. Commissioning associates software with hardware resources, resulting in a partition image. You begin the commissioning process by selecting a software template called a blueprint. The blueprint supplies the gold image (that is, the software that will run in the partition). Then you specify values for any additional required attributes, such as the following:

- Partition name
- Host Computer Name where the partition will reside
- Partition chassis
- Number of processor cores in the partition
- Partition memory size (a default value is provided, which you may change)
- Whether or not hyperthreading is enabled
- NIC ports and HBA ports owned by the partition
- Whether a NIC port is shared
- Whether a NIC port is teamed
- Whether a NIC port has peer forwarding enabled
- Boot disk storage space (LUN size) for the internal boot drive (if any)
- Number of data LUNs and their size
- Whether or not the partition image is started after a platform reboot
- Whether or not the partition image is part of one or more secure fabrics

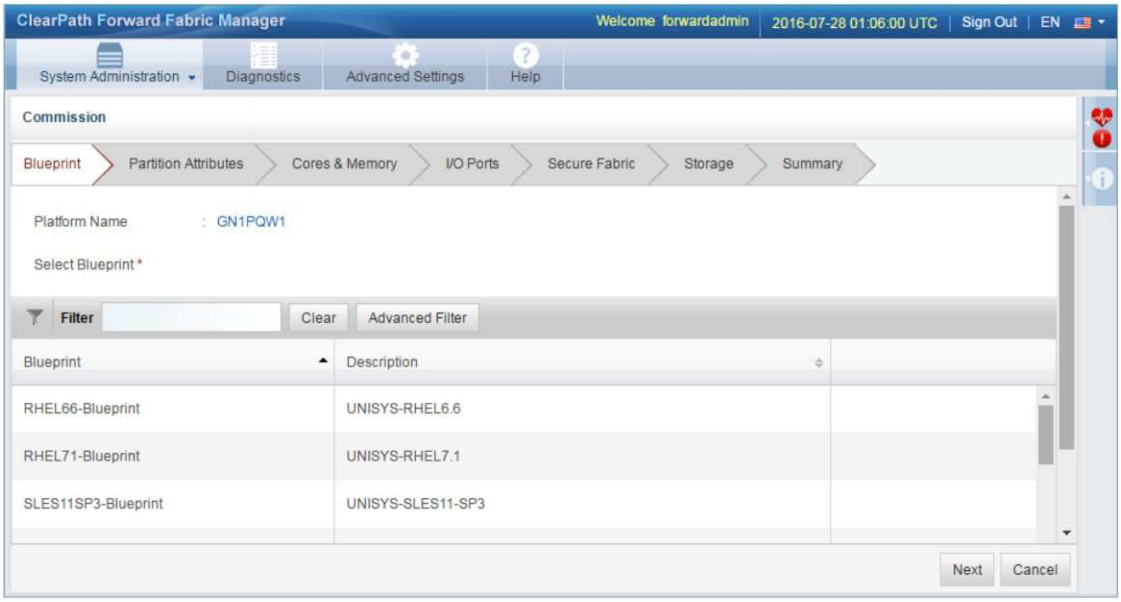
The Fabric Manager then creates (commissions) the partition image.

As a result of the commissioning process, the partition image

- Is enabled
- Is in a running state
- Appears in the left navigation pane of the Fabric Manager

At this point, the partition image has been assigned hardware resources and is capable of being booted and executing a customer workload.

The following figure shows the initial commissioning screen, in which you select the blueprint.



007645A

5.3. Commissioning a Partition Image

Note: *The commissioning procedure described in this section is applicable for platforms that are based on s-Par version 4.2 and above. If you are commissioning a partition image on a platform that is based on s-Par versions 4.1 or lesser, then refer to the* Installation, Administration, and Operations Guide *from the 2.0 documentation library under the ClearPath Forward portion of the Unisys Product Support site available at https://www.support.unisys.com/search2/DocumentationSearch.aspx?ID=8088&pla=ps&nav=ps*

Ensure that the required resources such as blueprint and gold image are available. Additionally, the Fabric Manager user interface provides information about the different partition images that you can commission on a particular platform. For more information about blueprints, gold images and partition images that you can commission on a particular platform, see the *ClearPath Forward Administration and Operations Guide* for more information.

Notes:

- *If you plan to commission the partition image on an external boot volume, verify that your storage administrator has prepared and configured the external storage device. For more information about commissioning partition images to boot from an external storage device, refer to Section 9, Configuring Partition Images to Boot from External Storage Device.*
- *While commissioning a partition image, Unisys recommends you to take the worksheet print out and manually fill the parameters of the partition being commissioned on a platform. This worksheet helps you to reconstruct the partition environment in the event of a catastrophic failure. See Appendix A, Worksheet for Commissioning, to learn more about the worksheet.*

- *You can commission a maximum of 16 NIC Ports and a maximum of 16 HBA Ports on a partition image.*
- *You can also assign a shared NIC port to a partition image. For more information about shared NIC ports, see the* ClearPath Forward Administration and Operations Guide.
- *Depending on your fabric configuration, some fields may not be editable and are greyed out.*

To commission a partition image

1. On the Fabric Manager user interface, point to **System Administration**, and then click **CPF System**.
2. Click **Platforms and Partitions**.

   The **Details: Platforms and Partitions** screen appears.
3. Select the platform on which you want to commission the partition image.
4. Click **Commission**.

   Alternatively, double-click the platform row, and then on the **Summary** tab of the platform, click **Commission**.

   A message informing that the system is discovering the resources for the commissioning appears. After discovering the required resources to commission a partition image, the Commission window appears.
5. In the Commission window, perform the steps in the respective tabs as described in the following topics and click **Submit**:
   - 5.3.1 Selecting Blueprint (Blueprint Tab)
   - 5.3.2 Setting Up Basic Partition Information (Partition Attributes Tab)
   - 5.3.3 Providing Configuration Details (Cores and MemoryTab)
   - 5.3.4 Selecting I/O Ports (I/O Ports Tab)
   - 5.3.5 Associating Secure Fabrics with Partition Image (Secure Fabric tab)
   - 5.3.6 Selecting Boot LUN and Data LUNs (Storage tab)
   - 5.3.7 Viewing Summary (View Summary Tab)

The newly commissioned partition image appears in the **Partitions** tab of the respective platform. To view the newly commissioned partition, on the **Details: Platforms and Partitions** screen, select the **Platforms** tab, and double-click the platform on which the partition was commissioned.

Post-commissioning Tasks

After commissioning a Unisys-supplied partition image, you should perform post-commissioning tasks to complete installing and configuring the operating system. For more information about the post-commissioning tasks, refer to the following:

- 5.4 Completing Installation and Configuration of a Unisys-supplied Windows Partition Image

- 5.5 Completing Installation and Configuration of a Unisys-supplied Linux Partition Image

5.3.1. Selecting Blueprint

In the **Blueprint** tab, select the desired blueprint and then click **Next**.

The Partition Attributes tab appears.

5.3.2. Setting Up Basic Partition Information

Note: *You should begin the commissioning process by selecting a blueprint in the* ***Blueprint*** *tab.*

In the **Partition Attributes** tab, provide appropriate information in the following fields and then click **Next**:

- **Partition Image Name***: Type a name for the partition image. This should be unique across the fabric because it is required for monitoring the state and health of the partition images within FM LAN subnet. This field is mandatory.

  Notes:

  - *The maximum length of the partition image name can be 15 alphanumeric characters along with "-". The name cannot start with the character "-".*
  - *The following is a list of names that you cannot use to name a partition image:*

0	forward-system	forwardsystem	localhost
FMP-1	FMP-2	secure-fabric	securefabric
secure-fabrics	securefabrics	ip-lan	iplan
fmlan	fm-lan	hdlan	hd-lan
physical-fabric	physicalfabric	physicalfabrics	physical-fabrics
switch	switches	forwardsystems	cpf-system

- **Host Computer***: Type the name of the host computer. This field is mandatory.

  Notes:

  - *The host computer name should be unique across the fabric if partition images are connected within the same customer LAN subnet.*
  - *The maximum length of the host computer name can be 15 alphanumeric characters along with "-". The name cannot start with the character "-".*

- **Initial State on Platform Reboot**: Select an option to set the initial state of the partition after a platform reboot. The available options are **Running** and **Stopped**. The default option is **Running**.

Note: *The Initial State value does not apply to the partition images that are currently disabled.*

- **Description**: Type a description for the partition image. This field is optional.

  Note: *Provide a meaningful description for the partition image. The maximum length of the description can be 256 alphanumeric characters along with space, "-", and ".". The length of any word in the description should not exceed 20 characters. It is recommended to add details of the ports added to the partition.*

- **Login Credentials**: Type a password in the **Password*** field and confirm the password in the **Confirm Password*** field. This field is mandatory.

  Notes:

  - *This password is used by the default Administrator (Windows) or root (Linux) account during commissioning for initial setup of the operating system. These credentials should only be used for commissioning and you should change these temporary credentials when you complete the initial installation and configuration of your operating system. Refer to the operating system documentation for more information.*
  - *You may enter a fictitious value if you are commissioning a Linux partition image from customer-supplied images. The host computer name and password from your prepared Linux operating system are captured as part of the image that you have created. Use that information to access your Linux partition image; the information in the host computer name and password fields during commissioning is ignored.*

5.3.3. Providing Configuration Details

Note: *You should begin the commissioning process by selecting a blueprint in the* ***Blueprint*** *tab.*

In the **Cores & Memory** tab, provide information in the appropriate fields and then click **Next**. The following table provides details about various fields in the **Cores & Memory** tab:

Field	Action
Partition Chassis	Choose the required partition chassis; for example, Chassis-B.
Cores	Choose the number of cores you want to assign to the partition image. The number of cores available depends on the partition chassis that you have chosen. The default value is 1.

Field	Action
Enable Hyper-Threading	Select the check box to enable selection of two logical processors per core. ***Note:*** *If Hyper-Threading is not supported by the platform or chassis, then this option is not available.*
Logical Processors	Displays the number of logical processors, based on the number of cores.
Memory	Choose the memory size that you want to assign to the partition image. The default value is 2. The memory range available depends on the partition chassis that you have chosen. The minimum value that can be chosen is 2 GB. ***Notes:*** • *Secure fabrics consume more memory. If you are planning to associate the partition image to a secure fabric, see the* ClearPath Forward Administration and Operations Guide *for detailed information about memory usage by secure fabrics.* • *If you are assigning a larger memory, then the Fabric Manager might take longer time to commission the partition image. For example, if you have assigned a memory of 20 TB size, then the Fabric Manager might take about 30 minutes to commission the partition image.*

5.3.4. Selecting I/O Ports

Note: *You should begin the commissioning process by selecting a blueprint in the* ***Blueprint*** *tab.*

In the **I/O Ports** tab, perform the following actions and then click **Next**:

1. (Optional) Select a NIC Port.

   Under **NIC Ports**, you can do the following:

   - Click on the required dedicated port.

     The Port Settings window appears. Select the **Assign** option, and click **OK**. The selected port icon changes to  .
   - Click on the required shared port.

The Select Logical Ports window appears. This window displays details of the logical ports.

a. Click on the required logical port.

   The Port Settings window appears.

b. Under the **Select Action** section, select the **Assign** option.

c. Set the attributes of the logical port:

   - (Optional) To enable teaming of the logical port, under the **Configure Attributes** section, select the **Teaming** check box.
   - (Optional) To enable peer forwarding of the logical port, under the **Configure Attributes** section, select the **Peer Forwarding** check box.

   Note: *You can enable/disable Teaming/Peer-Forwarding on the logical ports only if they were enabled on the physical port. For more information on NIC Teaming, see the* ClearPath Forward Administration and Operations Guide.

d. Click **OK**.

   The selected logical port icon changes to  .

2. (Optional) Select an HBA Port.

   You can associate an HBA port if you wish to commission the partition image on an external boot volume. To do this, under **HBA Ports**, click on the required port, then on the Port Settings window, select the **Assign** option, and click **OK**.

Notes:

- *You can select a maximum of 16 NIC ports and 16 HBA ports.*
- *A range of BDFs is applicable for NIC and HBA ports. You can reserve a Bus Device Function (BDF) for a partition. This enables easy mapping of an application to a persistent interface name with which the BDF is identified. When you Disable a port, a BDF from the range of BDFs is reserved for the partition. When required, you can Assign the BDF to the port. The BDF is then mapped to the port. To disable, click on the required port and then in the Port Settings window select the Disable option.*
- *If you are choosing a custom BDF, then it is appropriate to first select function 0 and then select the functions from 1 to 7. If you do not select function 0, then the Unisys aa78 device will be added automatically. This is applicable for each custom device number.*
- *If you are not choosing a custom BDF and not assigning port 0, then the Unisys aa78 device will be added automatically. This is applicable for each slot.*

Understanding the Legends on the I/O Ports Tab

The **I/O Ports** tab displays the port icons according to status of the ports. For example, an available port and an used port are represented by two different port icons. Icons display the status of Dedicated ports, Shared ports and Boot path ports.

Note:

- *Dedicated port: Can be used by only one partition at a time.*
- *Shared port: Can be logically be assigned multiple times.*
- *Boot path port: Primary boot path that connects to external boot volume.*

The following table provides information about the various port icons and the status that they represent:

Icon	Description
	Dedicated port, available to be assigned to this partition.
	Dedicated port, used by another partition. Cannot be assigned to this partition.
	Dedicated port, selected but yet to be assigned to this partition.
	Dedicated port, already in use by this partition.
	Dedicated port, selected to disable, not yet disabled. Has an allotted VBDF number, but is unused by this partition. Can be used later by this partition or by other partitions.
	Dedicated port, disabled by this partition. Has an allotted VBDF number, but is unused by this partition. Can be used later by this partition or by other partitions.
	Dedicated port, used previously by this partition and later released. Encountered conflict on attempt to re-use, if currently used by other partition.
	Dedicated port, selected to release, but not yet released for this partition.
	Dedicated port, status is unknown.
	Shared port, with available logical ports. Details displayed on hover or click on icon.
	Shared port, with no available logical ports. All are used by other partitions.
	Shared port, multiple logical ports selected to be assigned to this partition.
	Shared port, all logical ports already in use by this partition.

Icon	Description
	Shared port, where one or more logical ports previously used by this partition and later released. Encountered conflict on attempt to re-use, if at least one port is currently used by other partition.
	Boot path port, connecting to external boot volume, already in use by this partition.
	Boot path port, connecting to external boot volume is disabled.
	Boot path port, previously connecting to external boot volume for this partition, but later released. Encountered conflict on attempt to re-use if currently used by other partition.

5.3.5. Associating Secure Fabrics with Partition Image

Note: *You should begin the commissioning process by selecting a blueprint in the* ***Blueprint*** *tab.*

Prerequisites:

- You should have assigned sufficient memory to the partition image because the secure fabrics consume more memory. For more information about the memory usage by secure fabrics see the *ClearPath Forward Administration and Operations Guide*.
- If you are planning to associate a Windows partition image to a secure fabric, see the *ClearPath Forward Administration and Operations Guide* to know about the restrictions on Windows partitions associated with secure fabrics.

In the **Secure Fabric** tab, perform the following actions and then click **Next**:

1. Select one or more secure fabrics that you want to associate with this partition.

   Note: *Fabric Manager allows you to associate a partition image to more than one secure fabric.*

2. (Optional) You can enable the FM LAN, by selecting the **FM-LAN** check box. The FM LAN is disabled by default.

> **Caution**
>
> Before you enable the FM-LAN option, it is important that you understand the security risks associated with the use of the FM LAN. It is possible for an FM LAN Ethernet switch monitored by the Fabric Manager to have an access vulnerability. For more information on the security risks associated with the FM LAN, refer to the *ClearPath Forward Security Guide*.

3. Select a logical port from the **Logical Ports (BDF)** drop-down list of the selected secure fabric.

   The Bus Device Function (BDF), also called as logical port, identifies the logical port. You can assign the same logical port for multiple secure fabrics.

Note: *If you are associating the secure fabrics without assigning the first logical port, then the Unisys aa78 device will be added automatically.*

For more information about secure fabrics, see the *ClearPath Forward Administration and Operations Guide*.

5.3.6. Selecting Boot LUN and Data LUNs

Note: *You should begin the commissioning process by selecting a blueprint in the* ***Blueprint*** *tab.*

In the **Storage** tab, you can do the following:

Configure Internal Storage

Under the **Boot LUN** section, and under **Internal Storage**, select the appropriate LUN size in the **LUN Size – No.** drop-down list.

LUNs are identified by the ID number. For example, ID1, ID2, and so on. Once you select a LUN as the Boot LUN, it will not be available for selection as a Data LUN.

The following list provides general guidelines on the minimum internal storage that you may want to choose, depending on your OS and External Storage selection. The storage sizes listed below are indicative only and the LUN size may need to be increased depending on the amount of memory that you assigned to the partition image. For example, if you assign 3 TB of memory to the partition image, then a LUN size of 110 GB is required:

- A LUN size of at least 60 GB if you are commissioning a Windows partition image from Unisys-supplied images, and the boot volume is on internal storage.
- A LUN size of at least 20 GB if you are commissioning a Linux partition image from Unisys-supplied images, and the boot volume is on internal storage.
- A LUN of at least the size of the original disk size that the operating system you captured is installed on if you are commissioning a Linux partition image from customer-supplied images, and the boot volume is on internal storage.
- A LUN of the smallest disk size (for example, 1 GB) for containing necessary drivers, if the boot volume is on external storage and you will be configuring your partition to boot from an external storage device over fibre channel.
- A LUN size of at least 20 GB if you are commissioning a Linux partition image that you will be configuring to boot from an external storage device over iSCSI.

Configure External Storage

If you have selected an HBA port in the I/O Ports tab, then you can configure the partition image to use an external storage as a boot LUN using the following options:

- **Configure using Partition Image Console**: Choose this option if you wish to configure the external storage using the partition image console.

  If you choose this option, then you must select the Target Boot LUN when you install the OS using the partition image console. To know more about selecting the external Boot LUN using the partition image console, see the ClearPath Forward Installation and Getting Started Guide.
- **Configure Target Boot LUN Now**: Choose this option if you wish to configure the external storage using the Fabric Manager. If you choose this option, provide appropriate values in the following fields:
  - **Target WWPN**: Type the WWPN address in hexadecimal format. For example, 11:22:33:44:AB:CD:EF:AD.
  - **Target LUN No.**: Type the target LUN number. This number should be between 0 and 255.
  - **Primary Boot Path**: Select the path that you want to assign as the primary boot path. The default value is the HBA port that you have selected.

Notes:

- *Ensure that your storage administrator configures the LUN on the external storage device appropriately, factoring in the operating system vendor requirements, operating system, and the application configurations in blueprint and gold image, partition memory configuration, and so on. Refer to Windows and Linux documentation to determine an appropriate LUN size.*
- *At any point of time, if you wish to decommission this partition image you should erase the content of the external LUN. To know more about erasing the content of an external LUN, see the ClearPath Forward Security Guide.*

Configure Data LUN

You can configure a LUN of an appropriate size as the data LUN for the partition image. To do this, under the **Data LUN** section and under **Internal Storage**, select the appropriate LUN. You can choose multiple LUNs.

Notes:

- *You can assign up to 7 Data LUNs for a partition image.*
- *At any point of time, if you wish to decommission this partition image and need a backup of the data on these LUNs, you should request the administrator to create a manual backup of these LUNs and then erase the contents of the LUN.*
- *If you are commissioning a Windows partition image, you must bring the associated data LUNs online after commissioning the partition image.*
- *If you are commissioning a Linux partition image, you must mount the associated data LUNs After commissioning the partition image.*

5.3.7. Viewing Summary

Note: *You should begin the commissioning process by selecting a blueprint in the* ***Blueprint*** *tab.*

The **Summary** tab displays the summary of the settings chosen for the partition image that is being commissioned.

You can perform following actions on the **Summary** tab:

Action	Description
Back	Allows you to modify the settings chosen in the previous screens.

Action	Description
Submit	Begins the commissioning process with the current settings. After the commissioning is complete, the newly commissioned partition image appears in the **Manage CPF System** pane under the respective platform. The status of the partition image after commissioning will be **RUNNING**. You can also monitor the progress of the commissioning process by referring to the logs being generated under the **Diagnostics** tab.
Cancel	Cancels the commissioning process.

5.4. Completing Installation and Configuration of a Unisys-supplied Windows Partition Image

After you commission a partition image using one of the Unisys-supplied blueprints for Windows operating systems, perform the following to complete installing and configuring the operating system:

1. 5.4.1 Completing Windows OS Installation
2. 5.4.2 Changing Credentials for Default Windows Administrator Account
3. 5.4.3 Configuring Your Windows Boot Disk
4. 5.4.4 Bringing a Data LUN Online
5. 5.4.5 Configuring Customer Corporate LAN (Public LAN) Connections for Enterprise Partition Platforms
6. 5.4.6 Configuring Storage Area Network Connections for Enterprise Partition Platforms
7. 5.4.7 Completing Windows Configuration

5.4.1. Completing Windows OS Installation

1. Using Remote Desktop Protocol (RDP) client software (for example, Remote Desktop Connection on a Windows computer), access and log on to the Fabric Management Platform.
2. On the Fabric Management Platform, use the Fabric Manager user interface to launch a console for the desired partition. (See 12.2 Accessing the Partition Image Console (Partition Desktop) for more information.)

   A partition image console window appears and the Windows setup screen prompting for the product key is displayed.

Note: *Depending on your timing, the operating system may still be going through the setup process. For Windows Server 2008 R2, you may not see any progress until after the first reboot.*

3. Depending on the operating system, do one of the following to defer entering the product key and dismiss the window:

   - For Windows Server 2012 or Windows Server 2012 R2, click **Skip**.
   - For Windows Server 2008 R2, uncheck the check box to automatically activate Windows when online, and then click **Next**.

   Windows finalizes initial setup, and the partition reboots. Required third party utilities and applications are automatically installed, and the partition reboots again. The Windows log in prompt for credentials appears.

4. Log in using the credentials specified during commissioning.

   You are logged in, and if secure fabrics were specified during commissioning, a Windows PowerShell window appears, displaying the status as the configuration script associates the partition with the secure fabrics.

When the Windows Server Manager dashboard appears, proceed to change the temporary credentials used during commissioning to a more secure name and password. For more information, see 5.4.2 Changing Credentials for Default Windows Administrator Account.

5.4.2. Changing Credentials for Default Windows Administrator Account

The partition image was commissioned using the default Administrator account (**Administrator**) and the password you specified during commissioning. These temporary credentials should only be used for commissioning, and you should change the credentials to a more secure name and password. Refer to the operating system documentation for more information on how to change credentials.

5.4.3. Configuring Your Windows Boot Disk

When you commission a Windows partition image, the boot volume where the operating system is installed (C:) is automatically configured to be a single disk drive partition with the size of the virtual disk (LUN) you chose during commissioning. If you wish to configure multiple disk drive partitions on your partition image, use the Windows Disk Management console to reduce the size of the C: partition, and then configure additional disk partitions.

5.4.4. Bringing a Data LUN Online

The initial storage policy for the Windows operating system is OfflineShared, so data LUNs (disks) for a newly commissioned partition need to be explicitly brought online.

To bring a disk online, do the following:

1. Access the Windows Disk Management console (MMC snap-in).
2. Locate the disk in the graphical view pane at the bottom of the display window.
3. In the left-hand area for the disk, right-click the label, and then select **Online**.

   The disk is brought online.

If the disk was used previously, it is in the same state as when it was last used; if the disk was not used previously, it is uninitialized.

If necessary, initialize the disk: In the left-hand area for the disk in the graphical view pane, right-click the label of the disk, select **Initialize Disk**, select your desired disks in the disk initialization dialog box, choose the partition style, and then click **OK**.

If necessary, use the graphical view pane to create disk volumes: In the right-hand area for the disk in the graphical view pane, right-click the disk, select the type of volume, and then step through the wizard.

5.4.5. Configuring Customer Corporate LAN (Public LAN) Connections for Enterprise Partition Platforms

Access the operating system or operating systems on each enterprise partition platform and configure the network settings for the public NIC ports so they can communicate with your corporate network infrastructure and access the Internet as necessary (for example, to activate operating system licenses). Unisys-supplied partition images are pre-configured to use DHCP addressing by default. According to your site policies, set the IP addresses, net masks, and gateways, configure the hosts file (on Linux), and set up routing tables if desired. For exact procedures, refer to your operating system documentation for network configuration details.

Note: *Unisys turns off the NetworkManager service for Red Hat Enterprise Linux (RHEL) partition images; do not turn on the service. The ClearPath Forward fabric uses bonded networks, and you may encounter problems when the NetworkManager service is running.*

To identify the ports allocated to your partition image, use the Fabric Manager user interface to view the partition summary of your partition, and then click **Port & Config Preview** to display a logical diagram of the ports allocated to the partition.

5.4.6. Configuring Storage Area Network Connections for Enterprise Partition Platforms

Connect the fibre channel HBA ports for each partition on your enterprise partition platform to your storage infrastructure in accordance with your switch and storage provider documentation. When configuring unique settings for the Emulex fibre channel HBAs in your ClearPath Forward fabric, you may use the Emulex OneCommand Manager (OCM) utility. A qualified version of the utility for the fabric is available from the Unisys Product Support website.

To identify the ports allocated to your partition image, use the Fabric Manager user interface to view the partition summary of your partition, and then click **Port & Config Preview** to display a logical diagram of the ports allocated to the partition.

5.4.7. Completing Windows Configuration

Activate Your Windows Operating System License

Using one of the following methods, activate your Windows operating system licenses.

Over the Internet

When the partition images on your enterprise partition platforms are connected to a public network and can access the Internet, do one of the following to activate your Windows operating system licenses over the Internet:

- For Windows Server 2012 or Windows Server 2012 R2, locate and click the flag-shaped **Action Center** icon in your system tray, and then select **Activate Windows Now (important)**.
- For Windows Server 2008 R2, click the **Activate Windows** link in the Server Manager.

By Telephone

To activate your Windows operating system licenses by telephone, do the following:

1. Obtain the product keys from the Windows Certificates of Authenticity (COAs) affixed to the partitionable enterprise partition platform (PEPP).
2. Launch a Command Prompt window with administrative privileges.
3. At the prompt, execute the following command:

   ```
   slmgr /ipk XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
   ```

   Where *XXXXX-XXXXX-XXXXX-XXXXX-XXXXX* is the product key on your COA. Be sure to use the appropriate product key according to your site implementation of licensing for partitions on your platforms.

   A message that the product key was successfully installed appears.
4. Reboot the partition.
5. Launch a Command Prompt window with administrative privileges.
6. At the prompt, execute the following command for telephone-based activation:

   ```
   slui 4
   ```

   The Windows Activation wizard appears.
7. Step through the wizard to activate your license by telephone.

Configure Time and Time Zone

Unisys-supplied Windows partition images are set to use UTC by default. If applicable, set the correct time zone and time for your location.

Configure Windows Update

No Windows updates are included in the Unisys-supplied Windows images, and the Windows Update setting in the images is not configured. If applicable, configure the Windows Update setting and install any desired updates.

Configure MTU Size

The default maximum transmission unit (MTU) size for each InfiniBand interface is set to 1500 Byte packets. If large Jumbo Packet sizes are required, set the MTU size for each InfiniBand interface to 2044 to ensure smooth data transmission over the IP-LAN secure fabric.

To configure the MTU size, access the Device Manager MMC snap-in, locate and right-click the InfiniBand interface device, and then select **Properties**. In the properties dialog box for the device, click the **Advanced** tab, select the property **Jumbo Packet**, and then set the value to **2044**. Repeat for all InfiniBand interfaces.

Note that the MTU size must be set to the same value across all interfaces that will communicate with each other. That is, if an interface is in a Linux partition, a user with administrative privileges must set or change the value for the MTU size parameter within the interface configuration file (ifcfg-bond*x.yyyy*, where *x.yyyy* identifies the vBDF and pkey for the interface respectively) of the Linux operating system to 2044.

5.5. Completing Installation and Configuration of a Unisys-supplied Linux Partition Image

After you commission a partition image using one of the Unisys-supplied blueprints for Linux operating systems, perform the following to complete installing and configuring the operating system:

1. 5.5.1 Completing Linux OS Installation
2. 5.4.5 Configuring Customer Corporate LAN (Public LAN) Connections for Enterprise Partition Platforms
3. 5.4.6 Configuring Storage Area Network Connections for Enterprise Partition Platforms
4. 5.5.4 Completing Linux Configuration

5.5.1. Completing Linux OS Installation

1. Using Remote Desktop Protocol (RDP) client software (for example, Remote Desktop Connection on a Windows computer), access and log on to the Fabric Management Platform.
2. On the Fabric Management Platform, use the Fabric Manager user interface to launch a console for the desired partition. (See 12.2 Accessing the Partition Image Console (Partition Desktop) for more information.)

   A partition image console window appears and a graphical log-in prompt is displayed.

   Note: *Depending on your timing, the operating system may still be going through the setup process.*
3. Log in using the default **root** account credentials specified during commissioning.

   Note: *For security reasons, consider changing the password. Refer to the operating system documentation for more information on how to change credentials.*

5.5.2. Configuring Customer Corporate LAN (Public LAN) Connections for Enterprise Partition Platforms

Access the operating system or operating systems on each enterprise partition platform and configure the network settings for the public NIC ports so they can communicate with your corporate network infrastructure and access the Internet as necessary (for example, to activate operating system licenses). Unisys-supplied partition images are pre-configured to use DHCP addressing by default. According to your site policies, set the IP addresses, net masks, and gateways, configure the hosts file (on Linux), and set up routing tables if desired. For exact procedures, refer to your operating system documentation for network configuration details.

Note: *Unisys turns off the NetworkManager service for Red Hat Enterprise Linux (RHEL) partition images; do not turn on the service. The ClearPath Forward fabric uses bonded networks, and you may encounter problems when the NetworkManager service is running.*

To identify the ports allocated to your partition image, use the Fabric Manager user interface to view the partition summary of your partition, and then click **Port & Config Preview** to display a logical diagram of the ports allocated to the partition.

5.5.3. Configuring Storage Area Network Connections for Enterprise Partition Platforms

Connect the fibre channel HBA ports for each partition on your enterprise partition platform to your storage infrastructure in accordance with your switch and storage provider documentation. When configuring unique settings for the Emulex fibre channel HBAs in your ClearPath Forward fabric, you may use the Emulex OneCommand Manager (OCM) utility. A qualified version of the utility for the fabric is available from the Unisys Product Support website.

To identify the ports allocated to your partition image, use the Fabric Manager user interface to view the partition summary of your partition, and then click **Port & Config Preview** to display a logical diagram of the ports allocated to the partition.

5.5.4. Completing Linux Configuration

Configure Time and Time Zone

Unisys-supplied Linux partition images are set to use UTC by default. If applicable, set the correct time zone and time for your location.

Configure Linux Update

The Linux Online Updates setting is not configured in the Unisys-supplied Linux images. If applicable, configure the Linux Online Updates setting and install any desired updates.

Registering a SUSE Linux Partition with Novell Customer Center

All SUSE Linux Enterprise Server (SLES) operating systems purchased from Unisys for a partitionable enterprise partition platform (PEPP) can be registered with the SUSE Customer Center to receive additional software, updates, bug fixes, and security patches through a single unlimited virtualization subscription.

To register a SUSE LINUX partition with a subscription activation key, do the following:

1. Launch the YaST Control Center.
2. Select **Other** in the left column.

   The Other selections are displayed.
3. Select **Novell Customer Center Configuration** in the right column to launch the application.

   The Novell Customer Center Configuration window appears.
4. Select the **Configure Now (Recommended)** option, ensure minimally the **Registration Code** check box is checked, and then click **Next**.

   The Novell Customer Center System Registration page appears.
5. Type in the email address for your Novell Customer Center account and the activation code associated with the platform hosting your partition, and then click **Submit**.

   Note: *If you have multiple organizations configured in the Novell Customer Center, and this is the first partition you are registering using a particular activation code, you may be required to select the appropriate organization from the displayed list.*

Configure MTU Size

The default maximum transmission unit (MTU) size for each InfiniBand interface is set to 1500 Byte packets. If your Linux partition will be communicating with Windows partitions in the secure fabric and large Jumbo Packet sizes are required, set the MTU size for each InfiniBand interface to 2044 to ensure smooth data transmission over the IP-LAN secure fabric.

To configure the MTU size, navigate to the **/etc/sysconfig/networking/** directory for SUSE or the **/etc/sysconfig/network-scripts/** directory for RHEL, access the interface configuration file **ifcfg-bond*X.YYYY*** (where *X.YYYY* identifies the vBDF and secure fabric subnet tag PKEY for the interface respectively), locate the **MTU=<*value*>** line, and then set or change the <*value*> parameter to **2044**.

Note that the MTU size must be set to the same value across all interfaces that will communicate with each other. That is, if an interface is in a Windows partition, be sure to use the Windows operating system Device Manager MMC snap-in to set or change the MTU size value for all InfiniBand interfaces of the Windows partition to 2044.

5.6. Backing Up Application Operating Environments on Partitionable Enterprise Partition Platforms

You may use standard operating system or third party datacenter tools to back up the Windows or Linux operating environments that contain your applications according to your site policy.

The ClearPath Forward fabric does not support bare-metal restore of partition images. If the original partition image no longer exists, you commission a new partition image, and then recover the environment of the previous partition image onto the new partition image. When backing up your Windows or Linux operating environments, you do not need to back up the EFI system partition since it is automatically created when you commission a new partition image. For more information on backup and restore tools, see 14.5 Examples of Tools for Backing Up and Restoring Application Operating Environments.

Note: *The EFI system partition is a disk partition on the boot volume used by ClearPath Forward partition images and other machines that adhere to the Unified Extensible Firmware Interface (UEFI). It contains the boot loader, device drivers, system utilities, and other information specific to the current environment of the particular partition image.*

If you intend to restore your operating environment on a different partition image, be sure that you do not include the EFI system partition from the previous partition image (if it was backed up) as part of the restore process. It may contain invalid information for the new partition image.

Note: *If you previously made changes to files on the Linux /boot/efi partition of the original partition image (for example, operating system kernel changes, initrd and efi configuration file changes, or driver updates), you may need to reapply the changes to the new partition image after the restore process.*

Section 6
Creating a Partition with a Customer-Supplied OS on a PEPP

This section provides information on creating partitions on a partitionable enterprise partition platform (PEPP) with customer-supplied operating systems.

6.1. Overview of Installing a Customer-Supplied Windows or Linux OS on a Partitionable Enterprise Partition Platform

To install a customer-supplied operating system to a partition on a partitionable enterprise partition platform (PEPP),

1. Create operating system images from your own operating system installers with the utilities provided by Unisys.

   For more information, see

   - 6.2 Customer-Supplied Windows or Linux Operating System Images on Partitionable Enterprise Partition Platforms
   - 6.3 Understanding Customer-Supplied Windows Operating System Images
   - 6.4 Understanding Customer-Supplied Linux Operating System Images
   - 6.5 Creating a Customer-Supplied Windows Operating System Image
   - 6.6 Creating a Customer-Supplied Linux Operating System Image

2. Use the Fabric Manager user interface to add the operating system images and corresponding blueprint images to the appropriate platform.

   For more information, see 6.7 Uploading Customer-Supplied Operating System Images to Fabric Manager, 6.8 Adding a Gold Image, and 6.9 Adding a Blueprint.

3. Commission a partition image that uses your operating system image on that platform.

   For more information, see 5.2 Overview of Commissioning a Partition and 5.3 Commissioning a Partition Image.

   Note: *For more information on creating secure fabrics, refer to Section 3, Creating a Secure Fabric.*

4. After configuring and customizing the operating system and application operating environment, including bringing data LUNs (disks) online, be sure to back up your partition. For more information, see 5.6 Backing Up Application Operating

Environments on Partitionable Enterprise Partition Platforms.

Note: *When configuring a software firewall on a partition image, ensure that you configure the firewall to allow incoming ping requests through the ClearPath Forward Management LAN (FM LAN). The Fabric Manager monitors the health status of a partition image through ping checks; if the ping requests on the FM LAN to the partition image are blocked by a firewall, the Fabric Manager displays a warning state for the partition image's health (but does not generate an event).*

6.2. Customer-Supplied Windows or Linux Operating System Images on Partitionable Enterprise Partition Platforms

If the operating system is supported, you can create operating system gold images from your own operating system installation media using utilities that Unisys provides:

- Customer-Supplied OS Toolkit for Windows

  Use this toolkit to create operating system gold images from Microsoft Windows image (.wim) files, available on Windows operating system installation media that you obtain from your operating system vendor (for example, a DVD), or a previously created custom Microsoft Windows image file. The .wim file is used to create an image that may be uploaded to the Fabric Manager with a paired blueprint image.

- Customer-Supplied OS Toolkit for Linux

  Use this toolkit to create operating system gold images from existing instances of Linux operating systems. The configured operating system instance and installed application stack (if supported) is used to create an image that may be uploaded to the Fabric Manager with a paired blueprint image.

When you wish to commission a partition image that uses your operating system gold image, select the paired blueprint during commissioning.

Copies of the toolkits are available from the /Unisys/Tools/ directory on the Fabric Management Platform. To download a copy to your local workstation: Access the Fabric Management Platform, locate the /Unisys/Tools/ directory, and then download the appropriate toolkit to your local workstation.

The latest versions of the toolkits are also available from the Unisys Product Support website.

6.3. Understanding Customer-Supplied Windows Operating System Images

You use the Customer-Supplied OS Toolkit for Windows to create operating system gold images from your own Microsoft Windows image (.wim) files. Microsoft Windows image files are available on Windows operating system installation media that you obtain from your operating system vendor (for example, a DVD), or a custom .wim file that you previously created.

Note: *Unattended installation answer files are not supported for custom .wim files.*

The toolkit contains a utility with a graphic user interface that enables you to create an operating system gold image as well as the required corresponding blueprint image. You then copy the gold image and blueprint image to the Fabric Management Platform, and use the Fabric Manager user interface to add the images to the appropriate platform so that you can commission a partition image that uses your operating system image on that platform.

Note that each blueprint is matched to each operating system gold image you create using the toolkit. When you use the Fabric Manager user interface to add your operating system gold image to the platform, you must also add the corresponding blueprint image. When you wish to commission a partition image that uses your operating system image, you must select the appropriate blueprint matched to the image during commissioning.

Note: *Be aware that there is limited storage for images on each partitionable enterprise partition platform (PEPP).*

Although you can use the toolkit to create images of any version of the Windows operating system, note that Unisys only supports some versions. For a list of supported Windows operating systems, access the Unisys Product Support website, navigate to the Support Site page for your release, and then click **Operating Systems**. On the Operating Systems page, click **ClearPath Forward Supported Operating Systems** to display a PDF detailing the supported operating systems for the ClearPath Forward releases.

6.4. Understanding Customer-Supplied Linux Operating System Images

You use the Customer-Supplied OS Toolkit for Linux to create operating system gold images from existing instances of supported Linux operating systems for use in your fabric environment.

Note: *For a list of supported Linux operating systems, access the Unisys Product Support website, navigate to the Support Site page for your release, and then click* ***Operating Systems****. On the Operating Systems page, click* ***ClearPath Forward Supported Operating Systems*** *to display a PDF detailing the supported operating systems for the ClearPath Forward releases.*

The toolkit is distributed as an ISO image and is a collection of scripts, tools, and blueprint files, bundled into a bootable, live Linux environment—based on open source Ubuntu software—that helps you modify (prepare) a running Linux operating system for the fabric environment. Scripts in the toolkit are used to create an image from the prepared system, as well as a corresponding blueprint image. You then copy the paired images to the Fabric Management Platform, and use the Fabric Manager user interface to add the paired images to the appropriate platform. Once the images are added, you can commission a partition image that uses your operating system image on that platform.

Note: *When you wish to commission a partition image that uses your operating system image, you must select the paired blueprint during commissioning.*

Your existing instances of Linux operating systems must be running on hardware booted in UEFI mode. Both physical systems and virtual machines are supported when they are booted in UEFI mode.

6.5. Creating a Customer-Supplied Windows Operating System Image

The Customer-Supplied OS Toolkit for Windows requires:

- A Microsoft Windows image (.wim) file as a source file

  Microsoft Windows image files are available on Windows operating system installation media that you obtain from your operating system vendor (for example, a DVD), or a custom .wim file that you previously created.

  Note: *To learn more about .wim files and creating them, refer to documentation available from the Microsoft Windows website.*

- Administrative credentials to a workstation with the following:
  - Windows 7, Windows Server 2008 R2, or later (32-bit or x64-bit).
  - Windows PowerShell 4.0 or higher.
  - Disk space of at least 2.5 times the size of the source .wim file.

    For example, if your .wim file is 8 GB, be sure you have 20 GB available disk space.

Obtaining and Launching the Toolkit

1. Access the Fabric Management Platform, locate the /Unisys/Tools/ directory, and then download the Customer-Supplied OS Toolkit for Windows to your local workstation.
2. Unzip the toolkit package to your preferred location on your workstation.
3. Launch a Command Prompt window with administrative privileges.
4. Change the directory to where you unzipped the toolkit package.
5. Execute the following command:

```
powershell -executionpolicy bypass -File .\Windows-CSO-Tookit.<version>.ps1
```

   Where *<version>* is the version number in the filename.

Using the Toolkit to Create Images

To create an operating system image, launch the Customer-Supplied OS Toolkit for Windows, and do the following:

1. In the **Select Source WIM File** field, browse to your desired Microsoft Windows image (.wim) file.
2. In the **Select OS Image** field, select your desired operating system from the drop-down list.

   Note: *If your source .wim file is the Microsoft install.wim file, only the operating systems supported for the release are listed.*

3. In the **Select Target Folder** field, browse to the location where you want to store the operating system image you are creating and its corresponding blueprint.
4. In the **Image Name** field, if you do not wish to use the default name, type in a name for your image. The filenames for the image and corresponding blueprint will contain the text in this field, as well as automatically generated version information (for example, date and toolkit version number).

   Note: *Do not use spaces in the filename.*
5. In the **Image Description** field, fill in a short description.

   Note: *This description is displayed on the Fabric Manager user interface, and must be less than 32 characters.*
6. When all the required information is entered, click **Build Images**. Depending on your image size, the process can take 30 minutes or longer.

   When the process completes, a status dialog box appears.
7. Click **OK**.
8. If desired, click **View Log** to review the build log file in Notepad.
9. Click **Exit** to quit the utility.

The resulting operating system image and its corresponding blueprint are stored at the location you specified. Use the Fabric Manager user interface to add the operating system image and its corresponding two blueprint images to the desired platform. For more information, see 6.7 Uploading Customer-Supplied Operating System Images to Fabric Manager.

Note: *Be aware that there is limited storage for images on each partitionable enterprise partition platform (PEPP).*

6.6. Creating a Customer-Supplied Linux Operating System Image

This section provides details for creating a customer-supplied Linux operating system image. In general, the process is as follows:

1. Verify that the instance of the Linux operating system you want to use for creating your image meets requirements.
2. Prepare your Linux operating system for the fabric environment by loading the required drivers and dependency packages.
3. Capture the disk contents of your prepared Linux operating system: Boot from the toolkit ISO image and run the included script for capturing data.
4. Package the captured data into a customer-supplied operating system image and create the blueprint for pairing with it: Run the mkCSOimage script included in the toolkit.

Be sure to note down the original size of the disk that you are capturing a snapshot of. During commissioning, you may need to select a LUN size that is the same size or larger.

Verifying Requirements for Linux Operating System

The instance of the Linux operating system you want to use for creating your image must meet the following requirements:

- The operating system is supported for this release.

  Note: *For a list of supported Linux operating systems, access the Unisys Product Support website, navigate to the Support Site page for your release, and then click* ***Operating Systems****.On the Operating Systems page, click* ***ClearPath Forward Supported Operating Systems*** *to display a PDF detailing the supported operating systems for the ClearPath Forward releases.*

- The operating system is installed in UEFI mode.

  The operating system must be installed on a system that can boot into UEFI mode. Systems that only boot into the legacy BIOS mode are not supported.

  Note: *Your operating system installer automatically installs in UEFI mode if the system is booted in UEFI mode.*

- The operating system only uses a single disk.

  The toolkit can only capture a single disk device; multiple disk devices are not supported.

- The size of the operating system and any additional data or applications must compress to 4 GiB or less.

  The images created by the mkCSOimage script must be 4 GiB or less. If a resulting image is larger than 4 GiB, consider creating an image with only the operating system, and then loading data or applications after you commission your partition image.

Preparing Linux Operating System for Fabric Environment

Before using the toolkit to create your image, prepare your Linux operating system for the fabric environment:

1. Note down the size of the disk your operating system is installed on so that the appropriate (minimum) disk size can be selected during commissioning.

   Note: *Depending on parameters you specify when you capture the disk contents of your prepared Linux operating system, you may need to select a disk of the same size or larger during commissioning.*

2. Use the Unisys-CSO-prep.sh script in the toolkit to install required drivers:

   a. Present the contents of the toolkit ISO image to the operating system: Either directly mount the toolkit ISO image, or burn the toolkit ISO image to DVD and then use the physical media.

   b. Navigate to the Unisys directory at the root of the DVD, and then locate and run **Unisys-CSO-prep.sh**.

      The script verifies that the operating system is booted in UEFI mode, and performs a check for required packages. If dependencies are missing, the script attempts to install them, and reports an error if installation does not succeed.

The script then installs the following:

- Dynamic Kernel Module Support (DKMS) software
- Mellanox InfiniBand drivers
- Usysreport – a Unisys diagnostic tool
- ClearPath Forward Hardening Tool for Linux

Capturing a Snapshot of the Linux Operating System

After preparing your Linux operating system for the fabric environment, capture a snapshot:

1. Shutdown your Linux operating system and boot using the toolkit ISO image or DVD that you used to prepare your operating system.

   Note: *The Ubuntu environment in the toolkit is designed to boot in UEFI mode.*

   The Ubuntu environment in the toolkit is booted from a live CD ISO image, and the file system is a RAM disk of a size proportional to the amount of system memory. The amount of RAM disk space required for capturing your Linux environment to create a gold image and blueprint is approximately 2.5 times the size of the snapshot directory that the image-capture.sh script creates, and the required space can be as large as 9 GB. If the amount of available system memory is too small to provide sufficient RAM disk space, you can access and use external storage such as a directly connected storage device, or network storage with CIFS or NFS protocol. If you chose to use an external storage device, ensure the device is mounted and the files created by the toolkit are assigned to the device.

   When the boot finishes, the Unisys CSO Menu appears.

2. Type **1**, and then press **Enter** to initiate a script to capture a snapshot of your prepared Linux operating system.

   This script creates files to be used later to create a gold image, and requires information for creating the snapshot files. If there is missing information, the script interactively prompts for the information.

   Note: *Since there is no default value for the device to capture, the script will prompt for the information even in quiet mode if you do not specify the option.*

3. Type in a path to a directory for containing the snapshot files, or press **Enter** to use the default directory.

4. Select the disk to capture a snapshot of and then confirm your selection, or press **Enter** to use the default selection.

5. Enter your desired capture format, or press **Enter** to use the default SMART format.

   Notes:

   - *If your prepared Linux environment uses btrfs or LVM, you can use either the RAW format or the SMART format when capturing the snapshot of your Linux operating system. If your environment uses a combination of file systems that includes btrfs or LVM, Unisys recommends using the SMART format to intelligently capture the environment.*
   - *If you specify the RAW format, during commissioning, you must select a disk of the same size or larger than the size of the disk you are capturing.*

6. When queried to use proportional size increase on larger disks, enter your desired selection, or press **Enter** to use the default value Yes.

   The script proceeds to capture the snapshot, and the Unisys CSO Menu appears when the process completes.

Note: *The host computer name and password from your prepared Linux operating system will be captured. This information is retained in the partition image when you commission; that is, the input in the host computer name and password fields during commissioning is ignored.*

Packaging Snapshot Into Customer-Supplied Operating System Image and Creating Corresponding Blueprint

After capturing a snapshot of your operating system, do the following to convert the snapshot into a customer-supplied operating system image and create the corresponding blueprint:

1. Type **2**, and then press **Enter** to initiate a script for creating the image and corresponding blueprint.
2. Type in the path to the directory containing the snapshot files you captured previously, or, if you used the default directory when capturing the snapshot files, press **Enter** to point to the default directory.
3. Press **Enter** to point to the default directory containing the blueprint templates, or, if you wish to point to a unique blueprint template (for example, if directed by support personnel), enter the name of the directory.
4. Type in a path to the directory where you want to store the image you are creating and its blueprint.
5. Type in a number between 1 and 6 to number your image, or press **Enter** to use the default image number 1.
6. Type in a description of the image you are creating and its blueprint, or press **Enter** to use the default description CSO-Linux-Image-1.

   Note: *This description is displayed on the Fabric Manager user interface, and must be less than 32 characters.*

7. Type in the version number for the image you are creating and its blueprint, or press **Enter** to use the default version number 1.0.0.0000
8. Type in the full path name for the directory to temporarily store working files and scripts, or press **Enter** to use the directory /tmp.

   The script creates the image and a corresponding blueprint image, and reports the location and filename of the resulting .img files, along with MD5 checksums of each file.

Use the Fabric Manager user interface to add the .img files to the desired platform. For more information, see 6.7 Uploading Customer-Supplied Operating System Images to Fabric Manager.

6.7. Uploading Customer-Supplied Operating System Images to Fabric Manager

1. Copy the operating system image you created to the Fabric Management Platform.
2. Copy the corresponding blueprint image to the Fabric Management Platform.

   For Windows, the blueprint is supplied with the Customer-supplied OS Toolkit for Windows.

   For Linux, the blueprint is created by the mkCSOimage script in the Customer-supplied OS Toolkit for Linux.
3. Using the Fabric Manager user interface, add the image and the blueprint to the appropriate platform. See 6.8 Adding a Gold Image and 6.9 Adding a Blueprint for more information.

   Note: *Depending on the .img filename you specified when creating your operating system image, you may see a similar descriptive name appear in the Image Name column of Fabric Manager. Fabric Manager does not display the actual filename of the uploaded image; that is, it does not display the .img filename.*

You can now use the blueprint to commission a partition image that uses your operating system image on that platform. See 5.3 Commissioning a Partition Image for more information.

6.8. Adding a Gold Image

When you add a Gold Image, it is copied to the internal SAS disk of an associated EPP, so that it is available for commissioning.

Notes:

- *Unisys-supplied Gold Images are placed on a particular EPP's SAS disk at the factory.*
- *You must use Internet Explorer 11 or any latest version of Firefox or Chrome browser to add a gold image.*

You can add a Unisys-supplied gold image to a selected platform from the following sources:

- Physical media through the Fabric Manager Platform, DVD, or USB.
- File store on a server that resides outside the fabric, which can be accessed through the Fabric Manager.
- From the FFM Repository residing on the FMP.

You can also create and add operating system images to a selected platform. If you do so, you must also add the corresponding blueprint included in the toolkit for your operating system image.

To add a Gold Image

1. On the Fabric Manager user interface, click **Advanced Settings**.
2. Click the **Images** tab.

   The list of available images appears.
3. Verify that the name of the image you want to add is unique (does not appear on the list). If the name already appears, delete the existing image before adding the new gold image.

   To know more about deleting an existing image, refer the *ClearPath Forward Administration and Operations Guide.*
4. Click **Upload**.

   The Upload Image window appears.
5. Select the desired platform(s) to which you want to upload the image.

   Notes:

   - *To add an image to all the available platforms, select* ***Platform Name****.*
   - *Fabric Manager does not allow you to simultaneously upload multiple images to a platform.*
6. Under the **Select Image (FFM Repository/Choose a new File)** section, do either of the following:

   - Under **FFM Repository**, select the image that you want to upload.

     Note: *The FFM Repository is a repository folder on the FMP that stores the images. The path to access the images folder on the FMP is /FFM-Repo/images. Images are downloadable from a DVD or from the Unisys Support site to this folder. Images are also added to the FFM Repository when they are uploaded to a platform from any other location. Unisys recommends periodic deletion of older or unused versions of images. This helps to avoid issues that applications may encounter due to unavailability of adequate storage space.*
   - Under **New**, navigate to the location of the image file and click **Open**.

7. Click **Upload**.

   The uploading process continues in the background. In the **Events** tab the status of this activity is listed as **INITIATED**.

   During the upload, a new window appears that displays the upload progress. Once the upload is completed, this window closes and the events are entered in Event Console.

   Note: *The maximum size of the file that can be uploaded is 15 GB.*

8. After the event status becomes **SUCCESS**, click **Synchronize**.

   The uploaded image appears in the list of available images. The status of image upload appears under **Events** tab as an event **INITIATED** for both Fabric Manager platform and selected enterprise partition platform. Once the status of the event becomes **SUCCESS** for the platform, click **Synchronize** to view the uploaded image.

Notes:

- *If you are uploading the image from FMP to the platform, then the Event Console displays two events - one with INITIATED status and another with SUCCESS status.*
- *If you are uploading the image from any other location, the Event Console displays the following:*
  - *One event with INITIATED status and another with SUCCESS status for the upload operation from the location to the FMP.*
  - *One event with INITIATED status and another with SUCCESS status for the upload from the FMP to the platform.*

6.9. Adding a Blueprint

When you add a blueprint, it is copied to the internal SAS disk of an associated EPP. This makes the blueprint available for commissioning.

Notes:

- *Unisys-supplied blueprints are placed on a particular EPP's SAS disk at the factory.*
- *You must use Internet Explorer 11 or any latest version of Firefox or Chrome browsers to add a blueprint.*

You can add a Unisys-supplied blueprint to a selected platform from the following sources:

- Physical media such as internal SAS disks of the Fabric Manager Platform , DVD, or USB memory device.
- File store on a server that resides outside the fabric, which can be accessed through the Fabric Manager.
- From the FFM repository residing on the FMP.

See 6.2 Customer-Supplied Windows or Linux Operating System Images on Partitionable Enterprise Partition Platforms for more information.

To add a blueprint

1. On the Fabric Manager user interface, click **Advanced Settings**.
2. Select the **Blueprints** tab.

   The list of available blueprints appears.
3. Verify that the name of the blueprint you want to add is unique (does not appear on the list). If the name already appears, delete the existing blueprint before adding the new blueprint.For more information, refer the *ClearPath Forward Administration and Operations Guide*..

   Note: *Each blueprint must have a unique name.*
4. Click **Upload**.

   The Upload Blueprint window appears.
5. Select the desired platform(s) to which you want to add a blueprint.

   Notes:

   - *To add a blueprint to all the available platforms, select* ***Platform Name****.*
   - *Only the platforms on which s-Par is running are listed in the Upload Blueprints window.*
6. Under the **Select Blueprint (FFM Repository/Choose a new File)** section, do either of the following:

   - Under **FFM Repository**, select the blueprint that you want to upload.

     Note: *The FFM Repository is a repository folder on the FMP that stores the blueprints. The path to access the blueprint folder on the FMP is /FFM-Repo/blueprints. Blueprints are downloadable from a DVD or from the Unisys Support site to this folder. Blueprints are also added to the FFM Repository when they are uploaded to a platform from any other location. Unisys recommends periodic deletion of older or unused versions of blueprints. This helps to avoid issues that applications may encounter due to unavailability of adequate storage space.*
   - Under **New**, navigate to the location of the blueprint and click **Open**.
7. Click **Upload**.

   The uploading process continues in the background. In the **Diagnostics** tab the status of this activity is listed as **INITIATED**.

   During the upload, a new window appears that displays the upload progress. Once the upload is completed, this window closes and the events are entered in Event Console.

   Note: *The maximum size of the file that can be uploaded is 15 GB.*
8. After the event status becomes **SUCCESS** for the selected platform, click **Synchronize**.

   The uploaded blueprint appears in the list of available blueprints.

The status of blueprint upload appears under the **Diagnostics** tab as an event **INITIATED** for both the Fabric Management Platform and the selected enterprise partition platform. Once the status of the event becomes **SUCCESS** for the enterprise partition platform, click **Synchronize** to view the uploaded blueprint.

Notes:

- *If you are uploading the blueprint from FMP to the platform, then the Event Console displays two events - one with INITIATED status and another with SUCCESS status.*
- *If you are uploading the blueprint from any other location, the Event Console displays the following:*
  - *One event with INITIATED status and another with SUCCESS status for the upload operation from the location to the FMP.*
  - *One event with INITIATED status and another with SUCCESS status for the upload from the FMP to the platform.*

6.10. Overview of Commissioning a Partition

Commissioning is the process of creating a partition image by using the Fabric Manager user interface. Commissioning associates software with hardware resources, resulting in a partition image. You begin the commissioning process by selecting a software template called a blueprint. The blueprint supplies the gold image (that is, the software that will run in the partition). Then you specify values for any additional required attributes, such as the following:

- Partition name
- Host Computer Name where the partition will reside
- Partition chassis
- Number of processor cores in the partition
- Partition memory size (a default value is provided, which you may change)
- Whether or not hyperthreading is enabled
- NIC ports and HBA ports owned by the partition
- Whether a NIC port is shared
- Whether a NIC port is teamed
- Whether a NIC port has peer forwarding enabled
- Boot disk storage space (LUN size) for the internal boot drive (if any)
- Number of data LUNs and their size
- Whether or not the partition image is started after a platform reboot
- Whether or not the partition image is part of one or more secure fabrics

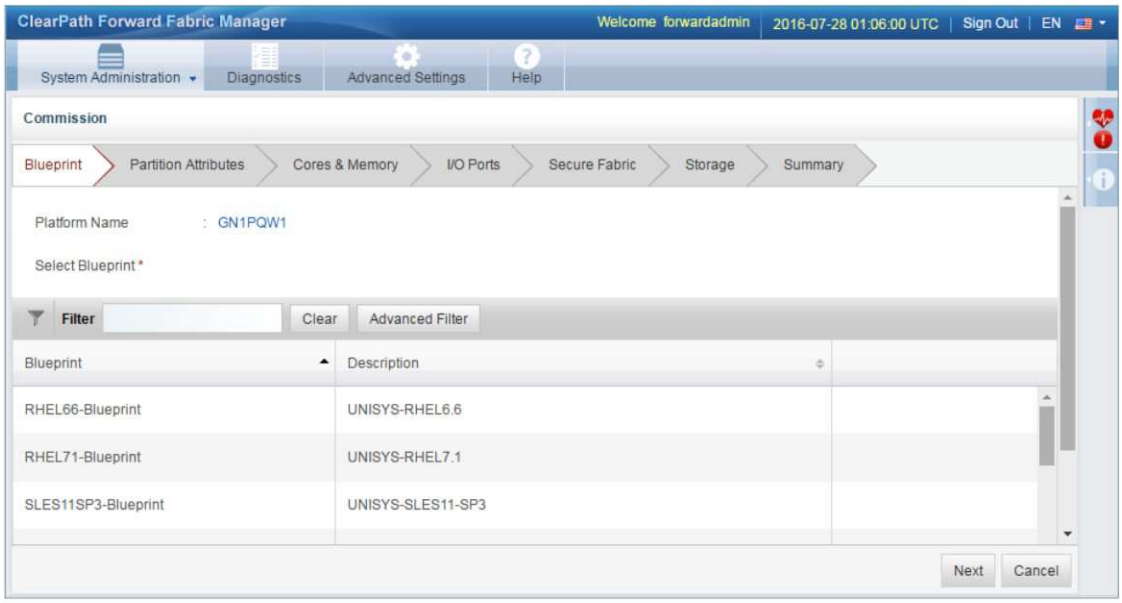
The Fabric Manager then creates (commissions) the partition image.

As a result of the commissioning process, the partition image

- Is enabled
- Is in a running state
- Appears in the left navigation pane of the Fabric Manager

At this point, the partition image has been assigned hardware resources and is capable of being booted and executing a customer workload.

The following figure shows the initial commissioning screen, in which you select the blueprint.



007645A

6.11. Commissioning a Partition Image

Note: *The commissioning procedure described in this section is applicable for platforms that are based on s-Par version 4.2 and above. If you are commissioning a partition image on a platform that is based on s-Par versions 4.1 or lesser, then refer to the* Installation, Administration, and Operations Guide *from the 2.0 documentation library under the ClearPath Forward portion of the Unisys Product Support site available at* https://www.support.unisys.com/search2/DocumentationSearch.aspx?ID=8088&pla=ps&nav=ps

Ensure that the required resources such as blueprint and gold image are available. Additionally, the Fabric Manager user interface provides information about the different partition images that you can commission on a particular platform. For more information about blueprints, gold images and partition images that you can commission on a particular platform, see the *ClearPath Forward Administration and Operations Guide* for more information.

Notes:

- *If you plan to commission the partition image on an external boot volume, verify that your storage administrator has prepared and configured the external storage device. For more information about commissioning partition images to boot from an external storage device, refer to Section 9, Configuring Partition Images to Boot from External Storage Device.*
- *While commissioning a partition image, Unisys recommends you to take the worksheet print out and manually fill the parameters of the partition being commissioned on a platform. This worksheet helps you to reconstruct the partition environment in the event of a catastrophic failure. See Appendix A, Worksheet for Commissioning, to learn more about the worksheet.*
- *You can commission a maximum of 16 NIC Ports and a maximum of 16 HBA Ports on a partition image.*
- *You can also assign a shared NIC port to a partition image. For more information about shared NIC ports, see the* ClearPath Forward Administration and Operations Guide.
- *Depending on your fabric configuration, some fields may not be editable and are greyed out.*

To commission a partition image

1. On the Fabric Manager user interface, point to **System Administration**, and then click **CPF System**.
2. Click **Platforms and Partitions**.

   The **Details: Platforms and Partitions** screen appears.
3. Select the platform on which you want to commission the partition image.
4. Click **Commission**.

   Alternatively, double-click the platform row, and then on the **Summary** tab of the platform, click **Commission**.

   A message informing that the system is discovering the resources for the commissioning appears. After discovering the required resources to commission a partition image, the Commission window appears.
5. In the Commission window, perform the steps in the respective tabs as described in the following topics and click **Submit**:
   - 5.3.1 Selecting Blueprint (Blueprint Tab)
   - 5.3.2 Setting Up Basic Partition Information (Partition Attributes Tab)
   - 5.3.3 Providing Configuration Details (Cores and MemoryTab)
   - 5.3.4 Selecting I/O Ports (I/O Ports Tab)
   - 5.3.5 Associating Secure Fabrics with Partition Image (Secure Fabric tab)
   - 5.3.6 Selecting Boot LUN and Data LUNs (Storage tab)
   - 5.3.7 Viewing Summary (View Summary Tab)

The newly commissioned partition image appears in the **Partitions** tab of the respective platform. To view the newly commissioned partition, on the **Details: Platforms and Partitions** screen, select the **Platforms** tab, and double-click the platform on which the partition was commissioned.

Post-commissioning Tasks

After commissioning a Unisys-supplied partition image, you should perform post-commissioning tasks to complete installing and configuring the operating system. For more information about the post-commissioning tasks, refer to the following:

- 5.4 Completing Installation and Configuration of a Unisys-supplied Windows Partition Image
- 5.5 Completing Installation and Configuration of a Unisys-supplied Linux Partition Image

6.11.1. Selecting Blueprint

In the **Blueprint** tab, select the desired blueprint and then click **Next**.

The Partition Attributes tab appears.

6.11.2. Setting Up Basic Partition Information

Note: *You should begin the commissioning process by selecting a blueprint in the* ***Blueprint*** *tab.*

In the **Partition Attributes** tab, provide appropriate information in the following fields and then click **Next**:

- **Partition Image Name***: Type a name for the partition image. This should be unique across the fabric because it is required for monitoring the state and health of the partition images within FM LAN subnet. This field is mandatory.

  Notes:

  - *The maximum length of the partition image name can be 15 alphanumeric characters along with "-". The name cannot start with the character "-".*
  - *The following is a list of names that you cannot use to name a partition image:*

0	forward-system	forwardsystem	localhost
FMP-1	FMP-2	secure-fabric	securefabric
secure-fabrics	securefabrics	ip-lan	iplan
fmlan	fm-lan	hdlan	hd-lan
physical-fabric	physicalfabric	physicalfabrics	physical-fabrics
switch	switches	forwardsystems	cpf-system

- **Host Computer***: Type the name of the host computer. This field is mandatory.

  Notes:

  - *The host computer name should be unique across the fabric if partition images are connected within the same customer LAN subnet.*
  - *The maximum length of the host computer name can be 15 alphanumeric characters along with "-". The name cannot start with the character "-".*

- **Initial State on Platform Reboot**: Select an option to set the initial state of the partition after a platform reboot. The available options are **Running** and **Stopped**. The default option is **Running**.

  Note: *The Initial State value does not apply to the partition images that are currently disabled.*

- **Description**: Type a description for the partition image. This field is optional.

  Note: *Provide a meaningful description for the partition image. The maximum length of the description can be 256 alphanumeric characters along with space, "-", and ".". The length of any word in the description should not exceed 20 characters. It is recommended to add details of the ports added to the partition.*

- **Login Credentials**: Type a password in the **Password*** field and confirm the password in the **Confirm Password*** field. This field is mandatory.

  Notes:

  - *This password is used by the default Administrator (Windows) or root (Linux) account during commissioning for initial setup of the operating system. These credentials should only be used for commissioning and you should change these temporary credentials when you complete the initial installation and configuration of your operating system. Refer to the operating system documentation for more information.*
  - *You may enter a fictitious value if you are commissioning a Linux partition image from customer-supplied images. The host computer name and password from your prepared Linux operating system are captured as part of the image that you have created. Use that information to access your Linux partition image; the information in the host computer name and password fields during commissioning is ignored.*

6.11.3. Providing Configuration Details

Note: *You should begin the commissioning process by selecting a blueprint in the* ***Blueprint*** *tab.*

In the **Cores & Memory** tab, provide information in the appropriate fields and then click **Next**. The following table provides details about various fields in the **Cores & Memory** tab:

Field	Action
Partition Chassis	Choose the required partition chassis; for example, Chassis-B.
Cores	Choose the number of cores you want to assign to the partition image. The number of cores available depends on the partition chassis that you have chosen. The default value is 1.
Enable Hyper-Threading	Select the check box to enable selection of two logical processors per core. ***Note:*** *If Hyper-Threading is not supported by the platform or chassis, then this option is not available.*
Logical Processors	Displays the number of logical processors, based on the number of cores.
Memory	Choose the memory size that you want to assign to the partition image. The default value is 2. The memory range available depends on the partition chassis that you have chosen. The minimum value that can be chosen is 2 GB. ***Notes:*** • *Secure fabrics consume more memory. If you are planning to associate the partition image to a secure fabric, see the* ClearPath Forward Administration and Operations Guide *for detailed information about memory usage by secure fabrics.* • *If you are assigning a larger memory, then the Fabric Manager might take longer time to commission the partition image. For example, if you have assigned a memory of 20 TB size, then the Fabric Manager might take about 30 minutes to commission the partition image.*

6.11.4. Selecting I/O Ports

Note: *You should begin the commissioning process by selecting a blueprint in the* ***Blueprint*** *tab.*

In the **I/O Ports** tab, perform the following actions and then click **Next**:

1. (Optional) Select a NIC Port.

   Under **NIC Ports**, you can do the following:

   - Click on the required dedicated port.

     The Port Settings window appears. Select the **Assign** option, and click **OK**. The selected port icon changes to  .

   - Click on the required shared port.

     The Select Logical Ports window appears. This window displays details of the logical ports.

     a. Click on the required logical port.

        The Port Settings window appears.

     b. Under the **Select Action** section, select the **Assign** option.

     c. Set the attributes of the logical port:

        - (Optional) To enable teaming of the logical port, under the **Configure Attributes** section, select the **Teaming** check box.
        - (Optional) To enable peer forwarding of the logical port, under the **Configure Attributes** section, select the **Peer Forwarding** check box.

        Note: *You can enable/disable Teaming/Peer-Forwarding on the logical ports only if they were enabled on the physical port. For more information on NIC Teaming, see the* ClearPath Forward Administration and Operations Guide.

     d. Click **OK**.

        The selected logical port icon changes to  .

2. (Optional) Select an HBA Port.

   You can associate an HBA port if you wish to commission the partition image on an external boot volume. To do this, under **HBA Ports**, click on the required port, then on the Port Settings window, select the **Assign** option, and click **OK**.

Notes:

- *You can select a maximum of 16 NIC ports and 16 HBA ports.*
- *A range of BDFs is applicable for NIC and HBA ports. You can reserve a Bus Device Function (BDF) for a partition. This enables easy mapping of an application to a persistent interface name with which the BDF is identified. When you Disable a port, a BDF from the range of BDFs is reserved for the partition. When required, you can Assign the BDF to the port. The BDF is then mapped to the port. To disable, click on the required port and then in the Port Settings window select the Disable option.*

- *If you are choosing a custom BDF, then it is appropriate to first select function 0 and then select the functions from 1 to 7. If you do not select function 0, then the Unisys aa78 device will be added automatically. This is applicable for each custom device number.*
- *If you are not choosing a custom BDF and not assigning port 0, then the Unisys aa78 device will be added automatically. This is applicable for each slot.*

Understanding the Legends on the I/O Ports Tab

The **I/O Ports** tab displays the port icons according to status of the ports. For example, an available port and an used port are represented by two different port icons. Icons display the status of Dedicated ports, Shared ports and Boot path ports.

Note:

- *Dedicated port: Can be used by only one partition at a time.*
- *Shared port: Can be logically be assigned multiple times.*
- *Boot path port: Primary boot path that connects to external boot volume.*

The following table provides information about the various port icons and the status that they represent:

Icon	Description
	Dedicated port, available to be assigned to this partition.
	Dedicated port, used by another partition. Cannot be assigned to this partition.
	Dedicated port, selected but yet to be assigned to this partition.
	Dedicated port, already in use by this partition.
	Dedicated port, selected to disable, not yet disabled. Has an allotted VBDF number, but is unused by this partition. Can be used later by this partition or by other partitions.
	Dedicated port, disabled by this partition. Has an allotted VBDF number, but is unused by this partition. Can be used later by this partition or by other partitions.
	Dedicated port, used previously by this partition and later released. Encountered conflict on attempt to re-use, if currently used by other partition.

Icon	Description
	Dedicated port, selected to release, but not yet released for this partition.
	Dedicated port, status is unknown.
	Shared port, with available logical ports. Details displayed on hover or click on icon.
	Shared port, with no available logical ports. All are used by other partitions.
	Shared port, multiple logical ports selected to be assigned to this partition.
	Shared port, all logical ports already in use by this partition.
	Shared port, where one or more logical ports previously used by this partition and later released. Encountered conflict on attempt to re-use, if at least one port is currently used by other partition.
	Boot path port, connecting to external boot volume, already in use by this partition.
	Boot path port, connecting to external boot volume is disabled.
	Boot path port, previously connecting to external boot volume for this partition, but later released. Encountered conflict on attempt to re-use if currently used by other partition.

6.11.5. Associating Secure Fabrics with Partition Image

Note: *You should begin the commissioning process by selecting a blueprint in the* ***Blueprint*** *tab.*

Prerequisites:

- You should have assigned sufficient memory to the partition image because the secure fabrics consume more memory. For more information about the memory usage by secure fabrics see the *ClearPath Forward Administration and Operations Guide*.
- If you are planning to associate a Windows partition image to a secure fabric, see the *ClearPath Forward Administration and Operations Guide* to know about the restrictions on Windows partitions associated with secure fabrics.

In the **Secure Fabric** tab, perform the following actions and then click **Next**:

1. Select one or more secure fabrics that you want to associate with this partition.

   Note: *Fabric Manager allows you to associate a partition image to more than one secure fabric.*

2. (Optional) You can enable the FM LAN, by selecting the **FM-LAN** check box. The FM LAN is disabled by default.

> **Caution**
>
> Before you enable the FM-LAN option, it is important that you understand the security risks associated with the use of the FM LAN. It is possible for an FM LAN Ethernet switch monitored by the Fabric Manager to have an access vulnerability. For more information on the security risks associated with the FM LAN, refer to the *ClearPath Forward Security Guide*.

3. Select a logical port from the **Logical Ports (BDF)** drop-down list of the selected secure fabric.

   The Bus Device Function (BDF), also called as logical port, identifies the logical port. You can assign the same logical port for multiple secure fabrics.

Note: *If you are associating the secure fabrics without assigning the first logical port, then the Unisys aa78 device will be added automatically.*

For more information about secure fabrics, see the *ClearPath Forward Administration and Operations Guide*.

6.11.6. Selecting Boot LUN and Data LUNs

Note: *You should begin the commissioning process by selecting a blueprint in the* ***Blueprint*** *tab.*

In the **Storage** tab, you can do the following:

Configure Internal Storage

Under the **Boot LUN** section, and under **Internal Storage**, select the appropriate LUN size in the **LUN Size – No.** drop-down list.

LUNs are identified by the ID number. For example, ID1, ID2, and so on. Once you select a LUN as the Boot LUN, it will not be available for selection as a Data LUN.

The following list provides general guidelines on the minimum internal storage that you may want to choose, depending on your OS and External Storage selection. The storage sizes listed below are indicative only and the LUN size may need to be increased depending on the amount of memory that you assigned to the partition image. For example, if you assign 3 TB of memory to the partition image, then a LUN size of 110 GB is required:

- A LUN size of at least 60 GB if you are commissioning a Windows partition image from Unisys-supplied images, and the boot volume is on internal storage.
- A LUN size of at least 20 GB if you are commissioning a Linux partition image from Unisys-supplied images, and the boot volume is on internal storage.
- A LUN of at least the size of the original disk size that the operating system you captured is installed on if you are commissioning a Linux partition image from customer-supplied images, and the boot volume is on internal storage.
- A LUN of the smallest disk size (for example, 1 GB) for containing necessary drivers, if the boot volume is on external storage and you will be configuring your partition to boot from an external storage device over fibre channel.
- A LUN size of at least 20 GB if you are commissioning a Linux partition image that you will be configuring to boot from an external storage device over iSCSI.

Configure External Storage

If you have selected an HBA port in the I/O Ports tab, then you can configure the partition image to use an external storage as a boot LUN using the following options:

- **Configure using Partition Image Console**: Choose this option if you wish to configure the external storage using the partition image console.

  If you choose this option, then you must select the Target Boot LUN when you install the OS using the partition image console. To know more about selecting the external Boot LUN using the partition image console, see the ClearPath Forward Installation and Getting Started Guide.
- **Configure Target Boot LUN Now**: Choose this option if you wish to configure the external storage using the Fabric Manager. If you choose this option, provide appropriate values in the following fields:
  - **Target WWPN**: Type the WWPN address in hexadecimal format. For example, 11:22:33:44:AB:CD:EF:AD.
  - **Target LUN No.**: Type the target LUN number. This number should be between 0 and 255.
  - **Primary Boot Path**: Select the path that you want to assign as the primary boot path. The default value is the HBA port that you have selected.

Notes:

- *Ensure that your storage administrator configures the LUN on the external storage device appropriately, factoring in the operating system vendor requirements, operating system, and the application configurations in blueprint and gold image, partition memory configuration, and so on. Refer to Windows and Linux documentation to determine an appropriate LUN size.*
- *At any point of time, if you wish to decommission this partition image you should erase the content of the external LUN. To know more about erasing the content of an external LUN, see the ClearPath Forward Security Guide.*

Configure Data LUN

You can configure a LUN of an appropriate size as the data LUN for the partition image. To do this, under the **Data LUN** section and under **Internal Storage**, select the appropriate LUN. You can choose multiple LUNs.

Notes:

- *You can assign up to 7 Data LUNs for a partition image.*
- *At any point of time, if you wish to decommission this partition image and need a backup of the data on these LUNs, you should request the administrator to create a manual backup of these LUNs and then erase the contents of the LUN.*
- *If you are commissioning a Windows partition image, you must bring the associated data LUNs online after commissioning the partition image.*
- *If you are commissioning a Linux partition image, you must mount the associated data LUNs After commissioning the partition image.*

6.11.7. Viewing Summary

Note: *You should begin the commissioning process by selecting a blueprint in the* ***Blueprint*** *tab.*

The **Summary** tab displays the summary of the settings chosen for the partition image that is being commissioned.

You can perform following actions on the **Summary** tab:

Action	Description
Back	Allows you to modify the settings chosen in the previous screens.

Action	Description
Submit	Begins the commissioning process with the current settings. After the commissioning is complete, the newly commissioned partition image appears in the **Manage CPF System** pane under the respective platform. The status of the partition image after commissioning will be **RUNNING**. You can also monitor the progress of the commissioning process by referring to the logs being generated under the **Diagnostics** tab.
Cancel	Cancels the commissioning process.

6.12. Backing Up Application Operating Environments on Partitionable Enterprise Partition Platforms

You may use standard operating system or third party datacenter tools to back up the Windows or Linux operating environments that contain your applications according to your site policy.

The ClearPath Forward fabric does not support bare-metal restore of partition images. If the original partition image no longer exists, you commission a new partition image, and then recover the environment of the previous partition image onto the new partition image. When backing up your Windows or Linux operating environments, you do not need to back up the EFI system partition since it is automatically created when you commission a new partition image. For more information on backup and restore tools, see 14.5 Examples of Tools for Backing Up and Restoring Application Operating Environments.

Note: *The EFI system partition is a disk partition on the boot volume used by ClearPath Forward partition images and other machines that adhere to the Unified Extensible Firmware Interface (UEFI). It contains the boot loader, device drivers, system utilities, and other information specific to the current environment of the particular partition image.*

If you intend to restore your operating environment on a different partition image, be sure that you do not include the EFI system partition from the previous partition image (if it was backed up) as part of the restore process. It may contain invalid information for the new partition image.

Note: *If you previously made changes to files on the Linux /boot/efi partition of the original partition image (for example, operating system kernel changes, initrd and efi configuration file changes, or driver updates), you may need to reapply the changes to the new partition image after the restore process.*

Section 7
Creating a Partition with a Customer-Supplied OS on a NEPP

This section provides information on installing a customer-supplied operating system on a nonpartitionable enterprise partition platform (NEPP).

7.1. Overview of Installing a Customer-Supplied OS on a Nonpartitionable Enterprise Partition Platform

To install a customer-supplied operating system on a nonpartitionable enterprise partition platform (NEPP) that is currently monitored and managed by the Fabric Manager,

1. If you do not have credentials with the following parameters for the platform management card of the nonpartitionable enterprise partition platform, contact Unisys to create a new user ID and password:
   - Role: Operator
   - Login to platform management card: Enabled
   - Access Virtual Console: Enabled
   - Access Virtual Media: Enabled
2. If necessary, download any needed drivers so that they will be available during the installation.

   For more information, see 7.2 Obtaining and Installing Drivers and Firmware.
3. Copy your operating system installation media image to the Fabric Management Platform.

   For more information, see 7.3 Making Operating System Installation Media Image Available for Installation.
4. Ensure the enterprise partition platform's RAID controller is configured with the desired LUNs. If necessary, modify the RAID configuration of the platform.

   For more information, see 7.4 Modifying RAID Configuration of the NEPP.
5. Install and configure your operating system.

   For more information, see one of the following:
   - 7.5 Installing and Configuring Windows Server
   - 7.6 Installing and Configuring SUSE LINUX Enterprise Server

- 7.7 Installing and Configuring Red Hat Enterprise Linux

Note: *When configuring a software firewall on a partition image, ensure that you configure the firewall to allow incoming ping requests through the ClearPath Forward Management LAN (FM LAN). The Fabric Manager monitors the health status of a partition image through ping checks; if the ping requests on the FM LAN to the partition image are blocked by a firewall, the Fabric Manager user interface displays a warning state for the partition image's health (but does not generate an event).*

6. If desired, associate your NEPP with a given secure fabric.

   For more information, refer to the *ClearPath Forward Administration and Operations Guide*.

7.2. Obtaining and Installing Drivers and Firmware

Latest interim corrections, patches, fixes, and various packages containing new adapter drivers and firmware are available for download from the Unisys Product Support website.

Note: *The Unisys Product Support website is constantly being updated. Driver and firmware files are subject to change at any time.*

1. Using a web browser, navigate to www.support.unisys.com and sign in.
2. On the Product Support Home page, expand **ClearPath Forward** if necessary, and then click **ClearPath Forward**.

   The Support Site page for the product appears.
3. Click **Drivers and Downloads**.

   The Drivers and Downloads page appears.
4. On the Drivers and Downloads page, click the **Hardware** tab.

   A list of all drivers and download choices appears.
5. Locate and click the new adapter drivers or firmware that you want to download.

   A page listing all available release levels appears.
6. Under the **Level Information** section, in the **Level/Downloads** column, click the latest release level.

   A page for the release level appears.
7. Under the **Download Information** section, click the desired downloadable file, and then save it to a location of your choice.

   Note: *If you are downloading files for installing a nonpartitionable enterprise partition platform, Unisys suggests that you collect them in a single folder for later ease of use. The folder and its contents are mounted as an image during the installation process—additional files will result in unnecessarily large virtual media.*
8. Review any available comments, read-me files, or installation instructions on the page.
9. If needed, transfer the downloaded files to the Fabric Management Platform.

If the files are for an enterprise partition platform, be sure to place them in a folder on the Fabric Management Platform so that the folder can be mounted using the partition image console during installation as virtual media.

If the files are for the Fabric Management Platform, extract the contents from the archive, and then review and perform the included installation instructions.

Note: *If you are installing multiple drivers, it may not be necessary to reboot the server immediately after the installation of an individual driver. Restart the server once the installation of all drivers is complete.*

Updating Firmware of Mellanox Cards on a Nonpartitionable Enterprise Partition Platform

1. Obtain the latest Mellanox firmware: Download the firmware update package from the Unisys Product Support website.

   Note: *All Mellanox cards have the correct level of firmware installed before shipping from Unisys.*

2. Review and perform the instructions in the package to update the firmware.

7.3. Making Operating System Installation Media Image Available for Installation

1. Using Remote Desktop Protocol (RDP) client software (for example, Remote Desktop Connection on a Windows computer), access and log on to the Fabric Management Platform.
2. Copy your operating system installation media image (.iso or .img) to the Fabric Management Platform.
3. From the Fabric Management Platform, use Fabric Manager to launch a console for the desired platform. (See 12.1 Launching the Platform Management Card (PMC) Virtual Console for more information.)

   If you receive a certificate warning message, click **Continue**. A platform management console window appears.
4. Log on to the platform management console using the credentials your Unisys service representative created for you in step 1 of 7.1 Overview of Installing a Customer-Supplied OS on a Nonpartitionable Enterprise Partition Platform.
5. On the **Attached Media** tab, verify that **Attach Mode** is set to **Auto-Attach**.
6. On the Virtual Console page, click **Launch Virtual Console**.

   A partition image console window appears.
7. From the partition image console, click the **Virtual Media** menu, and then click **Connect Virtual Media**.
8. Click the **Virtual Media** menu again, and then select **Map CD/DVD**.

   The Virtual Media – Map CD/DVD dialog box appears.

9. Click **Browse**, navigate to the operating system installation media image you previously copied to the Fabric Management Platform, select the image, and then click **Open**.

   The name of the image appears in the Drive/Image File field of the Virtual Media – Map CD/DVD dialog box.

10. Click **Map Device**.
11. From the partition image console, click the **Next Boot** menu, and then click **Virtual CD/DVD/ISO**.

    The Device Selected dialog box appears.

12. Read the contents of the Device Selected dialog box, and then click **OK**.

Proceed to the installation procedure for your particular operating system to install and configure it.

7.4. Modifying RAID Configuration of the NEPP

Before installing your Windows Server operating system on your nonpartitionable enterprise partition platform (NEPP), ensure the RAID controller is configured with the desired LUNs. Depending on the model of your enterprise partition platform (EPP), see the following sections for how to modify the RAID configuration of the EPP.

Note: *The following sections assume use of the partition image console launched from the platform management console Virtual Console page. Alternatively, you can cable a keyboard, video and mouse (KVM) to your platform, or use a LAN-based KVM solution.*

EPPs Other Than the 2-Socket EPP With Processor Type E5-26*xx* v3

For EPPs other than the 2-socket EPP with processor type E5-26*xx* v3, modify the RAID configuration with the PERC BIOS Configuration Utility:

1. Log on to the platform management console using the credentials your Unisys service representative created for you in step 1 of 7.1 Overview of Installing a Customer-Supplied OS on a Nonpartitionable Enterprise Partition Platform.
2. On the Virtual Console page, click **Launch Virtual Console**.

   A partition image console window appears.

3. Using the partition image console window to monitor the boot progress, boot the platform.
4. Immediately press the **Ctrl** and **R** keys simultaneously when the **PowerEdge Expandable RAID Controller BIOS** banner displays.

   The BIOS Configuration Utility user interface is displayed.

5. Using your arrow keys and the **Tab** key to navigate the menus, view or modify the RAID configuration of the platform.

2-Socket EPP With Processor Type E5-26*xx* v3: Simple RAID Configuration

For the 2-socket EPP with processor type E5-26*xx* v3, if you wish to configure all disks as a single virtual disk with a single RAID level, modify the RAID configuration with the Lifecycle Controller Configure RAID Wizard:

1. Log on to the platform management console using the credentials your Unisys service representative created for you in step 1 of 7.1 Overview of Installing a Customer-Supplied OS on a Nonpartitionable Enterprise Partition Platform.
2. On the Virtual Console page, click **Launch Virtual Console**.

   A partition image console window appears.
3. From the partition image console, click the **Next Boot** menu, and then click **Lifecycle Controller**.
4. Click **OK**.
5. From the partition image console, click the **Power** menu, click one of the following, and then click **Yes**:
   - **Power On System** if the server is currently powered off.
   - **Reset System** if the server is currently powered on.

   The platform boots and the Lifecycle Controller user interface is displayed.
6. Click **Configure RAID**, and then step through the configuration wizard to create a new RAID configuration for the platform.

2-Socket EPP With Processor Type E5-26*xx* v3: Complex RAID Configuration

For the 2-socket EPP with processor type E5-26*xx* v3, if you wish to configure the disks as multiple virtual disks or with multiple RAID levels, change the boot mode, and then modify the RAID configuration with the PERC BIOS Configuration Utility:

1. Log on to the platform management console using the credentials your Unisys service representative created for you in step 1 of 7.1 Overview of Installing a Customer-Supplied OS on a Nonpartitionable Enterprise Partition Platform.
2. On the Virtual Console page, click **Launch Virtual Console**.

   A partition image console window appears.
3. From the partition image console, click the **Next Boot** menu, and then click **BIOS Setup**.
4. Click **OK**.
5. From the partition image console, click the **Power** menu, click one of the following, and then click **Yes**:
   - **Power On System** if the server is currently powered off.
   - **Reset System** if the server is currently powered on.

   The platform boots and the System Setup user interface is displayed.

6. Click **System BIOS**.

   The System BIOS page appears.

7. Locate **Boot Mode**, and select **BIOS**.
8. Click **Back**.
9. Click **Finish**.
10. Click **Yes** to save changes, and then click **OK**.
11. Click **Finish**, and then click **Yes** to reboot the platform.
12. Using the partition image console window to monitor the boot progress, immediately press the **Ctrl** and **R** keys simultaneously when the **PowerEdge Expandable RAID Controller BIOS** banner displays.

    The BIOS Configuration Utility user interface is displayed.

13. Using your arrow keys and the **Tab** key to navigate the menus, view or modify the RAID configuration of the platform.
14. After configuring the RAID configuration of the platform, reboot the platform.
15. Using the platform management console to monitor the boot progress, press the **F2** key to enter the BIOS setup pages.

    The System Setup user interface is displayed.

16. Click **System BIOS**.

    The System BIOS page appears.

17. Locate **Boot Mode**, and select **UEFI**.
18. Click **Back**.
19. Click **Finish**.
20. Click **Yes** to save changes, and then click **OK**.
21. Click **Finish**, and then click **Yes** to reboot the platform.

7.5. Installing and Configuring Windows Server

Except for places identified as only for a specific operating system, the following information applies to Windows Server 2008 R2, Windows Server 2012 operating systems, and Windows Server 2012 R2 operating systems.

7.5.1. Installing Windows Server

To install your Windows Server operating system, perform the following:

1. Ensure that the operating system installation media image (.iso or .img) is available from the Fabric Management Platform. See 7.3 Making Operating System Installation Media Image Available for Installation for more information.
2. Ensure the RAID controller is configured with the desired LUNs. See 7.4 Modifying RAID Configuration of the NEPP for more information.

3. For Windows Server 2008 R2, obtain the drivers needed for accessing the RAID controller. See 7.2 Obtaining and Installing Drivers and Firmware for more information.

   Copy the extracted files to the Fabric Management Platform.

4. Obtain the drivers for the Intel network interfaces and the Mellanox InfiniBand interfaces. See 7.2 Obtaining and Installing Drivers and Firmware for more information on downloading drivers.

   Copy the files to the Fabric Management Platform.

5. Verify that the drivers you obtained are collected in a single folder on the Fabric Management Platform, and nothing else is in the folder.

   Note: *The folder and its contents are mounted as an image later—additional files will result in unnecessarily large virtual media.*

6. From the partition image console, click the **Virtual Media** menu, and then select **Create Image**.

   The Virtual Media – Create Image from Folder dialog box appears.

7. For the source folder, click **Browse**, navigate to the folder on the Fabric Management Platform containing all your downloaded drivers, and then click **Open**.

   Note: *Only the folder name is displayed; contents of the folder are not displayed.*

   The name of the image appears in the Source Folder field of the Virtual Media – Create Image from Folder dialog box.

8. In the Image File Name field, specify the location for the new image file.

9. Click **Create Image**.

   An image file is created in the specified location.

10. From the partition image console, click the **Virtual Media** menu. If virtual media is not already connected, select **Connect Virtual Media**.

11. Click the **Virtual Media** menu again, and then select **Map Removable Disk**.

    The Virtual Media – Map Removable Disk dialog box appears.

12. Specify the name of the image file created in step 9, and then click **Map Device**.

13. From the partition image console, click the **Next Boot** menu, and then click **Virtual CD/DVD/ISO**.

14. From the partition image console, click the **Power** menu, click one of the following, and then click **Yes**:

    - **Power On System** if the server is currently powered off.
    - **Reset System** if the server is currently powered on.

Notes:

- *Be aware that in the next step you will only have a few seconds to press a key to boot from the installation media image. The prompt to boot from CD or DVD appears after the message "Scanning for devices. Please wait, this may take several minutes... ." If you do not press a key in time, wait for the server to finish booting, and then repeat this step.*
- *If you see the message "Loading files..." and a progress bar showing files being loaded from the CD, skip to step 16.*

15. When the server boots and the message "Press any key to boot from CD or DVD" appears, quickly press any key to start the server from the installation media image.

    Files are copied from the installation media image. This process may take a few minutes.

16. In the Windows Server setup window, select the following:
    - From the **Language to install** list, select **English** (or other preference).
    - From the **Time and currency format** list, select **English (United States)** (or other preference).
    - From the **Keyboard or input method** list, select **US** (or other preference).
17. Click **Next**.
18. Click **Install Now**.
19. If prompted, enter the product key supplied with Windows Server to activate your installation.
20. Select the version of Windows Server you want to install and click **Next**.
21. Scroll down and read the license agreement.
22. Select **I accept the license terms** and click **Next**.
23. Select **Custom**.
24. For Windows Server 2012 and Windows Server 2012 R2, skip to the next step.

    For Windows Server 2008 R2, do the following:

    a. Click **Load Driver** in the Windows Server 2008 R2 setup window.

       The Load Driver dialog box opens.

    b. Click **Browse**, navigate to the folder containing the drivers for your RAID controller, and then click **OK**.

       Note: *The folder appears on a volume with the same name as the folder containing all your downloaded drivers.*

    c. Select the PERC H710 driver, and then click **Next**.

25. When Windows Server setup window displays all available hard disk space, select one of the following options to choose or create a disk drive partition to install the operating system:

    - **Allow Setup to create a partition**

      Use this option to specify the entire hard disk as one disk drive partition: Select the unallocated space of the hard disk where you want to install the operating system, and then click **Next**.

    - **Create a partition**

      Use this option to specify a portion of the hard disk as a disk drive partition: Select the unallocated space of the hard disk where you want to install the operating system, click **Drive options (advanced)**, click **New**, type in the amount of space (in MB) when prompted to indicate the amount of space to allocate, click **Apply**, and then click **Next**.

    - **Delete a partition**

      Use this option to delete an existing disk drive partition before creating a disk drive partition using one of the methods described previously.

    The software formats the selected disk drive partition and copies applicable files to the disk drive partition. This process takes several minutes. When the installation is complete, the server restarts automatically and a prompt to change the administrator password appears.

26. Enter the new password for the administrator account, and then log on.

    A configuration wizard window appears.

27. Step through the configuration wizard for setting up naming and basic networking.

28. Use the Microsoft Server Roles and Features functions to set up the server for your specific needs.

29. If applicable, use the product key supplied with Windows Server to activate your installation.

7.5.2. Installing and Configuring Intel Network Adapters with Intel PROSet for Windows

1. Using the partition image console, on the enterprise partition desktop, use Windows Explorer to locate the volume containing the Intel drivers installation package. The volume has the same name as the folder in which you placed all your downloaded drivers.

2. Extract the contents, and review any readme files or installation instructions.

3. Depending on the installation package, either execute the .exe file or extract the contents of the .zip file.

   An installation window appears when you execute the setup program.

4. Select **Setup Options**, select **Advanced Network Services**, and then click **Next**.

5. Click **Install** to begin the installation.

When the installation completes, the wizard displays a Completed window.

6. Click **Finish**.
7. Access the Windows Device Manager, double-click the network adapter **Intel(R) Gigabit 4P X540/I350-rNDC**.

   The network adapter properties dialog box appears.
8. On the **Teaming** tab, select **Team this adapter with other adapters**, and then click **New Team**.
9. For the team name, specify the name of the ClearPath Forward Management LAN (FM LAN), and then click **Next**.

   A dialog box appears for selecting adapters to include in the team.
10. Verify that both of the **Intel(R) Gigabit 4P X540/I350-rNDC** adapters are selected, and then click **Next**.
11. For the team type, select **Adapter Fault Tolerance**, and then click **Next**.
12. Click **Finish**, and then close the properties dialog box for the team that appears.
13. Access the Windows Control Panel, click **Network and Internet**, click **Network and Sharing Center**, click **Change adapter settings**, locate and right-click the connection for the teamed adapters, and then click **Properties**.

    The Local Area Connection Properties dialog box opens.
14. On the Networking tab, click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.

    The Internet Protocol Version 4 (TCP/IPv4) dialog box appears.
15. Select **Use the following IP address**, and then type in the address the Fabric Manager displays on the partition summary page as the FM LAN IP address for the partition on the nonpartitionable enterprise partition platform (NEPP). The subnet mask field is filled out automatically.
16. Click **OK** to close the Internet Protocol Version 4 (TCP/IPv4) Properties dialog box.
17. Click **OK** to close the Local Area Connection Properties dialog.

7.5.3. Installing and Configuring Mellanox InfiniBand Adapters for Windows

1. Using the partition image console, on the enterprise partition desktop, use Windows Explorer to locate the volume containing the Mellanox drivers installation package. The volume has the same name as the folder in which you placed all your downloaded drivers.
2. Execute the drivers installation program.

   An installation wizard window appears.
3. Accept the license agreement, and click **Next** to accept the defaults on each step of the wizard.
4. At the end of the wizard, after you click **Finish**, restart the platform to apply the new drivers.

5. Locate and launch the Device Manager module (MMC snap-in) of the Windows operating system.
6. Expand the **Network adapters** node, locate and right-click one of the two Mellanox ConnectX adapters, and then select **Properties**.

   The device properties window appears.
7. Select the **Teaming** tab, and verify both Mellanox ConnectX adapters are listed in the list of adapters.
8. Click **Create**, enter a name for the team in the **Team Name** field, and then select both adapters in the list of adapters.

   The **Primary** field updates to list both adapters.
9. In the **Primary** field, select the adapter without #*<number>* in the name, where *<number>* is a variable. This is typically the adapter that is listed first.
10. Click **Commit**.
11. Click **OK** to close the device properties window.

    The Device Manager module (MMC snap-in) list of network adapters refreshes to display a new Mellanox Virtual Miniport Driver with the team name you specified in step 8.
12. Access the Windows Control Panel, click **Network and Internet**, click **Network and Sharing Center**, click **Change adapter settings**, locate and right-click the connection for the Mellanox ConnectX-3 IPoIB adapter device (the default name is "Ethernet"), and then click **Properties**.

    The Local Area Connection Properties dialog box opens.
13. On the Networking tab, click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.

    The Internet Protocol Version 4 (TCP/IPv4) dialog box appears.
14. Select **Use the following IP address**, and then type in the address the Fabric Manager displays on the partition summary page as the IP-LAN secure fabric IP address for the partition on the nonpartitionable enterprise partition platform (NEPP). The subnet mask field is filled out automatically.
15. Click **OK** to close the Internet Protocol Version 4 (TCP/IPv4) Properties dialog box.
16. Click **OK** to close the Local Area Connection Properties dialog.

7.5.4. Configuring the Windows Firewall

To configure the Windows Firewall to allow ping requests through the ClearPath Forward Management LAN, do the following:

1. For Windows Server 2012 and Windows Server 2012 R2, right-click the lower left corner of the desktop, and then click **Search**.

   For Windows Server 2008 R2, click **Start**.
2. In the Search box, type **firewall**.
3. From the search results, select **Windows Firewall with Advanced Security**.

The Windows Firewall with Advanced Security window appears.

4. In the left pane, select **Inbound Rules**.
5. In the center pane, locate the **File and Printer Sharing (Echo Request – ICMPv4-In)** rule, and in the Profile column for the rule ensure that
   - For Windows Server 2012 and Windows Server 2012 R2, **Public** is specified.
   - For Windows Server 2008 R2, **All** is specified.
6. Right-click the rule, and then select **Enable Rule**.
7. Close the Windows Firewall with Advanced Security window.

7.5.5. Configuring NMI Memory Dumps for Windows Server 2008 R2

The Fabric Manager uses a non-maskable interrupt (NMI) to force a server memory dump when you request for a dump. Windows Server 2012 and later are configured by default to take a memory dump when a NMI is received, but Windows Server 2008 R2 is not. To configure Windows Server 2008 R2 to take a memory dump when an NMI occurs, refer to the Microsoft Knowledge Base article 927069 at http://support.microsoft.com/kb/927069.

7.6. Installing and Configuring SUSE LINUX Enterprise Server

This section describes how to use documentation available from SUSE to perform a complete, basic installation and configuration of a supported SUSE LINUX Enterprise Server operating system, and configuring the operating system for the ClearPath Forward fabric.

The installation procedure is complex and familiarity with Linux installations is recommended. For optimal results, follow the directions carefully.

For custom installations and questions, refer to SUSE LINUX Enterprise Server documentation, available at http://www.suse.com/documentation/. This site provides online version of numerous SUSE Linux manuals. Click the appropriate link for your operating system, and then click the desired manual.

If applicable, before you begin the installation, make sure that you have up-to-date backups of all data currently on your server. Some of the options available during the installation process overwrite all the information on the hard disk, including user data.

Caution

Only BIOS booting is supported.

7.6.1. Installing SUSE LINUX Enterprise Server

To install your supported SUSE LINUX Enterprise Server operating system, perform the following:

1. Access the SUSE Documentation website at http://www.suse.com/documentation/, click the appropriate link for your operating system, and then review Installation Quick Start information for your operating system.

   If desired, save a copy for reference during installation.

2. Ensure that the operating system installation media image (.iso or .img) is available from the Fabric Management Platform. See 7.3 Making Operating System Installation Media Image Available for Installation for more information.

3. From the partition image console, click the **Power** menu, and then click one of the following:

   - **Power On System** if the server is currently powered off.
   - **Reset System** if the server is currently powered on.

   The server boots up, and the SUSE LINUX Enterprise Server screen with the boot/installation options appears.

4. Select the installation option, and then step through the installation screens to perform a basic installation and configuration of the operating system. If necessary, refer to the operating system installation documentation for detailed procedures.

   When specifying installation parameters, note the following configuration details:

   - When setting up disk drive partitions, if you want a hard drive layout other than the default layout that is suitable for basic use and testing, perform the following procedure. Before performing these steps, review the suggested disk drive partitions and file systems carefully; this type of configuration depends largely on the machine environment and intended usage.

     a. Select to change the partitioning or create a new partition setup.

     b. Select **Custom partitioning (for experts)**, and then click **Next**.

     c. From the available disks, select the hard disk that you want to boot from, select **Overview**, and then check the **Disk Label** field to see if the disk is labeled correctly. In almost all cases, the label is msdos.

     d. Select the **Partitions** tab.

e. If the disk label from step c is correct (that is, the label is msdos), skip to the next step.

   If the disk label from step c is not correct (that is, the label is not msdos), do the following:

   - Select **Expert**, and then select **Create New Partition Table**.
   - Select the desired type: msdos.
   - If a warning about data loss appears, click **Yes**.

f. Click **Add** to add your desired new disk drive partitions.

   Note: *It is recommended that you create a minimum of two additional disk drive partitions. You should have at least one swap partition. Its size depends on the intended server usage, amount of memory, and the size of your hard drive. You must have a root (/) partition which should define the remainder of the disk, unless you plan to create additional disk drive partitions on the disk.*

- For a supported SUSE LINUX Enterprise Server 12 operating system, do the following to set up Kdump:

  a. On the Installation Settings screen, click the **Kdump** headline.

  b. In the left pane, click **Start-Up**, and then verify **Enable Kdump** is selected.

  c. In the left pane, click **Dump Filtering**, and then set the values as desired.

  d. Click **Dump Target** and set the values as desired.

     Note: *Be sure that the dump target has enough disk space to hold the vmcore file created by the dump process. The vmcore file size varies based on the dump filtering options that you select, but it may be approximately the size of the physical memory of the system.*

  e. Click **Email Notification**, and then set the values as desired.

  f. Click **Expert Settings**, and then set the values as desired.

  g. Click **OK**.

- Disable the AutoYaST profile: In the Clone System Configuration section, choose to not write the AutoYast profile.

5. After completing initial installation, depending on your operating system, do one of the following:

   - If you are installing and configuring a supported SUSE LINUX Enterprise Server 11 operating system, proceed to configure for SUSE LINUX kernel crash dumps.

     For more information, see 7.6.2 Configuring SUSE LINUX Kernel Crash Dumps for a Supported SUSE LINUX Enterprise Server 11 Operating System.

   - If you are installing and configuring a supported SUSE LINUX Enterprise Server 12 operating system, proceed to configure the IP LAN connection for SUSE LINUX.

     For more information, see 7.6.3 Configuring the (InfiniBand) IP-LAN Secure Fabric Connection for SUSE LINUX.

7.6.2. Configuring SUSE LINUX Kernel Crash Dumps for a Supported SUSE LINUX Enterprise Server 11 Operating System

Log in as root, and do the following:

1. Verify that the kdump and kexec-tools packages are installed by typing the following commands:

   ```
   rpm -q kexec-tools
   rpm –q kdump
   ```

2. If the kdump or kexec-tools packages need to be installed, type either or both of the following commands as needed:

   ```
   yast2 -i kexec-tools
   yast2 –i kdump
   ```

3. Launch YaST using the main desktop menu.

   The YaST main panel appears.

4. Click **System** and then click **Kernel Kdump**.

   The Kdump – Start-Up screen appears.

5. In the left pane, click **Dump Filtering**, and then set the values as desired.

6. Click **Dump Target** and set the values as desired.

   Note: *Be sure that the dump target has enough disk space to hold the vmcore file created by the dump process. The vmcore file size varies based on the dump filtering options that you select, but it may be approximately the size of the physical memory of the system.*

7. Click **Email Notification**, and then set the values as desired.

8. Click **Expert Settings**, and then set the values as desired.

9. Click **Start-Up**, and then select **Enable Kdump**.

10. Click **OK**.

11. If a message appears indicating a reboot is necessary to apply the changes, click **OK**.

12. Close **YaST**.

13. If you received a message that a reboot is necessary, you can wait to reboot after you configure the IP-LAN secure fabric and FM LAN connections, and update the UDEV persistent rules.

Proceed to configure the IP-LAN secure fabric connection for SUSE LINUX. For more information, see 7.6.3 Configuring the (InfiniBand) IP-LAN Secure Fabric Connection for SUSE LINUX.

7.6.3. Configuring the (InfiniBand) IP-LAN Secure Fabric Connection for SUSE LINUX

Log in as root, and do the following:

1. Create a file named **ifcfg-ib0** in the /etc/sysconfig/network directory with the following content:

```
BOOTPROTO=none
MTU=''
STARTMODE='hotplug'
USERCONTROL='no'
```

2. Create a file named **ifcfg-ib1** in the /etc/sysconfig/network directory with the following content:

```
BOOTPROTO=none
MTU=''
STARTMODE='hotplug'
USERCONTROL='no'
```

3. Create a file named **ifcfg-bond0** in the /etc/sysconfig/network directory with the following content:

```
BONDING_MASTER='yes'
BONDING_MODULE_OPTS='mode=active-backup miimon=250'
BONDING_SLAVE0='ib0'
BONDING_SLAVE1='ib1'
BOOTPROTO='static'
IPADDR='172.31.xx.1/16'
MTU=''
STARTMODE='auto'
USERCONTROL='no'
```

   Where *xx* is the platform number for your enterprise partition platform.

   Note: *The default subnet of the IP-LAN secure fabric is 172.31. If the subnet was changed (for example, during initial hardware installation and software configuration), be sure to use the new subnet value when configuring your network connections. If needed, use Fabric Manager to check the IP-LAN secure fabric IP address for the partition on the partition summary page of the nonpartitionable enterprise partition platform (NEPP).*

Proceed to configure the FM LAN connection for SUSE LINUX. For more information, see 7.6.4 Configuring the FM LAN Connection for SUSE LINUX.

7.6.4. Configuring the FM LAN Connection for SUSE LINUX

Log in as root, and do the following:

1. Create a file named **ifcfg-eth-fmp3** in the /etc/sysconfig/network directory with the following content:

```
BOOTPROTO=none
MTU=''
STARTMODE='hotplug'
USERCONTROL='no'
```

2. Create a file named **ifcfg-eth-fmp4** in the /etc/sysconfig/network directory with the following content:

```
BOOTPROTO=none
MTU=''
```

```
STARTMODE='hotplug'
USERCONTROL='no'
```

3. Create a file named **ifcfg-bond1** in the /etc/sysconfig/network directory with the following content:

```
BONDING_MASTER='yes'
BONDING_MODULE_OPTS='mode=active-backup miimon=250'
BONDING_SLAVE0='eth-fmp3'
BONDING_SLAVE1='eth-fmp4'
BOOTPROTO='static'
IPADDR='172.29.xx.1/16'
MTU="
STARTMODE='auto'
USERCONTROL='no'
```

   Where *xx* is the platform number for your enterprise partition platform.

   Note: *The default subnet of the FM LAN is 172.29. If the subnet was changed (for example, during initial hardware installation and software configuration), be sure to use the new subnet value when configuring your network connections. If needed, use the Fabric Manager user interface to check the FM LAN IP address for the partition on the partition summary page of the nonpartitionable enterprise partition platform (NEPP).*

4. If you have a firewall, ensure that your firewall rules allow responses to incoming pings on the FM LAN.

   Note: *The Fabric Manager monitors the health status of a partition image through ping checks; if the ping requests on the FM LAN to the partition image are blocked by a firewall, the Fabric Manager user interface displays a warning state for the partition image's health (but does not generate an event).*

Proceed to update the UDEV persistent rules for SUSE LINUX. For more information, see 7.6.5 Updating the UDEV Persistent Rules for SUSE LINUX.

7.6.5. Updating the UDEV Persistent Rules for SUSE LINUX

Log in as root, and add the following two commands—one command per single line—as the first entries in the **/etc/udev/rules.d/70-persistent-net.rules** file:

```
SUBSYSTEM=="net", ACTION=="add", DEVPATH=="/devices/pci0000:00/0
000:00:1c.4/0000:08:00.0/net*", NAME:="eth-fmp3"

SUBSYSTEM=="net", ACTION=="add", DEVPATH=="/devices/pci0000:00/0
000:00:1c.4/0000:08:00.1/net*", NAME:="eth-fmp4"
```

Proceed to configure OS support of NMI generated kdumps for SUSE LINUX. For more information, see 7.6.6 Configuring OS Support of NMI Generated Kdumps for SUSE LINUX.

7.6.6. Configuring OS Support of NMI Generated Kdumps for SUSE LINUX

If you wish to automatically generate a dump file in the event of a kernel panic, refer to the operating system documentation for information on configuring kdumps.

Reboot when you complete all configuration changes.

7.7. Installing and Configuring Red Hat Enterprise Linux

This section describes how to use documentation available from Red Hat to perform a complete, basic installation and configuration of a supported Red Hat Enterprise Linux (RHEL) operating system, and configuring the operating system for the ClearPath Forward fabric.

The installation procedure is complex and familiarity with Linux installations is recommended. For optimal results, follow the directions carefully.

For custom installations and questions, see the Red Hat Enterprise Documentation website at http://www.redhat.com/docs/. This site provides online versions of numerous Red Hat manuals. Select **Red Hat Linux** from the list and click **Go** to access manuals specifically for Red Hat Linux.

If applicable, before you begin the installation, make sure that you have up-to-date backups of all data currently on your server. Some of the options available during the installation process overwrite all the information on the hard disk, including user data.

Caution

Only BIOS booting is supported.

7.7.1. Installing Red Hat Enterprise Linux

To install your supported Red Hat Enterprise Linux (RHEL) operating system, perform the following:

1. Access and review the installation information for your operating system available on the Red Hat Enterprise Documentation website:
   - For RHEL 6: https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Installation_Guide/ch-guimode-x86.html
   - For RHEL 7:

https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Installation_Guide/chap-installing-using-anaconda-x86.html

If desired, save a copy for reference during installation.

2. Ensure that the operating system installation media image (.iso or .img) is available from the Fabric Management Platform. See 7.3 Making Operating System Installation Media Image Available for Installation for more information.
3. From the partition image console, click the **Power** menu, and then click one of the following:
   - **Power On System** if the server is currently powered off.
   - **Reset System** if the server is currently powered on.

   The server boots up, and the Red Hat Enterprise Linux installation screen appears.
4. Step through the installation screens to perform a basic installation and configuration of the operating system. If necessary, refer to the operating system installation documentation for detailed procedures.

   When specifying installation parameters, note the following for adding support for InfiniBand:
   - For RHEL 6, do the following after selecting the type of server installation:
     a. Select **Customize now**, and then click **Next**.
     b. Select **Infiniband Support**, and then select other packages that you want to add.
     c. Click **Next** to begin the installation.
   - For RHEL 7, do the following:
     a. On the main menu, click **Software Selection**.
     b. Depending on your needs, in the **Base Environment** column, select either **Infrastructure Server** or **Server with GUI**.
     c. In the **Adds-Ons for Selected Environment** column, click **Infiniband Support**.
     d. Click **Done**.
5. After completing initial installation, proceed to configure the IP-LAN secure fabric connection for Red Hat Linux.

   For more information, see 7.7.2 Configuring the (InfiniBand) IP-LAN Secure Fabric Connection for Red Hat Linux.

7.7.2. Configuring the (InfiniBand) IP-LAN Secure Fabric Connection for Red Hat Linux

The default IP over InfiniBand (IPoIB) interfaces—typically ib0 and ib1—are used to interface with the IP-LAN secure fabric. If you wish to associate your operating system with a secure fabric other than the IP-LAN secure fabric, create virtual IPoIB interfaces, bond the virtual IPoIB interfaces for resilient operation, and assign a appropriate secure fabric IP address.

For more information on creating and bonding virtual IPoIB interfaces in a Red Hat Linux operating environment, and associating the virtual IPoIB interfaces with a secure fabric, refer to the *ClearPath Forward Administration and Operations Guide*.

Note: *The use of bonded virtual IPoIB interfaces together with bonding of the default IPoIB interfaces in a Red Hat Linux operating environment is restricted in the current release. If the default IPoIB interfaces are bonded, be sure to reconfigure the default IPoIB interfaces to remove the bond before bonding the virtual IPoIB interfaces.*

Depending on whether you will be associating your operating system with the IP-LAN secure fabric or another secure fabric, perform one of the following procedures.

Assigning IP Addresses for the Default InfiniBand Ports and Bonding the Ports

To bond the default IP over InfiniBand (IPoIB) interfaces and configure the IP-LAN secure fabric connection, log in as root, and do the following:

1. Create a file named **ifcfg-ib0** in the /etc/sysconfig/network-scripts directory with the following content:

```
TYPE=InfiniBand
BOOTPROTO=none
MASTER=bond0
SLAVE=yes
NAME=ib0
DEVICE=ib0
ONBOOT=yes
```

2. Create a file named **ifcfg-ib1** in the /etc/sysconfig/network-scripts directory with the following content:

```
TYPE=InfiniBand
BOOTPROTO=none
MASTER=bond0
SLAVE=yes
NAME=ib1
DEVICE=ib1
ONBOOT=yes
```

3. Create a file named **ifcfg-bond0** in the /etc/sysconfig/network-scripts directory with the following content:

```
DEVICE=bond0
NAME=bond0
TYPE=Bond
BONDING MASTER=yes
BONDING_OPTS="mode=active-backup fail_over_mac=0"
BOOTPROTO=none
IPADDR=172.31.xx.1
PREFIX=16
NETWORK=172.31.0.0
BROADCAST=172.31.255.255
```

```
ONBOOT=yes
```

Where *xx* is the platform number for your enterprise partition platform.

Note: *The default subnet address of the IP-LAN secure fabric is 172.31.0.0/16. If the subnet was changed (for example, during initial hardware installation and software configuration), be sure to use the new subnet address value when configuring your network connections. If needed, use Fabric Manager to check the IP-LAN secure fabric IP address for the partition on the partition summary page of the nonpartitionable enterprise partition platform (NEPP).*

4. Execute the following commands to restart all InfiniBand interfaces and apply your changes:

```
systemctl restart network
nmcli con reload
```

Assigning IP Addresses for the Default InfiniBand Ports Without Bonding the Ports

If you wish to associate your operating system with a secure fabric other than the IP-LAN secure fabric, log in as root, and do the following to configure the default IP over InfiniBand (IPoIB) interfaces:

1. Create a file named **ifcfg-ib0** in the /etc/sysconfig/network-scripts directory with the following content:

```
TYPE=InfiniBand
BOOTPROTO=none
IPADDR=172.31.xx.1
NETMASK=255.255.0.0
BROADCAST=172.31.255.255
NAME=ib0
DEVICE=ib0
ONBOOT=yes
```

Where *xx* is the platform number for your enterprise partition platform.

Note: *The default subnet address of the IP-LAN secure fabric is 172.31.0.0/16. If the subnet was changed (for example, during initial hardware installation and software configuration), be sure to use the new subnet address value when configuring your network connections. If needed, use Fabric Manager to check the IP-LAN secure fabric IP address for the partition on the partition summary page of the nonpartitionable enterprise partition platform (NEPP).*

2. Create a file named **ifcfg-ib1** in the /etc/sysconfig/network-scripts directory with the following content:

```
TYPE=InfiniBand
BOOTPROTO=none
IPADDR=172.31.xx.2
NETMASK=255.255.0.0
BROADCAST=172.31.255.255
NAME=ib1
DEVICE=ib1
```

```
ONBOOT=yes
```

Where *xx* is the platform number for your enterprise partition platform.

3. Execute the following commands to restart all InfiniBand interfaces and apply your changes:

```
systemctl restart network
nmcli con reload
```

Proceed to configure the FM LAN connection for Red Hat Linux. For more information, see 7.7.3 Configuring the FM LAN Connection for Red Hat Linux.

7.7.3. Configuring the FM LAN Connection for Red Hat Linux

Log in as root, and do the following:

1. Create a file named **ifcfg-eth-fmp3** in the /etc/sysconfig/networks-scripts directory with the following content:

```
DEVICE=eth-fmp3
TYPE=Ethernet
ONBOOT=yes
BOOTPROTO=none
NM_CONTROLLED=no
SLAVE=yes
MASTER=bond1
USERCTL=no
HOTPLUG=yes
```

2. Create a file named **ifcfg-eth-fmp4** in the /etc/sysconfig/network-scripts directory with the following content:

```
DEVICE=eth-fmp4
TYPE=Ethernet
ONBOOT=yes
BOOTPROTO=none
NM_CONTROLLED=no
SLAVE=yes
MASTER=bond1
USERCTL=no
HOTPLUG=yes
```

3. Create a file named **ifcfg-bond1** in the /etc/sysconfig/network-scripts directory with the following content:

```
DEVICE=bond1
IPADDR=172.29.xx.1
PREFIX=16
ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=none
MTU=
USERCTL=no
BONDING_OPTS="mode=active-backup miimon=250"
```

Where *xx* is the platform number for your enterprise partition platform.

Note: *The default subnet of the FM LAN is 172.29. If the subnet was changed (for example, during initial hardware installation and software configuration), be sure to use the new subnet value when configuring your network connections. If needed, use the Fabric Manager user interface to check the FM LAN IP address for the partition on the partition summary page of the nonpartitionable enterprise partition platform (NEPP).*

4. Update the file named **/etc/modprobe.d/bonding.conf** with the following line:

```
alias bond1 bonding
```

5. If you have a firewall, ensure that your firewall rules allow responses to incoming pings on the FM LAN.

   Note: *The Fabric Manager monitors the health status of a partition image through ping checks; if the ping requests on the FM LAN to the partition image are blocked by a firewall, the Fabric Manager user interface displays a warning state for the partition image's health (but does not generate an event).*

Proceed to update the UDEV persistent rules for Red Hat Linux. For more information, see 7.7.4 Updating the UDEV Persistent Rules for Red Hat LINUX.

7.7.4. Updating the UDEV Persistent Rules for Red Hat LINUX

Log in as root, and add the following four commands—one command per single line— as the first entries in the **/etc/udev/rules.d/70-persistent-net.rules** file:

```
SUBSYSTEM=="net", ACTION=="add", DEVPATH=="/devices/pci0000:00/0
000:00:1c.4/0000:08:00.0/net*", NAME:="eth-fmp3"

SUBSYSTEM=="net", ACTION=="add", DEVPATH=="/devices/pci0000:00/0
000:00:1c.4/0000:08:00.1/net*", NAME:="eth-fmp4"

SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", ATTR{dev_id}=="0
x0", ATTR{type}=="32", NAME:="ib0"

SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", ATTR{dev_id}=="0
x1", ATTR{type}=="32", NAME:="ib1"
```

Proceed to configure OS support of NMI generated kdumps for Red Hat Linux. For more information, see 7.7.5 Configuring OS Support of NMI Generated Kdumps for Red Hat LINUX.

7.7.5. Configuring OS Support of NMI Generated Kdumps for Red Hat LINUX

If you wish to automatically generate a dump file in the event of a kernel panic, refer to the operating system documentation for information on configuring kdumps.

Reboot when you complete all configuration changes.

7.8. Associating a Windows or Linux Operating Environment with a Secure Fabric

For instructions on associating a nonpartitionable enterprise partition platform (NEPP) with a Windows or Linux operating environment with a secure fabric, refer to the *ClearPath Forward Administration and Operations Guide*.

Section 8
Integrating VMware Virtual Machines into the Fabric

If your enterprise environment also utilizes VMware virtualization technologies, you can leverage the high-speed Interconnect and other benefits a ClearPath Forward fabric provides by configuring your environment and distributed applications to span VMware virtual machines as well as partitions in the fabric.

This section describes how to integrate the bare-metal hypervisor VMware vSphere® ESXi 5.5 running on a nonpartitionable enterprise partition platform (NEPP) with the ClearPath Forward fabric, and is intended for users of the fabric who are also familiar with VMware vSphere ESXi installation, including system administrators, network administrators, and Unisys service representatives.

8.1. Prerequisites

Have the following available before performing any installation or configuration tasks:

- A nonpartitionable enterprise partition platform (NEPP) that is currently monitored and managed by the Fabric Manager
- Installation media for VMware vSphere ESXi 5.5
- Installation and configuration documentation for VMware vSphere ESXi 5.5

  Refer to the VMware website or any documentation accompanying the installation media.
- Mellanox InfiniBand driver

  Download the driver for VMware vSphere ESXi 5.5 from the Download tab on the Mellanox website:

  http://www.mellanox.com/page/products_dyn?product_family=36&mtag=vmware_drivers

8.2. Installing VMware vSphere ESXi on a Nonpartitionable Enterprise Partition Platform

You can install the bare-metal hypervisor VMware vSphere ESXi on a nonpartitionable enterprise partition platform (NEPP) in the ClearPath Forward fabric. To install VMware vSphere ESXi on an NEPP, obtain the required installation media, and use the associated VMware documentation to install and configure the hypervisor.

http://pubs.vmware.com/vsphere-55/topic/com.vmware.vsphere.install.doc/GUID-7C9A1E23-7FCD-4295-9CB1-C932F2423C63.html

8.3. Enabling ESXi Shell Access

You use the ESXi Shell to install drivers for the VMware vSphere ESXi host in later procedures. If access to the ESXi Shell is not enabled, refer to VMware documentation for detailed configuration steps to enable it.

http://pubs.vmware.com/vsphere-55/topic/com.vmware.vcli.getstart.doc/cli_jumpstart.3.5.html#1005045

8.4. Removing Mellanox Ethernet and Other In-box Drivers

Do the following to remove unneeded Mellanox drivers for the VMware vSphere ESXi host:

1. From the ESXi system's direct console (DCUI), access the main screen, and then press **Alt+F1** to open a virtual console window.
2. Log in as root.
3. Enter the following ESXCLI commands to remove Mellanox Ethernet drivers:

```
#> esxcli software vib remove -n net-mlx4-ib
#> esxcli software vib remove -n scsi-ib-iser
#> esxcli software vib remove -n net-rdma-cm
#> esxcli software vib remove -n net-ib-addr
#> esxcli software vib remove -n net-ib-cm
#> esxcli software vib remove -n net-ib-umad
#> esxcli software vib remove -n net-ib-sa
#> esxcli software vib remove -n net-ib-mad
#> esxcli software vib remove -n net-ib-core
```

4. Enter the following ESXCLI commands to remove other Mellanox in-box drivers:

```
#> esxcli software vib remove -n net-mlx4-en
#> esxcli software vib remove -n net-mlx4-core
```

5. Reboot the ESXi host.

8.5. Installing Mellanox InfiniBand Driver

Do the following to install the Mellanox InfiniBand driver for the VMware vSphere ESXi host:

1. Ensure the Mellanox InfiniBand driver for VMware vSphere ESXi 5.5 is available. If necessary, download the driver from the Download tab on the Mellanox website:

   http://www.mellanox.com/page/products_dyn?product_family=36&mtag=vmware_drivers

2. Using a secure file transfer client (for example, FileZilla), copy the ZIP file containing the driver to a known location on the ESXi host; for example, the **/var/log/vmware** directory.
3. From the ESXi system's direct console (DCUI), access the main screen, and then press **Alt+F1** to open a virtual console window.
4. Log in as root.
5. Enter the following ESXCLI command to install the Mellanox InfiniBand driver:

   ```
   #> esxcli software vib install -d  <path>/<bundle_zip_file>
   ```

   Where

   - *<path>* is the location you previously copied the ZIP file containing the driver to.
   - *<bundle_zip_file>* is the name of the ZIP file containing the driver.

   For example

```
#> esxcli software vib install -d  /var/log/vmware /MLNX-OFED-ESX-1.8.2.4-
10EM- 500.0.0.472560.zip
```

6. Reboot the ESXi host.

8.6. Verifying Installation of Mellanox InfiniBand Driver

Do the following to verify that the Mellanox InfiniBand driver for the VMware vSphere ESXi host was installed:

1. From the ESXi system's direct console (DCUI), access the main screen, and then press **Alt+F1** to open a virtual console window.
2. Log in as root.
3. Enter the following ESXCLI command:

   ```
   #> esxcli software vib list | grep Mellanox
   ```

   If the driver was successfully installed, results similar to the following are displayed:

```
net-ib-cm1.8.2.4-1OEM.500.0.0.472560 Mellanox PartnerSupported 2014-03-06
net-ib-core1.8.2.4-1OEM.500.0.0.472560 Mellanox PartnerSupported 2014-03-06
net-ib-ipoib1.8.2.4-1OEM.500.0.0.472560 Mellanox PartnerSupported 2014-03-06
net-ib-mad1.8.2.4-1OEM.500.0.0.472560 Mellanox PartnerSupported 2014-03-06
net-ib-sa1.8.2.4-1OEM.500.0.0.472560 Mellanox PartnerSupported 2014-03-06
net-ib-umad1.8.2.4-1OEM.500.0.0.472560 Mellanox PartnerSupported 2014-03-06
net-mlx4-core1.8.2.4-1OEM.500.0.0.472560 Mellanox PartnerSupported 2014-03-06
net-mlx4-ib1.8.2.4-1OEM.500.0.0.472560 Mellanox PartnerSupported 2014-03-06
scsi-ib-srp1.8.2.4-1OEM.500.0.0.472560 Mellanox PartnerSupported 2014-03-06
```

8.7. Creating a Virtual Machine Virtual Switch for Secure Fabric Connections

Do the following to create a virtual switch (vSwitch), and add network segments to the virtual switch for secure fabrics:

1. Referring to VMware documentation, create a virtual switch for VMware vSphere ESXi virtual machines (guests), and associate the switch with the Mellanox InfiniBand ports.

   http://pubs.vmware.com/vsphere-55/topic/com.vmware.vcli.examples.doc/cli_manage_networks.11.5.html

2. For each secure fabric you want your VMware vSphere ESXi virtual machines (guests) to associate with, add a network segment to the virtual switch associated with the Mellanox InfiniBand uplink ports. Be sure to name each network segment with an identifiable name (Network Label), and assign a VLAN ID using the subnet tag of the secure fabric.

8.8. Configuring VMware Virtual Machine Connection to Secure Fabrics

To configure networking for VMware vSphere ESXi virtual machines (guests) so that they can communicate over the ClearPath Forward fabric, do the following for each virtual machine that will be accessing the fabric:

1. When creating or configuring the virtual machine, be sure to add the network adapter type **VMXNET 3**, and then select the VLAN-tagged network segment of the virtual switch with the VLAN ID (secure fabric subnet tag) of the secure fabric you want the virtual machine to associate with.

   (For more information on creating a virtual switch and network segments, refer to 8.7 Creating a Virtual Machine Virtual Switch for Secure Fabric Connections.)

2. After booting the virtual machine, configure network settings for the Ethernet adapters in the operating system on the virtual machine. Be sure to statically assign a secure fabric IP address to each secure fabric virtual interface configured in the virtual machine. For example, for the IP-LAN secure fabric, assign an IP address of 172.31.*x.y* (where *x* is in the range 64 through 127, and *y* is in the range 1 through 249).

8.9. Configuring the FM LAN Connection for VMware vSphere ESXi Host

For the Fabric Manager user interface to display the health status of the VMware vSphere ESXi host on the nonpartitionable enterprise partition platform (NEPP), configure a connection between the Fabric Manager and the VMware vSphere host on the ClearPath Forward Management LAN (FM LAN).

1. Identify the network name of the virtual network adapters associated with network adapters connected to the FM LAN.

   LOM ports 3 and 4 on the NEPP are cabled respectively to the two Ethernet LAN switches for FM LAN traffic. Use the VMware vSphere Client or vCenter to locate and identify the virtual NICs associated with LOM ports 3 and 4.

   For more information, see 8.9.1 Identifying the Virtual Network Adapters Associated with FM LAN.

2. Using the VMware vSphere Client or vCenter, create a VMkernel virtual switch with the virtual network adapters associated with the FM LAN as the uplinks for the switch, and assign the FM LAN IP address of the NEPP to the VMkernel port.

   For more information, see 8.9.2 Creating a VMkernel Virtual Switch for FM LAN Connection.

8.9.1. Identifying the Virtual Network Adapters Associated with FM LAN

LOM ports 3 and 4 on the nonpartitionable enterprise partition platform (NEPP) are cabled respectively to the two Ethernet LAN switches for ClearPath Forward Management LAN (FM LAN) traffic. Use the VMware vSphere Client or vCenter to locate and identify the names of the virtual network adapters associated with LOM ports 3 and 4.

1. Using the VMware vSphere Client or vCenter, locate and select the desired NEPP, and then click the **Configuration** tab.
2. In the left-hand **Hardware** pane, click **Network Adapters**.

   A list of network adapters appears.
3. Locate the two 1 GbE network adapters LOM port 3 and LOM port 4 on the NEPP, and then note down the names displayed in the Device column. Typically, these ports are named vmnic2 and vmnic3.

   Notes:

   - *Typically, the two 10 GbE network adapters LOM port 1 and LOM port 2 on the NEPP are named vmnic0 and vmnic1.*
   - *Depending on the sequence in which a port is discovered by the VMware vSphere host, the number* x *in the device name vmnic*x *may be different.*
   - *To verify that you located the correct ports, compare the MAC addresses listed in vSphere Client with the MAC addresses listed in the platform's Platform Management Console.*

8.9.2. Creating a VMkernel Virtual Switch for FM LAN Connection

Create a VMkernel virtual switch with the virtual network adapters associated with the ClearPath Forward Management LAN (FM LAN) as the uplinks for the switch.

1. Using the VMware vSphere Client or vCenter, if necessary, locate and select the desired nonpartitionable enterprise partition platform (NEPP), and then click the **Configuration** tab.
2. In the left-hand **Hardware** pane, click **Networking**, and then click **Add Networking** in the right-hand pane.

   The Add Network Wizard appears.
3. On the Connection Type screen, in the Connection Types section, select **VMkernel**, and then click **Next**.
4. On the VMkernel – Network Access screen, select the virtual network adapters you previously identified (see 8.9.1 Identifying the Virtual Network Adapters Associated with FM LAN), and then click **Next**.
5. On the VMkernel – Connection Settings screen, in the **Network Label** field, enter a name for easy identification of this LAN subnet (for example, FM-LAN), ensure the **VLAN ID** field is set as **None (0)**, and then click **Next**.
6. On the VMkernel – IP Connection Settings screen, select the option **Use the following IP settings**, type in the FM LAN IP address and subnet mask for the NEPP, and then click **Next**.

   If needed, use the Fabric Manager user interface to check the FM LAN IP address and subnet mask for the platform on the summary page of the NEPP, for example, 172.31.*x*.1/255.255.0.0 (where *x* is the platform number).
7. Review the summary, and then click **Finish** to create the virtual switch.

   The VMware vSphere Client or vCenter displays the new virtual switch on the Networking screen of the Configuration tab.
8. Verify that the uplink ports of the virtual switch for FM LAN connection are set up to operate in the active-backup failover mode:

   a. Locate the virtual switch, and the click **Properties**.

      A virtual switch properties dialog box appears.

   b. On the **Ports** tab, select the virtual switch for FM LAN connection (for example, FM-LAN), and then review its properties displayed in the right-hand sections. If needed, scroll down to the Effective Policies section to review the Failover and Load Balancing settings.

   c. If necessary, adjust the failover settings: Click **Edit** to access the virtual switch properties dialog box, select the **NIC Teaming** tab, set **Network Failover Detection** to be **Link status only**, set **Failback** to be **Yes**, and verify the order of the uplink network adapter ports for active and standby status. Click **OK**, and then click **Close** to apply the properties.

8.10. (Optional) Configuring the FM LAN Connection for VMware Virtual Machines

Optionally, you can configure a network connection to the ClearPath Forward Management LAN (FM LAN) for VMware virtual machines (guests) by adding a standard port group to the FM LAN connection virtual switch. (For more information on creating the

FM LAN connection virtual switch, see 8.9.2 Creating a VMkernel Virtual Switch for FM LAN Connection.)

8.10.1. Adding a Standard Port Group to FM LAN Connection Virtual Switch

To add a standard port group to the VMkernel virtual switch for the ClearPath Forward Management LAN (FM LAN) connection, do the following:

1. Using the VMware vSphere Client or vCenter, locate and select the desired nonpartitionable enterprise partition platform (NEPP), and then click the **Configuration** tab.
2. In the left-hand **Hardware** pane, click **Networking**, and then click **Add Networking** in the right-hand pane.

   The Add Network Wizard appears.
3. On the Connection Type screen, in the Connection Types section, select **Virtual Machine**, and then click **Next**.
4. On the Virtual Machines – Network Access screen, locate and select the virtual switch associated with the virtual network adapters associated with the FM LAN (for example, FM-LAN with vmnic2 and vmnic3), and then click **Next**.
5. On the Virtual Machines – Connection Settings screen, in the **Network Label** field, enter a name for easy identification of this LAN subnet (for example, vmFM-LAN), ensure the **VLAN ID** field is set as **None (0)**, and then click **Next**.
6. Review the summary, and then click **Finish** to add the standard port group network interface to the virtual switch.

8.10.2. Configuring VMware Virtual Machine Connection to the FM LAN

To configure networking for VMware vSphere ESXi virtual machines (guests) so that they can connect to the ClearPath Forward Management LAN (FM LAN), do the following for each virtual machine that will be accessing the FM LAN:

1. During creating or configuration of the virtual machine, when specifying network adapters, be sure associate the FM LAN connection virtual switch with one of the network adapters. (For more information on creating the FM LAN connection virtual switch, see 8.9.2 Creating a VMkernel Virtual Switch for FM LAN Connection.)
2. After booting the virtual machine, configure network settings for the Ethernet adapters in the operating system on the virtual machine. Be sure to assign the FM LAN IP address to the network adapter associated with the FM LAN.

Section 9
Configuring Partition Images to Boot from External Storage Device

This section provides an overview and describes how to configure your partition images to boot from an external storage device (for example, a storage area network).

9.1. Booting from Internal or External Storage

Partition blueprints and operating system gold images reside on an enterprise partition platform's (EPP's) internal disk storage. Using a blueprint, you commission a partition image, which provides the running partition with hardware resources and an operating system.

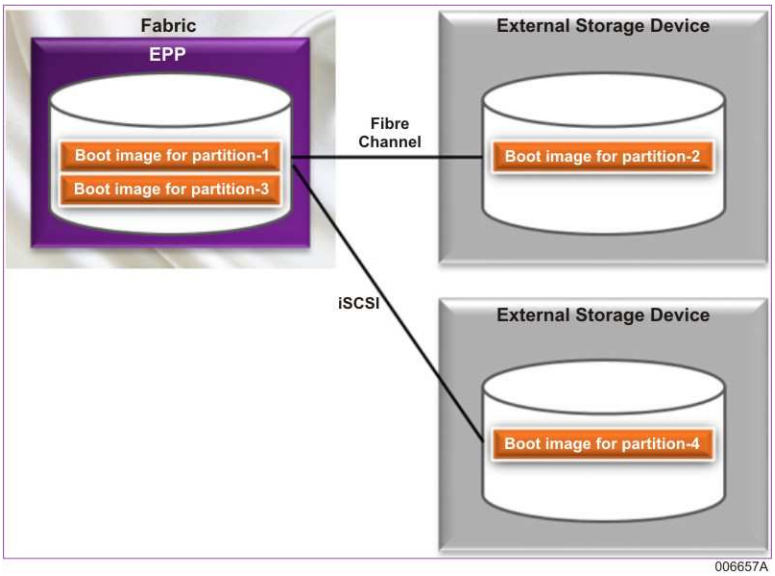
By default, a partition operating system boots from the EPP's internal disk storage. However, you may configure your partition image to boot from an external storage device (for example, a storage area network) rather than from the EPP's internal disk storage. Depending on your enterprise network architecture, your external storage device may be connected to the fabric with dedicated fibre channel cabling or the iSCSI storage networking protocol.

As part of this process

- The operating system image is copied onto the external storage device.
- The partition is configured to boot from that external storage device rather than from the EPP's internal disk storage.

One advantage to placing the boot volume on external storage is that it is easier to recover the partition in case of platform failure.

Booting from external storage is on a partition-by-partition basis. On a given EPP, some partitions may boot from internal storage, while others boot from external storage.



Note that it is the customer's responsibility to ensure that the platform from which the external storage logical unit number (LUN) is accessed has a valid license for running the operating system.

9.2. Booting from External Storage Device over Fibre Channel

Note: *Booting a Windows Server 2008 R2 SP1 partition from an external storage device is not supported.*

If you wish to boot your partition from an external storage device over fibre channel, you need to obtain the external storage WWPN (target name) and LUN number (target number) from your storage administrator so that you can fill in the required target information after selecting the external storage option during commissioning. For more information on commissioning, see 5.3 Commissioning a Partition Image.

If the partition you wish to boot from an external storage device over fibre channel is a Windows partition, be sure there is only a single storage processor path to the external storage device before commissioning the partition. If necessary, request your storage administrator disconnect paths to LUNs that will not be designated as the boot LUN for the partition. After you complete installation of the Windows operating system on the partition, your storage administrator can reattach any desired additional LUNs.

To configure the external storage device, your storage administrator may need the WWPN values of the HBA ports of your partitionable enterprise partition platform (PEPP) that will be used as the boot paths for the partition you wish to boot from the external storage device. For more information, see 9.2.1 Identifying World Wide Port Name (WWPN) of HBA Ports.

During commissioning, when you choose to boot a partition image from external storage device over fibre channel, you have the following options for entering parameters for the boot LUN:

- **Configure using Partition Image Console**

  This option allows you to use the boot LUN selection utility available through the partition image console to configure detailed parameters for the target boot LUN. For more information on accessing a partition desktop, see 12.2 Accessing the Partition Image Console (Partition Desktop); for more information on using the boot selection utility, see 9.2.2 Configuring Detailed Parameters for Target Boot LUN.

- **Configure Target Boot LUN Now**

  This option allows you to use the Fabric Manager to configure basic parameters for the target boot LUN.

  If user interaction is required during booting to the external storage device, the Fabric Manager user interface displays an alert. Access the partition desktop to monitor the status and view any messages. For more information on accessing a partition desktop, see 12.2 Accessing the Partition Image Console (Partition Desktop); for more information on situations that require user interaction, see 9.2.3 Resolving Situations Requiring User Interaction.

To configure a secondary boot path for an existing partition on an external storage device, see 9.2.4 Configuring Secondary Boot Path for an Existing Partition on External Storage.

To configure a backup partition, see 9.2.5 Configuring a Backup Partition.

Notes:

- *For ease of initial installation and configuration of the operating system on a new partition, Unisys recommends initially commissioning a partition with a single boot path and a single storage processor path to the external storage device.*
- *On the rare occasion, the Fabric Manager may incorrectly report that the commissioning process failed—for example, when a Linux partition is re-commissioned in a recovery situation to boot an existing boot LUN on the external storage. Verify whether the commissioning process completed successfully by logging onto the partition desktop to review and observe any information displayed on the desktop.*

9.2.1. Identifying World Wide Port Name (WWPN) of HBA Ports

If you plan to commission a partition image to a boot volume on an external storage device, you need to identify the HBA ports of your Partitionable Enterprise Partition Platform (PEPP) that will be allocated to the partition, as well as the initiator World Wide Port Name (WWPN) of the HBA ports, and provide the information to the storage administrator. The storage administrator needs this information to configure visibility from the HBA ports of the PEPP to the LUN on the external storage device where you will be creating the partition boot volume. You can view the WWPN of all the HBA ports of the platform in the **Config Info** tab.

To view the WWPN information of a particular HBA port

1. On the Fabric Manager user interface, point to **System Administration**, and then click **CPF System**.

   The **Details: CPF-System** screen appears on the right pane.

2. Click **Platforms and Partitions**.

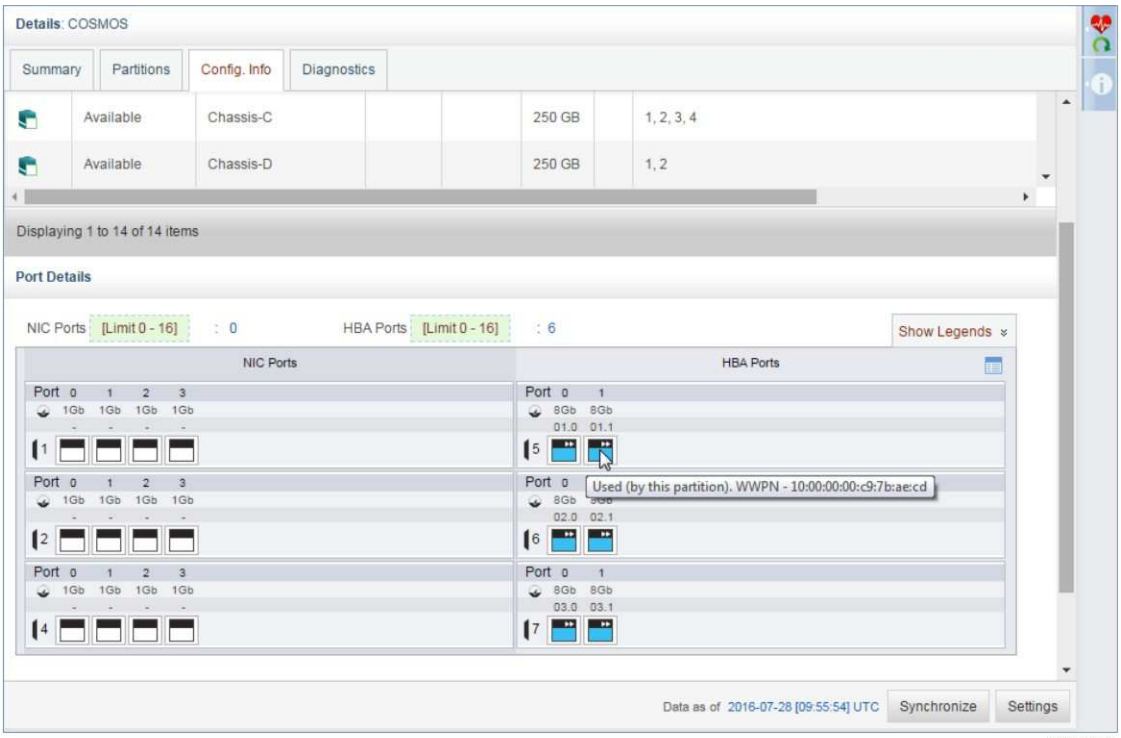
   The **Details: Platforms and Partitions** screen appears on the right pane.

3. On the **Platforms** tab, double-click the platform of which you want to view the configuration information.

4. Click **Config. Info** tab.

5. Under **Port Details**, hover the cursor on the graphical representation of the HBA port. The WWPN of the port is displayed in a pop-up box.

The following image shows an example of the pop-up box displaying the WWPN of a particular HBA port.



007469B

You can also view and optionally export the list of all the HBA ports and their WWPNs. To view the list of HBAs and their WWPNs

1. On the Fabric Manager user interface, point to **System Administration**, and then click **CPF System**.

   The **Details: CPF-System** screen appears on the right pane.

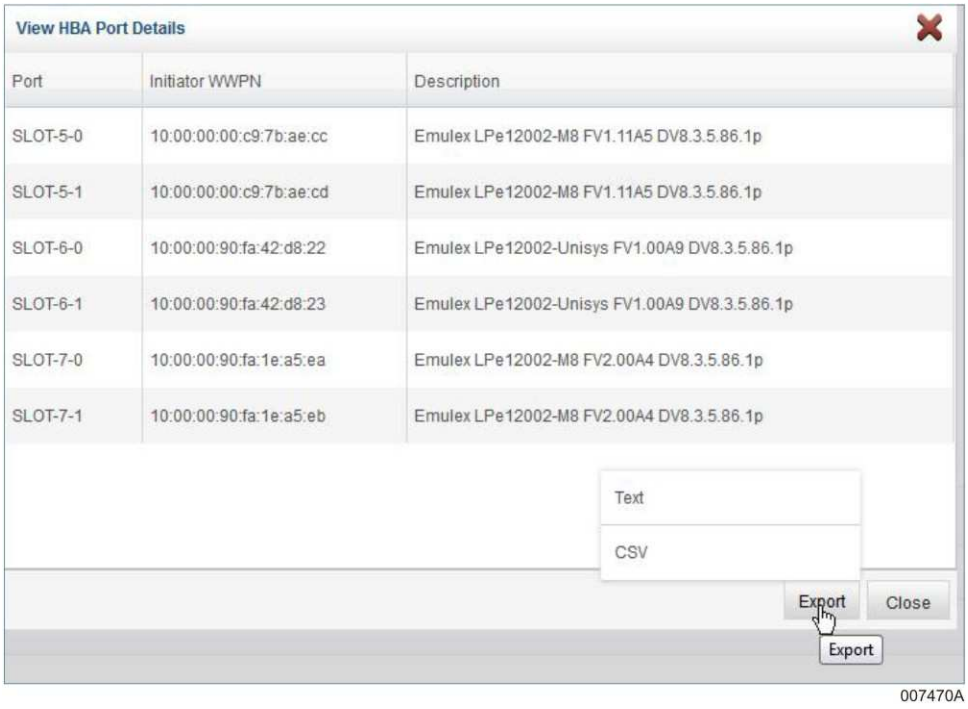
2. Click **Platforms and Partitions**.

   The **Details: Platforms and Partitions** screen appears on the right pane.

3. On the **Platforms** tab, double-click the platform of which you want to view the configuration information.
4. Click **Config. Info** tab.
5. Under **Port Details,** on the upper right corner of the **HBA ports** column, click . The **View HBA Port Details** dialog box appears. The information displayed includes the slot number, the port number and the corresponding WWPN (otherwise known as WWN of the port) for all the HBA ports on the platform.

   To export the complete list of HBA Ports and their WWPNs, click **Export**. The list is exported as a file. Store the file on your local machine in any preferred folder. When providing the information to your storage administrator, be sure to identify the specific HBA ports that will be the boot paths for your partition.

The following image is an example of the View HBA Port Details dialog box.



9.2.2. Configuring Detailed Parameters for Target Boot LUN

When you choose to boot a partition image from external storage device over fibre channel and the **Configure using Partition Image Console** option, access the partition desktop (see 12.2 Accessing the Partition Image Console (Partition Desktop)) and then use the boot LUN selection utility available through the partition image console to configure detailed parameters for the target boot LUN.

- Using the Boot LUN Selection Utility for Windows
- Using the External Boot Device Selection Utility for Linux

Using the Boot LUN Selection Utility for Windows

Note: *Be sure there is only one path to the boot LUN on the external storage device. The Windows Preinstallation Environment (WinPE) that installation scripts run under during commissioning does not support multiple paths to the boot LUN.*

Access the partition desktop (see 12.2 Accessing the Partition Image Console (Partition Desktop)) and do the following to configure detailed parameters for the target boot LUN:

1. From the list displayed under the **Initiatior WWPN** section of the Boot LUN Selection utility, select the WWPN of the initiator port you want for your boot path.

   The bottom area of the utility displays status as well as additional instructions for completing the configuration step.

2. From the list displayed under the **Target WWPN** section, select the WWPN of the target port.

   All the LUNS connected to the selected target WWPN are displayed under the Target LUN section, and details for the selected LUN are displayed.

   Notes:

   - *If the selected target LUN is smaller than 32GB, a warning message appears. Click **OK** to keep your selection and enable the Continue button in the utility, or click **Cancel** and then select a different LUN.*
   - *If partitions exist on the selected target LUN, the LUN EMPTY entry displays the status "No, Contains Data".*

3. Review the bottom area of the utility for details of your boot path. Make any desired adjustments.
4. Click **Continue**, and then click **OK** to proceed with commissioning.

Using the External Boot Device Selection Utility for Linux

Access the partition desktop (see 12.2 Accessing the Partition Image Console (Partition Desktop)) and do the following to configure detailed parameters for the target boot LUN:

Note: *For some options, the utility displays additional information at the bottom of the console window.*

1. On the HBA Port Selection screen, press the up or down arrow keys to highlight and select the HBA port you want to boot from.
2. Press the **Tab** key to select **Next – Select the target WWPN**, and then press **Enter**.
3. On the Remote Port Name Selection screen, press the up or down arrow keys to highlight and select the target WWPN for accessing the boot LUN on the external storage device.
4. Press the **Tab** key to select **Next – Select the boot lun**, and then press **Enter**.

5. On the Boot LUN Selection screen, press the up or down arrow keys to highlight and select the desired LUN.
6. Press the **Tab** key to select **Next – Continue commissioning**, and then press **Enter**.

Note: *If the specified LUN contains partitions, a message is displayed. Refer to LUN is not Empty for more information on resolving the situation.*

9.2.3. Resolving Situations Requiring User Interaction

When you choose to boot a partition image from external storage device over fibre channel and the **Configure Target Boot LUN Now** option to use the Fabric Manager to configure basic parameters for the target boot LUN, the Fabric Manager user interface may alert you that user interaction is required during the commissioning process. You should access the partition desktop (see 12.2 Accessing the Partition Image Console (Partition Desktop)) to monitor status and view any messages.

Some situations that require user interaction include:

- Unable to Connect to the External Storage Device Using the Specified WWPN
- No Matching LUN Found on External Storage Device
- LUN is not Empty

Unable to Connect to the External Storage Device Using the Specified WWPN

An error message is displayed on the partition desktop, reporting that the installation script was not able to access the target LUN through the specified path.

Note: *For some options on a Linux partition, the installation script displays additional information at the bottom of the console window.*

Possible Cause

The external storage device is not connected to the HBA port selected during commissioning.

Solution

1. Check the cabling connections, and adjust the cabling if appropriate.

   If you adjusted the cabling, on the partition desktop, select to retry the connection to the external storage device; the commissioning and installation scripts should now proceed without errors. If the scripts encounter more errors, note down the available HBA device values, choose to exit the commissioning and installation scripts, and then proceed to the next step.

2. Verify with the storage administrator the HBA ports you should be selecting for your partition.
3. Use Fabric Manager to decommission the non-functional partition, and then commission a new partition with the appropriate HBA port value.

Possible Cause

The WWPN number was not entered correctly during commissioning.

Solution

1. Messages on the partition desktop display the target WWPN value you entered, as well as the WWPN value of the detected external storage device. Compare the information to identify where the error is.
2. After noting down the correct value, choose to exit the commissioning and installation scripts.
3. Use the Fabric Manager user interface to decommission the non-functional partition, and then commission a new partition with the appropriate WWPN value.

No Matching LUN Found on External Storage Device

An error message is displayed on the partition desktop, reporting that the installation script was not able to locate a LUN using the specified LUN number.

Note: *For some options on a Linux partition, the installation script displays additional information at the bottom of the console window.*

Possible Cause

The external storage device is not connected to the HBA port selected during commissioning.

Solution

Check the cabling connections, and adjust the cabling if appropriate.

If you adjusted the cabling, on the partition desktop, select to retry the connection to the external storage device; the commissioning and installation scripts should now proceed without errors. If the scripts encounter more errors, it is likely the LUN number was not entered correctly during commissioning.

Possible Cause

The LUN number was not entered correctly during commissioning.

Solution

1. Messages on the partition desktop display the target LUN value you had entered, as well as the LUN values detected on the external storage device. If applicable, compare the information to identify where the error is.
2. After noting down the available values, choose to exit the commissioning and installation scripts.
3. Use the Fabric Manager user interface to decommission the non-functional partition, and then commission a new partition with the appropriate LUN value.

LUN is not Empty

If the specified LUN contains partitions, an error message is displayed on the partition desktop, reporting that the LUN is not empty. The following options are also displayed:

- Install the new image to the LUN

  If you want to erase the contents on the LUN and install the new image on LUN, select this option, and then select OK.

- Only configure the HBA port

  If you only want to configure the partition to have boot access to the LUN and not overwrite the existing content on the LUN, select this option, and then select OK.

  Typically, this option is used when creating a backup partition for high availability purposes. To prevent corruption of data on the LUN on the external storage device, the initial state of the partition is set to Stopped.

- (Linux only) Exit the script

  If you want to exit the script so that you can run other applications for troubleshooting purposes, select this option, and then select OK.

- Abort commissioning the partition

  If you want to stop commissioning a partition on the LUN, select this option, and then select OK. Be sure to use Fabric Manager to decommission the non-functional partition.

Note: *For some options on a Linux partition, the installation script displays additional information at the bottom of the console window.*

9.2.4. Configuring Secondary Boot Path for an Existing Partition on External Storage

If you wish to configure a secondary boot path for a partition, use the standard operating system utilities available on the partition after commissioning your partition.

To configure a secondary boot path for your partition on the external storage device, do the following:

1. Use the Fabric Manager user interface to commission a partition on the external storage device, specifying only the primary boot path.
2. After the operating system is loaded on the LUN in the external storage device, access the partition desktop and configure settings for multiple paths (for example, multi-path IO capability) in the operating system and any applicable software.
3. On the external storage device, configure an additional path to the boot LUN through another HBA port assigned to the partition.

   Note: *For Windows partitions, be sure to perform this step after the partition is commissioned. The Windows Preinstallation Environment (WinPE) that installation scripts run under during commissioning does not support multiple paths to the boot LUN.*
4. Access the partition, and use the Emulex OneCommand® Manager (OC Manager) running in the partition operating system to configure the secondary HBA port as a valid boot path to the boot volume.

The secondary boot path is now available on subsequent boots of the partition if the primary boot path is not available.

9.2.5. Configuring a Backup Partition

If you have an existing partition on a platform that is booting to the external storage device and wish to configure a partition on a different platform to access the same boot volume—for example, a backup partition for recovery purposes in case of the first platform fails—do the following:

1. Using the Fabric Manager user interface, commission a partition on the other platform, specifying the boot path to the same WWPN and LUN number (targets) as the existing partition. To prevent corruption of data on the LUN on the external storage device, be sure to specify an initial state of **Stopped** for the partition image.

   Since the LUN contains information from the existing partition, Fabric Manager alerts you that user interaction is required.
2. Access the partition desktop, and choose to only configure the HBA port.

   The installation script configures the partition to have boot access to the LUN, but does not overwrite the existing LUN contents.
3. If desired, verify that the backup partition is configured to access the same boot volume: Using the Fabric Manager user interface, stop the existing partition, start the backup partition, and then access the partition desktop to verify that it is the correct system.

9.3. Booting from External Storage Device over iSCSI

After commissioning a SUSE LINUX operating system partition image on the internal storage of a partitionable enterprise partition platform (PEPP), you can configure the partition image to boot from an external storage device over iSCSI.

In general, the process is as follows:

1. Prepare the external storage device as an iSCSI target.
2. Prepare the partition on the PEPP as an iSCSI initiator.
3. If desired, prepare a second partition as a backup partition.

   Unisys recommends using a partition on another platform.
4. Verify that the Linux OS disk drive partition /root is on the iSCSI target.

9.3.1. Preparing External Storage Device as iSCSI Target

To prepare an external storage device as an iSCSI target, request your storage administrator to configure the external storage device as an iSCSI target, including creating a single LUN (virtual disks) for each partition. For more information, refer to the vendor documentation.

Note: *The scripts provided by Unisys expect the iSCSI target to have only a single LUN; the scripts will partition the LUN into the required Linux OS disk drive partitions.*

Be sure to obtain the following information from your storage administrator:

- Name of the iSCSI target.
- If configured, user ID and password for the target.
- IP address of the iSCSI target.
- If configured on the external storage device, the name of the iSCSI initiator.

  The iSCSI initiator is the partition on the partitionable enterprise partition platform (PEPP). If your storage administrator configured the external storage device with a name, be sure to use the same name in the Partition Image Name field when commissioning your partition—the initiator name must match the name of the external storage device.

9.3.2. Preparing Partition on PEPP as iSCSI Initiator

Do the following to commission a SUSE LINUX partition image on a partitionable enterprise partition platform (PEPP), and then move the Linux OS disk drive partitions /boot, /var, /root, /swap, and /tmp to the iSCSI target. The Linux OS disk drive partition /efi must remain on the internal storage of the PEPP.

Note: *A backup copy of the /efi disk drive partition is kept on the SAN to facilitate copying of the PEPP partition.*

1. Be sure the iSCSI target is available.
2. Use the Fabric Manager user interface to commission a SUSE LINUX partition image on your PEPP. For more information, see 5.2 Overview of Commissioning a Partition and 5.3 Commissioning a Partition Image.
3. Change the run level of the partition to single user mode. For example,

   ```
   telinit S
   ```

4. Enter the password for the root user ID at the partition desktop prompt.
5. Locate and run the interactive iSCSI installation script. For example,

   ```
   /usr/local/bin/iscsiadd.sh
   ```

   The script launches and loads networking drivers for connecting to the iSCSI target.
6. When queried for the initiator name, verify that the name matches an initiator name specified by the storage administrator for the iSCSI target, and then press **Enter**.
7. When queried for an IP address for the iSCSI target, enter the information you obtained from your storage administrator.

   The script verifies the IP address as well as the state of iSCSI.

   Note: *If the IP address you entered is not correct, you are prompted to enter a new IP address.*
8. When queried for user ID and password for accessing the target, if configured, enter the information you obtained from your storage administrator. Otherwise, press **Enter**.

   Note: *If the target is not available, you may see messages similar to the following, and you are prompted to enter a new IP address.*

```
PING 172.31.180.1 (172.31.180.1) 56(84) bytes of data.
From 172.31.3.3: icmp_seq=1 Destination Host Unreachable
--- 172.31.180.1 ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms
```

9. If the external storage device does not have a target with the same name as your partition, you are prompted to select a target. Use the up and down arrow keys to select your desired target, press **Tab** to select **OK**, and then press **Enter** to confirm your choice.

   Note: *Examples in following steps use* iqn.usrv-flx3:0 *as the target name.*

   The script accesses the target and configures the Linux OS disk drive partitions, and status messages similar to the following are displayed:

```
Logging in to [iface: default, target: iqn.usrv-flx3:0, portal: 172.31.180.1,3260] (multiple)
Login to [iface: default, target: iqn.usrv-flx3:0, portal: 172.31.180.1,3260] successful.
TARGET is "iqn.usrv-flx3:0"
Found LUN 0
…
Kernel image:   /boot/vmlinuz-3.0.76-0.11-default
Initrd image:   /boot/initrd-3.0.76-0.11-default
…
Kernel Modules: hwmon thermal_sys thermal processor fan scsi_mod scsi_tgt scsi_transport_fc
lpfc megaraid_sas libata libahci ahci uischanmod spardump sparstop visorchannel visordiag
visorchipset uislibmod virtpcimod virthbamod virtnicmod visorbus visorclientbus
```

```
visorserialclient visorconinclient visorvideoclient visornoop ipv6_lib compat ib_addr ib_core
ib_mad ib_sa ib_cm ib_ipoib mlx5_core mlx5_ib ib_uverbs ib_ucm ib_umad mlx4_core
mlx4_en mlx4_ib scsi_dh scsi_dh_hp_sw scsi_dh_alua scsi_dh_rdac scsi_dh_emc mbcache jbd ext3
scsi_transport_iscsi libiscsi libiscsi_tcp iscsi_tcp af_packet bonding crc32c iscsi_boot_sysfs
iscsi_ibft uio cnic bnx2i nls_utf8 crc-t10dif sd_mod
Features:       acpi block network iscsi resume.userspace resume.kernel kdump
61644 blocks
mkinitrd was successful.
```

The script then copies the file systems from the internal storage to the target. When the root file system is copying, the script may pause and display status messages similar to the following:

```
Features:       acpi block network iscsi resume.userspace resume.kernel kdump
61634 blocks
mkinitrd was successful.
/var:                16933 19278
```

10. Verify that all patches were applied successfully and status messages similar to the following are displayed:

```
Successful application of patch /usr/local/iscsiboot/src/aaa_base-11-6.90.1.patch
Successful application of patch /usr/local/iscsiboot/src/open-iscsi-2.0.873-0.21.1.patch
```

11. If desired, prepare a second partition as a backup partition. See 9.3.3 Preparing Backup Partition. Otherwise, proceed to 9.3.4 Verifying Location of /root to reboot your partition and verify that the Linux OS disk drive partition /root is on the iSCSI target.

9.3.3. Preparing Backup Partition

Ensure the first partition is either not running or not rebooted after it was prepared as an iSCSI initiator, and then do the following to prepare another partition as an iSCSI initiator and configure it as the backup partition to the first partition.

Note: *Unisys recommends using a partition on another platform as a backup partition.*

1. Be sure the iSCSI target is available.
2. Use the Fabric Manager user interface to commission a SUSE LINUX partition image on your PEPP. For more information, see 5.2 Overview of Commissioning a Partition and 5.3 Commissioning a Partition Image.
3. Change the run level of the partition to single user mode. For example,

   ```
   telinit S
   ```

4. Enter the password for the root user ID at the partition desktop prompt.
5. Locate and run the interactive iSCSI installation script. For example,

   ```
   /usr/local/bin/iscsiadd.sh
   ```

   The script launches and loads networking drivers for connecting to the iSCSI target.
6. When queried for an initiator name, be sure to use the name of the iSCSI target that you used when preparing your first partition, and then press **Enter**.
7. When queried for an IP address for the iSCSI target, be sure to enter the IP address of the iSCSI target that you used when preparing your first partition.

8. When queried for user ID and password for accessing the target, if configured, enter the information you obtained from your storage administrator. Otherwise, press **Enter**.
9. If the external storage device does not have a target with the same name as your partition, you are prompted to select a target. Use the up and down arrow keys to select the iSCSI target that you used when preparing your first partition, press **Tab** to select **OK**, and then press **Enter** to confirm your choice.
10. When queried whether you wish to erase existing disks on the iSCSI target, press **N** to answer No.
11. When the script completes final configuration tasks, reboot the backup partition.

9.3.4. Verifying Location of /root

To verify that /root is located on the iSCSI target, do the following:

1. Reboot your partition and log in.
2. Display the mount list, filtered by grep. For example,

   ```
   grep ' / ' /proc/mounts
   ```

   The mount list, filtered by grep, is displayed. For example,

```
rootfs / rootfs rw 0 0
/dev/sdb5 / ext3 rw,relatime,errors=continue,user_xattr,acl,barrier=1,data=ordered 0 0
```

3. List disk drive partitions with labels. For example,

   ```
   ls -l /dev/disk/by-label | grep sd5
   ```

4. Verify that ISCROOT points to the device listed in the grep filter output.

   Using the example mount list in step 2, ISCROOT should be pointing to sdb5, matching the device "/dev/sdb5" listed on the second line of the grep filter output.

Section 10
Starting and Stopping Partitions and Platforms During Normal Operations

This section provides information on starting and stopping partitions and platforms during normal operations using the Fabric Manager. During normal operations partitions and platforms can be shutdown gracefully. A graceful shutdown is an orderly shutdown of the partition image or platform.

10.1. Gracefully Shutting Down a Partition Image

Graceful shutdown is an orderly shut down of the partition image.

To shut down the partition image gracefully

1. On the Fabric Manager user interface, point to **System Administration**, and then click **CPF System**.
2. Click **Platforms and Partitions**.

   The **Details: Platforms and Partitions** screen appears.
3. Click **Partitions** tab.

   The list of partition images appears.
4. Double-click the partition image you want to gracefully shutdown.

   The **Summary** tab displays the information about the selected partition image.
5. Click **Soft Shutdown**.

   The status of the partition image changes to **Stopped** and then **Disabled**.

10.2. Starting a Partition Image

Prerequisite: The EPP has to be powered on and the desired partition image is in stopped state.

Notes:

- *By default, after commissioning the partition image the status of the partition image will be always **RUNNING**. It is not necessary to start the partition image after commissioning the partition image.*
- *Starting the partition image is required only when*
  - *The partition image has previously been stopped or shut down.*
  - *The platform has been powered off and the initial state is set to stopped.*

To start a partition image

1. On the Fabric Manager user interface, point to **System Administration**, and then click **CPF System**.
2. Click **Platforms and Partitions**.

   The **Details: Platforms and Partitions** screen appears.
3. Click the **Partitions** tab.
4. Double-click the partition image that you want to start.

   The **Summary** tab displays the information about the selected partition image.
5. Click **Start**.

   The status of the partition image changes to **RUNNING**.

10.3. Performing Soft Shutdown on a Platform

The soft shutdown is an orderly shutdown of the platform and is also known as graceful shutdown. Soft shutdown is equivalent to pressing **Start** and then clicking the **Shut-down** and **Ok** buttons in a computer running the Windows operating system.

Following are the sequence of actions that are performed when you choose to soft shutdown a platform:

- Partition images are shut down.
- After all the partition images are shut down, the service partitions are shut down.
- Platform management card hardware is powered off.

You can gracefully shutdown a platform, if the platform is in a powered-on state.

To perform soft shutdown

1. On the Fabric Manager user interface, point to **System Administration**, and then click **CPF System**.

   The **Details: CPF-System** screen appears on the right pane.

2. Click **Platforms and Partitions**.

   The platforms and partitions are listed under their respective tabs in the **Details: Platforms and Partitions** screen on the right pane.

3. In the **Platforms** tab, double-click the platform that you want to gracefully shut down.

   The summary information about the platform appears.

4. In the **Summary** tab, click **Soft-Shutdown**.

   A message asking if you want to shut down the platform appears.

5. Click **Yes**.

   The selected platform gracefully shuts down.

Further Information

You must shut down multiple platforms one by one. Fabric Manager does not allow you to shut down all the platforms at the same time.

10.4. Powering-On a Platform

The powering-on platform operation is equivalent of pressing the physical power switch. This operation can only be performed if the platform is in a powered-off state. This option is disabled if the platform is already powered on.

Prerequisite: Platform is powered off.

To power on a platform

1. On the Fabric Manager user interface, point to **System Administration**, and then click **CPF System**.

   The **Details: CPF-System** screen appears on the right pane.

2. Click **Platforms and Partitions**.

   The platforms and partitions are listed under their respective tabs in the **Details: Platforms and Partitions** screen on the right pane.

3. In the **Platforms** tab, double-click the platform that you want to power on.

   The summary information about the platform appears.

4. In the **Summary** tab, point to **Advanced**, and click **Power On**.

   The selected platform is powered on. In the **Summary** tab, the status of the platform changes to **On**.

Section 11
Viewing, Adding, and Deleting Platforms

This section provides information about managing platforms.

11.1. Viewing the Platform Summary

The following table describes the various attributes of the platform that you can view on the platform summary:

Attribute	Description	Example
Summary		
Name	Denotes the name assigned to a platform when it is added to the fabric.	BankA
Description	Provides the description of a platform when it is added to the fabric.	This platform contains all the banking applications related to BankA.
Type	Describes the type of the platform when it is added to the fabric. The values can be NEPP or PEPP.	PEPP
Platform Number	This number is a unique numerical value that a user or the Fabric Manager assigns to a platform when it is added to the fabric. The number identifies the platform internally. The value ranges from numbers 1 to 16.	5

Attribute	Description	Example
DNS RAC Name	Denotes the Domain Name System Remote Access Controller name. It is a combination of platform name and number. It is defined automatically when a platform is added to the fabric. It is displayed in the web page header when you access the platform management console of the platform. ***Note:*** *Since the Fabric Manager does not use the DNS, it cannot be used to access the platform management console. To access the platform management console, use the IP address of the platform.*	BankA-5
Service Tag	Indicates the unique number of the platform hardware provided by the manufacturer. In the Call Home, this number is referred as platform serial number. It is a key identifier for the maintenance entitlement. You can reference this number when approaching Unisys for the support.	DWC4KY1
Maintenance Mode	Defines the status of the maintenance mode. It is enabled when maintenance activities are carried out on the fabric.	Disabled
Model No.	Displays the model number of the platform.	3560R G3
Processor Type	Denotes the processor brand, product line, model number, and operating frequency.	Intel(R) Xeon(R) CPU E5-2667 v2 @ 3.30GHz
Processor Frequency	Indicates the platform processor frequency.	3.3 GHz (per processor)
Sockets	Defines the number of sockets supported by the platform processor.	2

Attribute	Description	Example
Cores	Defines the number of cores supported by the platform processor.	16 (8 per socket)
Memory	Indicates the total memory available in the platform.	127 GB
Platform Overview		
Health	Denotes the status of the platform health. It can be one of the following: **Unknown**: Indicates that the Fabric Manager is unable to understand the status of the platform. **Ok**: Indicates that there are no issues found in platform. **Warning**: Indicates that the platform needs the attention. For example, Warning is displayed when the platform has an unsupported Software or Firmware version. **Critical**: Indicates that the platform needs immediate attention. For example, Critical is displayed when the temperature of the platform has exceeded the threshold value. This might cause a hardware failure.	Ok

Attribute	Description	Example
Events Statistics	Displays the number of critical, warning, and unknown events. Click on an event type to see all the events of that particular type that are generated for the platform. Click on View All to see all the events that are generated for the platform. ***Note:*** *The Nagios events do not impact the platform health. If the Nagios events are generated on a platform, then the* ***Event Statistics*** *of that platform indicates the critical events. However the platform health status still remains* ***Ok****.*	
Power	Indicates the status of the platform. It can be either **On** or **Off**.	On
s-Par® Instance	Denotes the version number and status of the s-Par® instance. The status can be either Running or Stopped. ***Notes:*** • *s-Par® instance is displayed only for PEPP.* • *If the s-Par version is displayed as "blank", then click* ***Advanced Settings****, and in the* ***s-Par Firmware*** *tab click* ***Synchronize****.*	Running
Partition Status	Displays the count of partition images that are in various states such as "Running", "Stopped", "Disabled", "In-Progress", "Unknown", and "Failed".	

To view the platform summary

1. On the Fabric Manager user interface, point to **System Administration**, and then click **CPF System**.

   The **Details: CPF-System** screen appears on the right pane.

2. Click **Platforms and Partitions**.

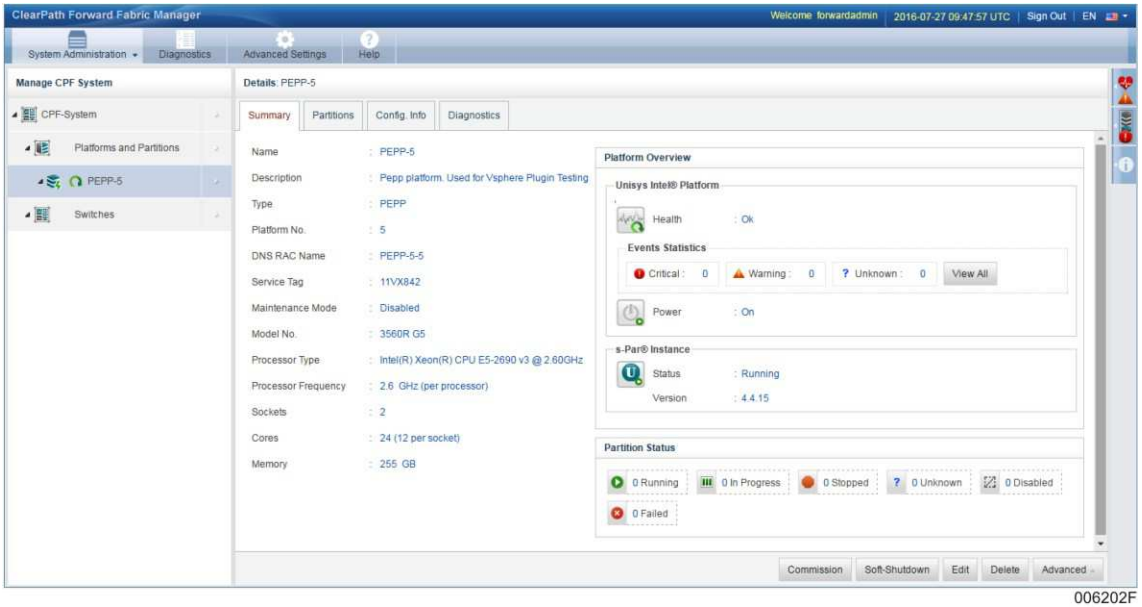
   The **Details: Platforms and Partitions** screen appears on the right pane.

3. On the **Platforms** tab, double-click the platform of which you want to view the summary.

   The Details: <platform name> screen appears.

4. Click the **Summary** tab.

   The summary of the platform appears.



006202F

11.2. Viewing Configuration Information of a Platform

The Fabric Manager user interface allows you to view the

- Partition images that you can commission on the selected platform
- Partition images that are already commissioned on that platform
- Partition image configuration details such as number of ports, cores, LUN size, and so on

To view the **Config. Info** tab

1. On the Fabric Manager user interface, point to **System Administration**, and then click **CPF System**.

   The **Details: CPF-System** screen appears on the right pane.

2. On the left pane, click **Platforms and Partitions**.

   The **Details: Platforms and Partitions** screen appears on the right pane.

3. On the **Platforms** tab, double-click the platform of which you want to view the configuration information.

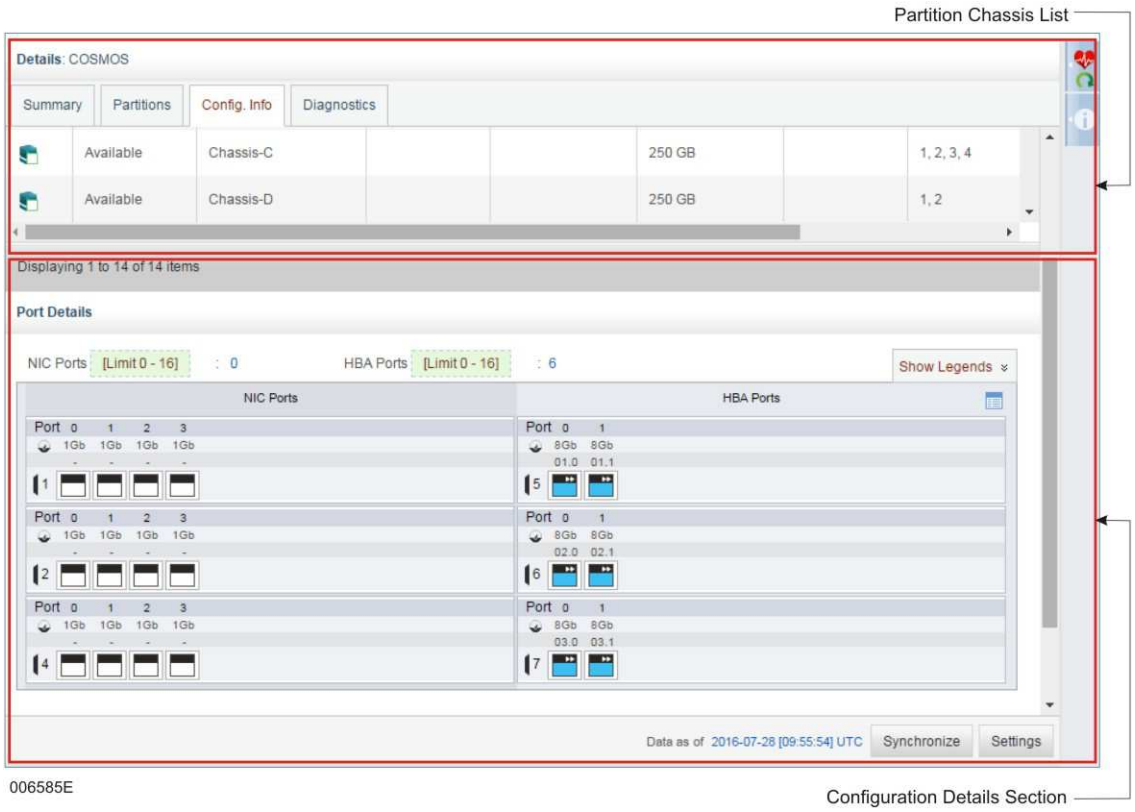
   The Details: <platform name> screen appears.

4. Click **Config. Info** tab.

The **Config. Info** tab comprises the following:

- 11.2.1 Partition Chassis List
- 11.2.2 Configuration Details Section
- 9.2.1 Identifying World Wide Port Name (WWPN) of HBA Ports

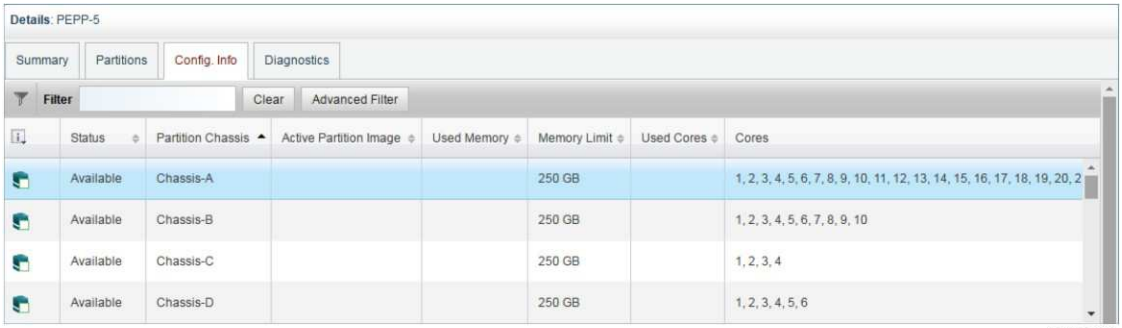
The following is an example of the **Config. Info** tab:



11.2.1. Partition Chassis List

This is the list of the partition chassis that are available for commissioning. It also includes the partition images that are already commissioned.

The following is an example of the partition chassis list in the **Config. Info** tab:



006587C

The partition chassis list provides you the following information:

- **Status**: Displays the status of the partition image. The status can be:
  - **Available**: Indicates that the partition image is not yet commissioned.
  - **Not Available**: Indicates that a partition image is not commissioned on the selected chassis but the resources required by the chassis are being used by a partition image commissioned on another chassis.
  - **Used**: Indicates that the partition image is already commissioned.
- **Partition Chassis**: Displays all the chassis available on a platform, for example, Chassis-A.
- **Active Partition Image**: Displays the name of the partition image that is commissioned on the Partition Chassis.
- **Used Memory**: Displays the memory size assigned to this partition image.
- **Memory Limit**: Displays the maximum memory size that can be assigned to the partition image commissioned on this Partition Chassis.
- **Active Cores**: Displays the processor cores associated with the partition image.
- **Cores**: Displays the cores that can be associated with a partition image.

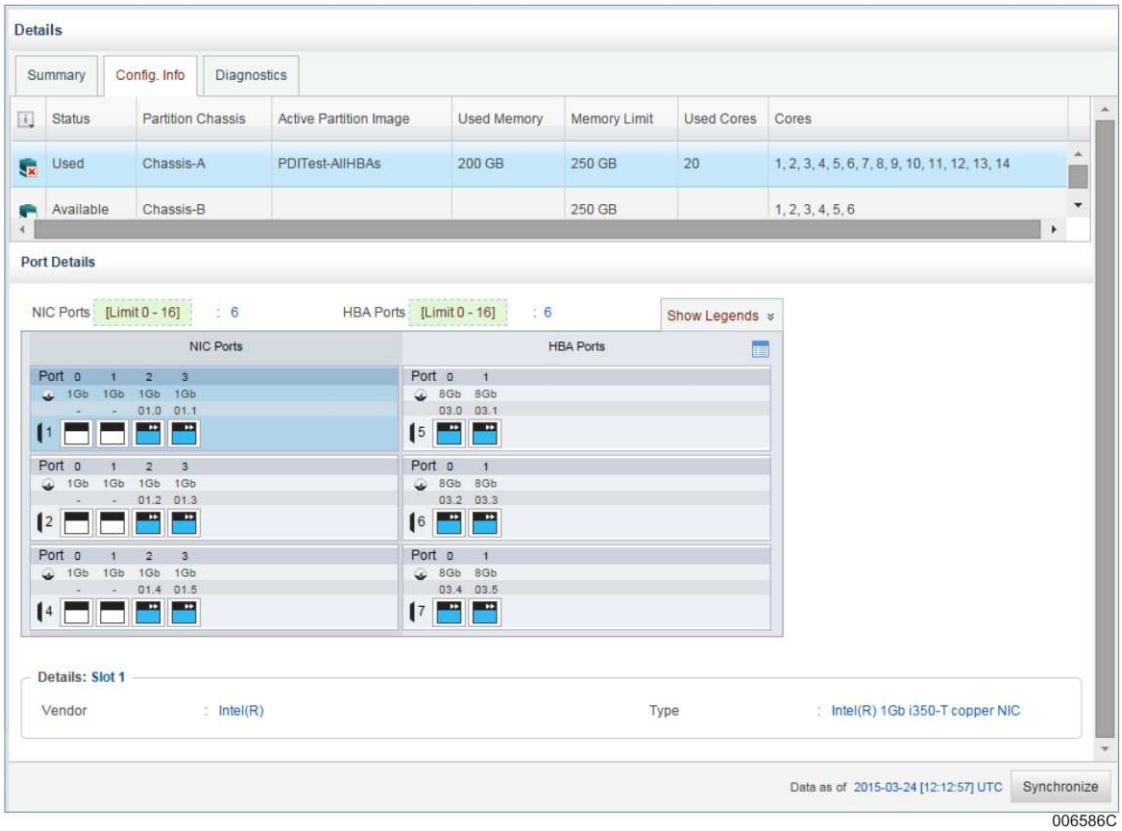
Note: *To know more about partition chassis, refer to the* ClearPath Forward Overview and Planning Guide.

11.2.2. Configuration Details Section

This section displays information about NIC and HBA ports.

The **Port Details** section displays the configuration details of the NIC and HBA Ports.

The following is an example of the **Port Details:** section in the **Config. Info** tab:



006586C

The **Port Details** section provides you the following information:

NIC Ports: Displays the number of NIC ports configured for the selected partition image. For each NIC port, it displays information about the network speed and if assigned, the Virtual Bus Device Function number of the port. When you position the pointer on any of the ports, a pop-up displays additional information about that port, such as whether the port is dedicated or shared, in use or available. In the case of shared ports, you can find information about the used and available number of logical ports.

HBA Ports: Displays the number of HBA ports that are configured for the selected partition image. For each HBA port, it displays information about the network speed and the Virtual Bus Device Function number of the port. When you position the pointer on any of the ports, a pop-up displays additional information about that port. The pop-up also displays the initiator World Wide Port Number (WWPN) of the HBA port. To view or export a complete list of HBA ports and their WWPNs, click in the upper right corner of **HBA Ports**.

Notes:

- *To learn more about various port icons displayed in the **Details** section, click **Show Legends**.*
- *You can use the Synchronize button to refresh the data in the **Details** section when*
  - *Platforms are added or deleted.*
  - *Partition images are commissioned on the platform.*
  - *Partition image attributes are modified.*

  *The date and time of the last synchronization is displayed next to the **Synchronize** button. It is recommended to perform synchronization before you start the partition image commissioning procedure.*
- *The **Synchronize** button should be used only when the power state of the Platform Management Card is ON and the s-Par® is in RUNNING state.*

11.2.3. Identifying World Wide Port Name (WWPN) of HBA Ports

If you plan to commission a partition image to a boot volume on an external storage device, you need to identify the HBA ports of your Partitionable Enterprise Partition Platform (PEPP) that will be allocated to the partition, as well as the initiator World Wide Port Name (WWPN) of the HBA ports, and provide the information to the storage administrator. The storage administrator needs this information to configure visibility from the HBA ports of the PEPP to the LUN on the external storage device where you will be creating the partition boot volume. You can view the WWPN of all the HBA ports of the platform in the **Config Info** tab.

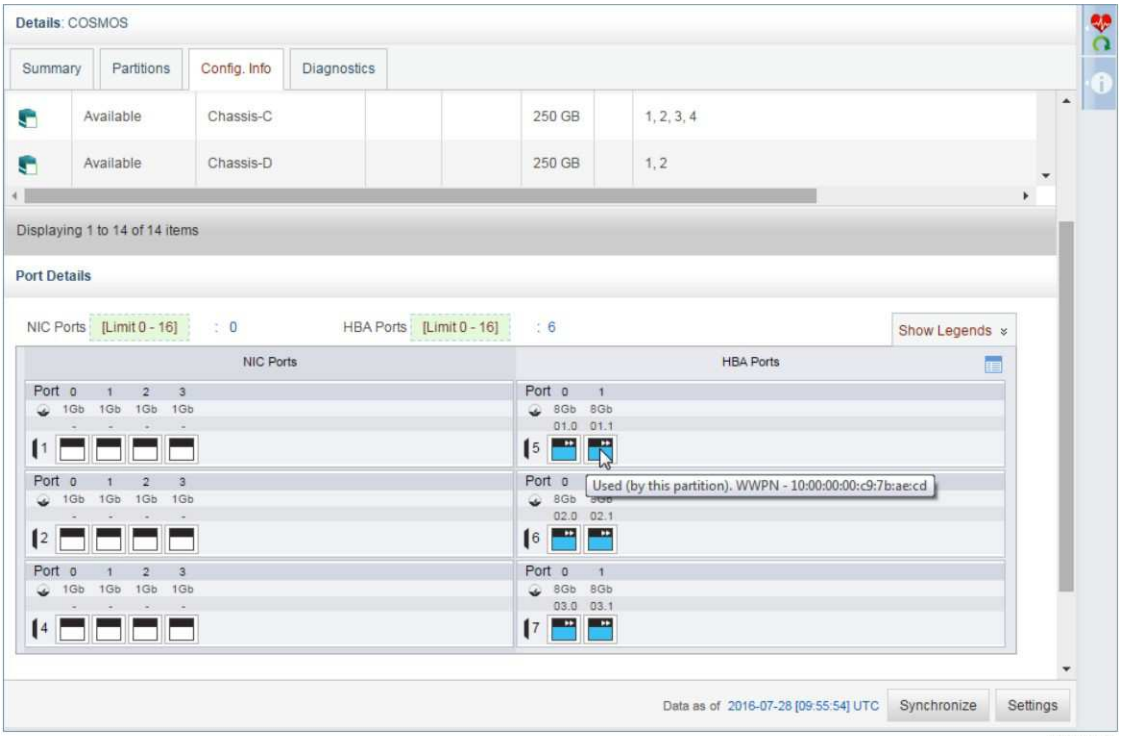
To view the WWPN information of a particular HBA port

1. On the Fabric Manager user interface, point to **System Administration**, and then click **CPF System**.

   The **Details: CPF-System** screen appears on the right pane.
2. Click **Platforms and Partitions**.

   The **Details: Platforms and Partitions** screen appears on the right pane.
3. On the **Platforms** tab, double-click the platform of which you want to view the configuration information.
4. Click **Config. Info** tab.
5. Under **Port Details**, hover the cursor on the graphical representation of the HBA port. The WWPN of the port is displayed in a pop-up box.

The following image shows an example of the pop-up box displaying the WWPN of a particular HBA port.



007469B

You can also view and optionally export the list of all the HBA ports and their WWPNs. To view the list of HBAs and their WWPNs

1. On the Fabric Manager user interface, point to **System Administration**, and then click **CPF System**.

   The **Details: CPF-System** screen appears on the right pane.

2. Click **Platforms and Partitions**.

   The **Details: Platforms and Partitions** screen appears on the right pane.

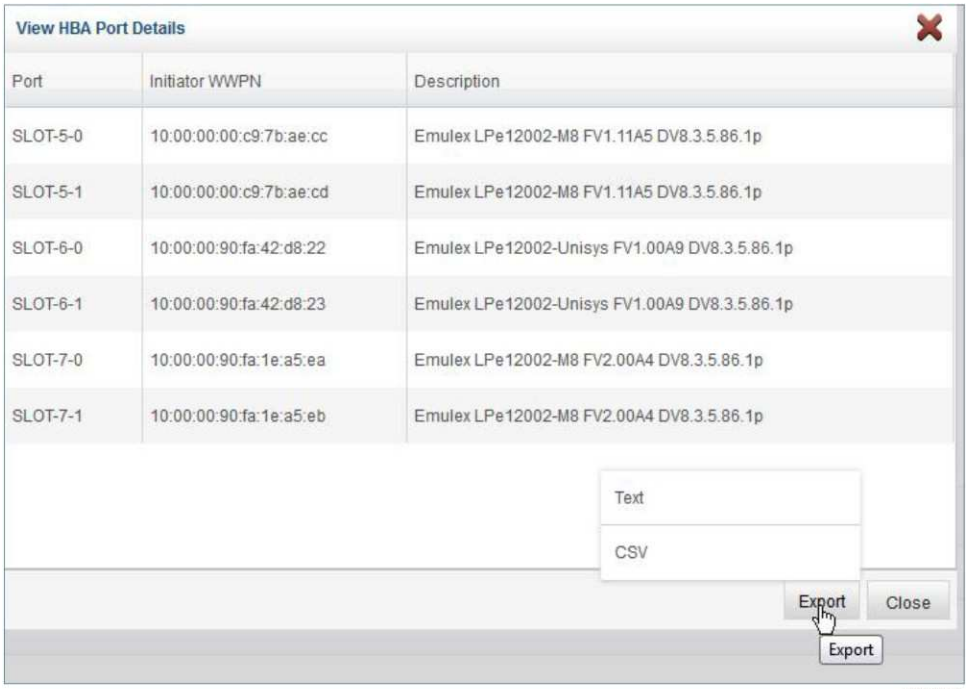
3. On the **Platforms** tab, double-click the platform of which you want to view the configuration information.

4. Click **Config. Info** tab.

5. Under **Port Details,** on the upper right corner of the **HBA ports** column, click . The **View HBA Port Details** dialog box appears. The information displayed includes the slot number, the port number and the corresponding WWPN (otherwise known as WWN of the port) for all the HBA ports on the platform.

   To export the complete list of HBA Ports and their WWPNs, click **Export**. The list is exported as a file. Store the file on your local machine in any preferred folder. When providing the information to your storage administrator, be sure to identify the specific HBA ports that will be the boot paths for your partition.

The following image is an example of the View HBA Port Details dialog box.

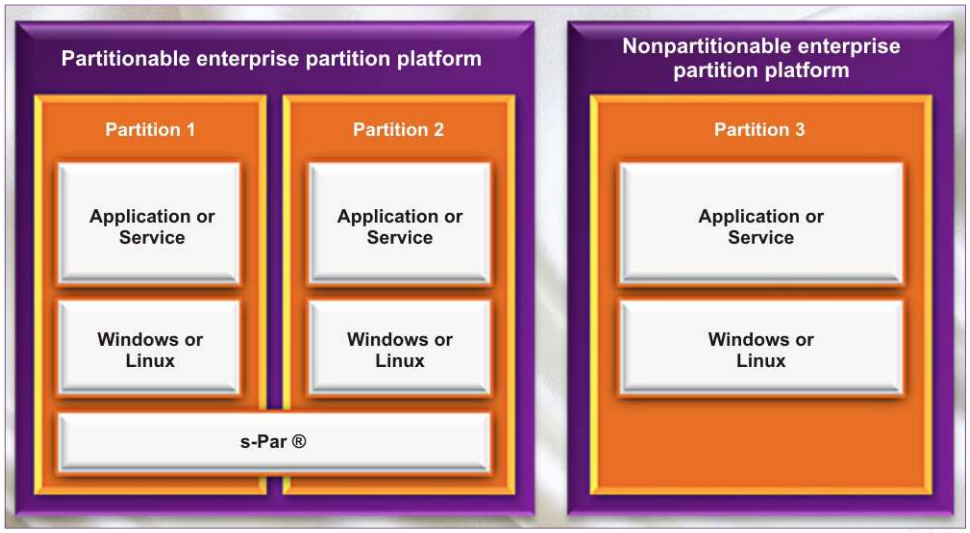


11.3. Adding a Platform to the Fabric

Platforms are physical computers in the fabric on which you can host one or more partition images. The Fabric Manager allows you to add additional enterprise partition platforms to the fabric. You can add up to 32 platforms to a fabric.

There are two types of platforms

- Nonpartitionable enterprise partition platform (NEPP): A Unisys enterprise partition platform (EPP) that does not run Unisys Secure Partitioning (s-Par®) firmware and thus can run only a single operating environment.
- Partitionable enterprise partition platform (PEPP): A Unisys enterprise partition platform (EPP) that runs Unisys Secure Partitioning (s-Par®) firmware and thus can run multiple operating environments (operating systems) simultaneously.



Note: *Both field engineers (users with the FF_FieldEngineer role) and administrators (users with the FF_Administrator role) have required privileges to add a platform to a fabric.*

Prerequisites

- Default IP address of platform management card (PMC), and s-Par® management services (sMS) should be configured.
- PMC should be AC powered on and reachable.
- Platform should be connected to the FM LAN.

  Note: *If more than one platform is being added to an existing fabric, then the platform*

  - *Must have the AC power applied one at a time.*
  - *Must be configured separately because they have overlapping IP addresses.*

- If you have changed the default subnet addresses for the FM LAN, then the first two octets of the platform IP address should be the same as the subnet address set in edit system.

  To know more about editing system attributes, refer the *ClearPath Forward Administration and Operations Guide.*

  Note: *Only the field engineers (users with the FF_FieldEngineer role) can change the subnet address of FM LAN.*

- To add the NEPP Platform, you should assign the FM LAN IP to the OS installed on the NEPP partition image. If the FM LAN subnet IP is <x.x> and platform number is y, then FM LAN IP becomes x.x.y.1. You can change this if the OS is installed on NEPP platform.

To add a platform to the fabric

1. On the Fabric Manager user interface, point to **System Administration**, and then click **CPF System**.

   The **Details: CPF-System** screen appears on the right pane.

2. Click **Platforms and Partitions**.

   The Details: Platforms and Partitions screen appears on the right pane.

3. Click **ADD** on the right pane.

   Alternatively, click the arrow next to **CPF-System**, point to **Add**, and click **Platform**.

   A message confirming the verification of power supply connection or network connection appears.

4. Click **Yes**.

   The Add Platform window appears.

5. In **Platform Type**, select one of the following options:

   - **PEPP**: Partitionable enterprise partition platform with s-Par®
   - **NEPP**: Non-partitionable enterprise partition Platform

   If you choose **PEPP**, perform the following steps:

   a. In the **Platform Name**, type a unique name for the platform. This is a mandatory field.

      Note: *The maximum length of the platform name can be up to 16 alphanumeric characters along with "-". The name cannot start with the character "-".*

   b. In the **Platform Number** field, select the required platform number.

   c. In **Platform Description**, type a description for the platform.

      Note: *Provide a meaningful description for the platform. The maximum length of the platform description can be up to 256 alphanumeric characters along with space, "-", and ".". The length of any word in the description should not exceed 20 characters.*

If you choose **NEPP**, perform the following steps:

a. In the **Platform Name**, type a unique name for the platform. This is a mandatory field.

Notes:

- *The maximum length of the platform name can be up to 16 alphanumeric characters along with "-". The name however cannot start with the character "-".*
- *The following is a list of names that you cannot use to name a platform:*

0	forward-system	forwardsystem	localhost
FMP-1	FMP-2	secure-fabric	securefabric
secure-fabrics	securefabrics	ip-lan	iplan
fmlan	fm-lan	hdlan	hd-lan
physical-fabric	physicalfabric	physicalfabrics	physical-fabrics
switch	switches	forwardsystems	cpf-system

b. In the **Platform Number** field, select the required platform number.

c. In the **Platform Description**, type a description for the platform.

Note: *Provide a meaningful description for the platform. The maximum length of the platform description can be up to 256 alphanumeric characters along with space, "-" and ".". The length of any word in the description should not exceed 20 characters.*

d. In **Partition Image Name**, type a unique name for partition. This is a mandatory field.

Note: *The maximum length of the partition image name can be up to 15 alphanumeric characters along with "-". The name however cannot start with the character "-".*

e. In **Partition Image Description**, type a description for the platform.

Note: *Provide a meaningful description for the Partition Image. The maximum length of the Partition Image description can be up to 256 alphanumeric characters along with space, "-" and ".". The length of any word in the description should not exceed 20 characters.*

6. Click **Add**.

A message appears informing you that the platform is added successfully and an initiated audit event is displayed in the Events Console.

If the EPP is successfully added, it appears under **Manage CPF System** with the current state information. Also, on the **Details: Platforms and Partitions** pane, a summary of the newly added platform appears.

You can now commission a partition image on the newly added platform. See 5.3 Commissioning a Partition Image for more information.

Notes:

- *The Add platform action does not block you from performing other operations simultaneously.*
- *If the EPP is successfully added, then it is visible under* ***Manage CPF System*** *with the current state information. Also, on the* ***Details: Platforms and Partitions*** *pane, a summary of the newly added platform appears and a success audit event is generated.*
- *If you try to add or delete a platform when an add platform is already in progress, then an error message appears informing you that the add platform operation is failed as an Add or Delete operation is already in progress and a failure audit event is generated.*

11.4. Deleting Partitionable EPP

You may need to delete the partitionable EPP when it needs to be replaced with a new one, or if the platform is not required.

Prerequisites:

- All the partition images under the platform are decommissioned.
- Platform is in running state.

To delete the partitionable EPP

1. On the Fabric Manager user interface, point to **System Administration**, and then click **CPF System**.

   The **Details: CPF-System** screen appears on the right pane.

2. Click **Platforms and Partitions**.

   The Details: Platforms and Partitions screen appears on the right pane.

3. On the **Platforms** tab, click the partitionable EPP that you want to delete and then click **Delete** on the right pane.

4. Under the **Summary** tab, click **Delete**.

   Alternatively, on the left pane, click the arrow next to the partitionable EPP, and then click **Delete**.

   A confirmatory message asking if you want to delete the partitionable EPP appears.

5. Click **Ok**.

   A message appears informing you that the platform is deleted successfully and an initiated audit event is displayed in the Events Console.

Notes:

- *The Delete platform action does not block you from performing other operations simultaneously.*
- *It is recommended to delete all the events related to the deleted partitionable EPP.*

- *If the delete platform operation is successful, then a success audit is generated. The deleted partitionable EPP will not be visible under **Manage CPF System** and cannot be used any further.*
- *If a delete platform is not successful, then a Failure audit event is generated.*
- *If you try to add or delete a platform when a delete platform is already in progress, then an error message appears informing you that the delete platform operation is failed as Add or Delete operation is already in progress and a failure audit event is generated.*

11.5. Deleting Nonpartitionable EPP

Prerequisites:

- Nonpartitionable EPP is powered off.
- Partition image under nonpartitionable EPP is in stopped state.

To delete the nonpartitionable EPP

1. On the Fabric Manager user interface, point to **System Administration**, and then click **CPF System**.

   The **Details: CPF-System** screen appears on the right pane.

2. Click **Platforms and Partitions**.

   The **Details: Platforms and Partitions** screen appears on the right pane.

3. On the **Platforms** tab, double-click the nonpartitionable EPP that you want to delete, and then click **Delete** on the right pane.

   Alternatively, click the arrow next to the nonpartitionable EPP, and then click **Delete**.

   A confirmatory message asking if you want to delete the nonpartitionable EPP appears.

4. Click **Ok**.

   A message appears informing you that the platform is deleted successfully and an initiated audit event is displayed in the Events Console.

Notes:

- *It is recommended to delete all the events related to the deleted non-partitionable EPP.*
- *If the delete platform is successful, then the platform is deleted from the Event Console and a success audit is generated. The deleted non-partitionable EPP will not be visible under **Manage CPF System** and cannot be used any further.*
- *If a delete platform is not successful, then a failure audit event is generated.*
- *If you try to add or delete a platform when a delete platform is already in progress, then an error message appears informing you that the delete platform operation is failed as Add or Delete operation is already in progress and a failure audit event is generated.*

Section 12
Launching the PMC Virtual Console and Partition Image Console

This section provides information on launching the PMC Virtual Console and Partition Image Console (partition desktop). Many procedures in ClearPath Forward documentation require that you launch these consoles.

12.1. Launching the Platform Management Card (PMC) Virtual Console

Using the Platform Management Card, you can perform advanced tasks such as configuring platform management card virtual console properties and users, performing remote management tasks, and troubleshooting remotely managed systems.

> **Caution**
>
> Do not change the default DNC RAC name, IP address, NTP settings and Time zone settings on the Platform Management Card (PMC). By default, the time zone is set to UTC. Any change to one of these will alter the time zone setting, which in turn will impact the event time stamps.

Note:

- *Only users with the Field Engineer role can perform this operation.*
- *This operation can be performed only from the Fabric Management Platform. When you log on to the Fabric Management Platform, you can access the desktop of the partition images that are commissioned using the Fabric Manager user interface. The partition desktop can only be accessed from a Firefox browser session on the Fabric Management Platform since the access is restricted to the FM LAN environment.*

To launch PMC

1. Using a RDP client software (for example, Remote Desktop Connection on a Windows computer), access and log on to the Fabric Management Platform.
2. On the Fabric Management Platform, enter http://localhost in a browser to access the Fabric Manager, point to **System Administration**, and then click **CPF System**.
3. Click **Platforms and Partitions**.

   The **Details: Platforms and Partitions** screen appears on the right pane.
4. On the **Platforms** tab, double-click the platform for which you want to launch PMC Console.
5. Under the **Summary** tab, click **Launch Console**.

   The PMC console opens in a new browser tab.

   Note: *Remember to log out and close the console when you are done with your session.*

12.2. Accessing the Partition Image Console (Partition Desktop)

If you are logged on to the Fabric Management Platform, you can access the desktop of the partition images that you commissioned using the Fabric Manager user interface. The partition desktop can only be accessed from a Firefox browser session on the Fabric Management Platform since the access is restricted to the FM LAN environment.

Note: *You cannot access the Partition Image Console or Partition Desktop for nonpartitionable EPP partition images.*

Prerequisites:

- You are in the FM LAN environment and logged on to the Fabric Management Platform.
- The following software packages are installed on the Fabric Management Platform:
  - Wine
  - Unisys auth service package
  - Partition desktop software

  Typically, Unisys installs the software before shipping the Fabric Management Platform.
- The following software services are running on the Fabric Management Platform:
  - rcunisysauthservice status
  - rcwinbind status
  - rcsmb status

  Typically, the services are set to run by default.

To access a partition desktop:

1. Using Remote Desktop Protocol (RDP) client software (for example, Remote Desktop Connection on a Windows computer), access and log on to the Fabric Management Platform.
2. On the Fabric Management Platform, enter http://localhost in a browser to access the Fabric Manager.
3. Use Fabric Manager to locate the desired partition image and verify that the current status is RUNNING.
4. Click **Launch Console** to open a partition image console window.
5. Log in with appropriate credentials.

   The default users are Administrator and Operator. Use the password that you provided while running the post installation script.

Note: *Remember to log out and close the console when you are done with your session.*

Section 13
Hardening and Unhardening Application Operating Environments

Unisys implements best practices for secure operating system configurations to make your application operating environments more robust, resilient, and secure.

13.1. Hardening Your Operating System

To ensure that your ClearPath Forward fabric is resilient and secure while continuously meeting the needs of your enterprise-class applications, Unisys combines its experience with recommendations for enterprise systems from operating system vendors and industry security experts, and recommends implementing best practices when configuring Windows and Linux operating systems in the fabric.

Typically, operating system configurations are permissive out of the box from operating system vendors, and the emphasis is on ease of use, not security. While such settings may suffice for the commodity market, mission critical enterprise systems require more secure configurations, in particular the following areas:

- Disk partitioning settings
- Auditing and logging settings
- Networking and firewall settings
- Password policies
- File and directory permissions
- Automatic or manual updating of software

Caution

Issues involved in improving the security of a system are complex and Unisys strongly recommends the administrator seek additional information on the latest security best practices by referencing all available resources.

Leveraging its extensive experience in the industry and understanding of the needs of the ClearPath Forward fabric, Unisys integrates its knowledge with best practices (as of May 2015) from multiple sources for recommendations and tools for hardening the operating system configurations in such environments. Some sources include:

- Microsoft documentation for Windows Server, for example
  - Windows Server 2008 R2

    http://technet.microsoft.com/en-us/library/dd548350.aspx
  - Windows Server 2012

    http://technet.microsoft.com/en-us/library/hh831360.aspx
- Red Hat documentation for Red Hat Enterprise Linux (RHEL), for example
  - https://access.redhat.com/site/documentation/Red_Hat_Enterprise_Linux/
  - https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Security_Guide/index.html
  - https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Security-Enhanced_Linux/index.html
- SUSE documentation for SUSE LINUX Enterprise Server (SLES), for example
  - https://www.suse.com/documentation/sles11/
  - https://www.suse.com/documentation/sles11/book_security/?page=/documentation/sles11/book_security/data/book_security.html
  - https://www.suse.com/documentation/sles11/book_hardening/?page=/documentation/sles11/book_hardening/data/book_hardening.html
- Various publications by the Center for Internet Security, in particular security benchmark configuration recommendations, available at

  http://www.cisecurity.org/resources-publications/
- Various Security Technical Implementation Guides (STIGs). For more information on STIGs, refer to

  http://iase.disa.mil/stigs/Pages/index.aspx

  Note: *This website may not be accessible from all global locations.*

13.2. ClearPath Forward Hardening Tools for Windows and Linux

The ClearPath Forward Hardening Tools are scripts that help you apply configuration files containing hardening parameter settings on a target operating system. You can also use the hardening tools to audit your current operating system security settings, generate a report, or apply a different configuration file to remove or restore hardening parameter settings. The hardening tools contain brief descriptions of the security parameters, and the effect of enabling or disabling the settings. For detailed descriptions, refer to the extensive documentation available from the operating system vendors and industry security experts (see list in 13.1 Hardening Your Operating System).

For user convenience, as a starting point, Unisys developed a series of configuration files describing levels of hardening with predefined security levels Unisys recommends for operating environments in the fabric.

You can create your own configuration files with customized settings to suit your particular needs: Create a local copy of one of the supplied configuration files, and then modify the settings in it.

Note: *The supplied configuration files are only a starting point Unisys provides for your convenience, and are based upon best practices as of May 2015. For current best practices, consult your Unisys service representative.*

Requirements for Use of ClearPath Forward Hardening Tools

The ClearPath Forward Hardening Tools have been qualified for use with the following operating systems:

- Windows Server 2008 R2 SP1
- Windows Server 2012
- SUSE Linux Enterprise Server (SLES) 11 SP3
- Red Hat Enterprise Linux (RHEL) 6.4

If you wish to use the hardening tools on a later version of an operating system that is supported for use with the fabric, contact your Unisys sales representative for assistance. For more details on the latest list of supported operating systems, refer to the ClearPath Forward Supported Operating Systems link that is available from the ClearPath Forward portion of the Unisys Product Support site.

Levels of Hardening for Windows Operating Systems Predefined by Unisys

The security settings for operating systems commissioned with Unisys-supplied blueprints are the same settings provided by Microsoft; and the security settings for operating systems commissioned with customer-supplied blueprints are the same settings as when you created your customer-supplied operating system image.

- None – Default level until the initial run of the ClearPath Forward Hardening Tool for Windows.

  If you changed any security settings in the operating system, your default reflects the base security settings provided out of the box plus any custom security settings that you have manually applied to the operating system.

  Note: *The value of None is not a valid option when running the hardening tool.*

- 0 – Settings for level 0 are captured when the hardening tool is first run. A snapshot of the existing settings is saved as level 0, thereby providing a baseline for rollback purposes if needed.

  Note: *If you changed settings in your operating system before running the ClearPath Forward Hardening Tool for Windows for the first time, the modified settings will be captured and saved as the baseline (that is, as level 0 of hardening).*

- 1 – Medium hardened, defined by Unisys as the recommended hardened state.
- 2 – Extremely hardened, defined by Unisys for use when high levels of security are needed. However, these settings may prevent some applications from running or stop some operations from working.

Levels of Hardening for Linux Operating Systems Predefined by Unisys

The security settings for operating systems commissioned with Unisys-supplied blueprints are the same settings provided by SUSE or Red Hat; and the security settings for operating systems commissioned with customer-supplied blueprints are the same settings as when you created your customer-supplied operating system image.

- None – Default level of security settings that are provided out of the box by the Linux operating system vendor.

  Notes:

  - *The value of None is not a valid option when running the hardening tool.*
  - *If you wish to save a copy of these security settings as a baseline for rollback purposes, you can create a configuration file based on the existing settings. See 13.5 Capturing a Snapshot of Existing Security Settings for more information.*

- 0 – Minimally hardened, defined by Unisys (as of May 2015) as bare minimum security.
- 1 – Medium hardened, defined by Unisys as the recommended hardened state.
- 2 – Extremely hardened, defined by Unisys for use when high levels of security are needed. However, these settings may prevent some applications from running or stop some operations from working.

13.3. Using the ClearPath Forward Hardening Tool for Windows

Note: *The ClearPath Forward Hardening Tool for Windows has been qualified for use with the following operating systems:*

- *Windows Server 2008 R2 SP1*
- *Windows Server 2012*

If you wish to use the hardening tool on a later version of an operating system that is supported for use with the fabric, contact your Unisys sales representative for assistance. For more details on the latest list of supported operating systems, refer to the ClearPath Forward Supported Operating Systems link that is available from the ClearPath Forward portion of the Unisys Product Support site.

The ClearPath Forward Hardening Tool for Windows provides a configuration file with predefined security levels for improving the security of the operating system. The tool is a Windows PowerShell script named **Apply-Hardening.ps1**, and is available at C:\ProgramData\Unisys\Hardening. The script also stores rollback files, logs, and other artifacts it creates in the same folder.

Before running the script, be sure that the Windows PowerShell execution policy is set to RemoteSigned. To check and set the execution policy (if needed),

1. Locate and right-click **Windows PowerShell**, select **Run as administrator**, type **Get-ExecutionPolicy** at the prompt, and then press **Enter**.

   The current execution policy setting is displayed. By default, the setting is Restricted.

2. If the setting is not RemoteSigned, note down the setting, type **Set-ExecutionPolicy RemoteSigned -force** at the prompt, and then press **Enter**.

If desired, restore the Windows PowerShell execution policy setting to the recorded value after you run the hardening script.

To run the script, locate and right-click **Windows PowerShell**, select **Run as administrator**, and then enter the following command at the prompt

```
C:\ProgramData\Unisys\Hardening\Apply-Hardening.ps1 -level <level number> <options>
```

Where

- *<level number>* specifies the level of hardening. Valid values are 0, 1, or 2.
- *<options>* specify whether to audit your current operating system security settings and generate a report, apply a configuration file without creating a rollback file of the current settings, or apply a specific configuration file.

Option	Description
–reportOnly	Generates an audit report. By default, the hardening tool applies security settings changes according to rules in the configuration file, and does not generate a report. Include this option to generate a report that compares the current operating system security settings to the recommended settings for the specified level. No changes are made to the operating system security settings. The report file is available at C:\ProgramData\Unisys\Hardening\report.txt.
–noRollback	Skips the creation of a rollback file. By default, before applying any security setting changes, the hardening tool creates a rollback file containing the current settings of the operating system (C:\ProgramData\Unisys\Hardening\rollback<*timestamp*>.xml). Include this option to omit the creation of a rollback file.
–file <*file name*>	Specifies a file that contains a set of hardening rules (security settings) in the recognized XML format. Use this option to apply one of the intermediate rollback files previously created by the tool, or to apply a custom configuration file. To create a custom configuration file, make a copy of the Unisys-supplied configuration file and modify the copy with your desired security setting values. If a file is specified, it is used instead of the Unisys-supplied configuration file. If no file is specified, the Unisys-supplied configuration file (C:\ProgramData\Unisys\Hardening\rules<*OS version*>.xml) is used. This option is ignored if the –level parameter is set to 0.
–verbose	Displays details in the Windows PowerShell window as the hardening script executes. By default, the hardening tool runs silently. Include this option to display details—warning messages appear in yellow, and errors appear in red. This setting does not affect contents of the log or report files.

Remember to reboot your operating system after running the script.

For detailed help and more information on the syntax, enter the following command at a Windows PowerShell prompt:

```
get-help C:\ProgramData\Unisys\Hardening\Apply-Hardening.ps1 -detailed
```

Examples

To set the operating system security settings to the level 1 settings in the Unisys-supplied configuration file:

```
C:\ProgramData\Unisys\Hardening\Apply-Hardening.ps1 -level 1
```

To generate an audit report of how the current operating system security settings are different from the level 1 settings in the Unisys-supplied configuration file, as well as display the report in the Windows PowerShell window:

```
C:\ProgramData\Unisys\Hardening\Apply-Hardening.ps1 -level 1 –reportOnly –verbose
```

To roll back the operating system security settings to the level 0 settings, and display progress in the Windows PowerShell window:

```
C:\ProgramData\Unisys\Hardening\Apply-Hardening.ps1 –level 0 –verbose
```

To set the operating system security settings to the level 2 settings in the Unisys-supplied configuration file, without creating a rollback file:

```
C:\ProgramData\Unisys\Hardening\Apply-Hardening.ps1 -level 2 –noRollback
```

To roll back the operating system security settings to the level 2 settings in the configuration file captured on September 19, 2013:

```
C:\ProgramData\Unisys\Hardening\Apply-Hardening.ps1 –level 2 –file C:\ProgramData\
Unisys\hardening\Rollback\intermediate\0919201350804.xml
```

13.4. Using the ClearPath Forward Hardening Tool for Linux

Note: *The ClearPath Forward Hardening Tool for Linux has been qualified for use with the following operating systems:*

- *SUSE Linux Enterprise Server (SLES) 11 SP3*
- *Red Hat Enterprise Linux (RHEL) 6.4*

If you wish to use the hardening tool on a later version of an operating system that is supported for use with the fabric, contact your Unisys sales representative for assistance. For more details on the latest list of supported operating systems, refer to the ClearPath Forward Supported Operating Systems link that is available from the ClearPath Forward portion of the Unisys Product Support site.

The ClearPath Forward Hardening Tool for Linux provides configuration files with predefined security levels for improving the security of the operating system. The hardening script is available at /usr/bin/harden.

The system administrator can use the tool to

- Compare the current state of the security settings of the operating system to details in a configuration file to see if a particular setting is enabled or disabled.

  An example of a command for verifying the current state of the security settings of the operating system to a particular configuration file:

  ```
  harden -c /var/lib/harden/configs/Harden-SLES11SP3-Level1-default.cfg
  ```

- Audit the current state of the security settings of the operating system and generate a report describing areas that could be hardened to further improve security.

Note: *As some recommendations may conflict with application needs, be sure to consider the requirements of applications on the partition before modifying any settings.*

An example of a command for performing an audit of the security settings of the operating system and generating a report of possible steps than can be taken to improve the security of the operating system:

```
harden -r
```

- Create a configuration file based on the current state of the security settings of the operating system.

  An example of creating a configuration file based on the current state of the security settings of the operating system:

  ```
  harden -o /tmp/my_custom_settings.cfg
  ```

  The administrator may edit the file to enable or disable a number of the settings before applying the custom configuration file.

- Apply a configuration file to adjust security policies on the operating system.

  An example of a command for applying a particular configuration file:

```
harden -i /var/lib/harden/configs/Harden-SLES11SP3-Level1-default.cfg
```

13.5. Capturing a Snapshot of Existing Security Settings

You can use the ClearPath Forward Hardening Tools to save a copy of your current operating system security settings. This may be useful as a baseline for rollback purposes if needed.

Windows Operating Systems

By default, the ClearPath Forward Hardening Tool for Windows always creates a rollback file containing the current settings of the operating system before applying any security setting changes. When the hardening tool is first run, the existing security settings are saved as level 0 of hardening and a baseline for rolling back.

To save a copy of the initial state of the security settings of the operating system, do the following to create the level 0 configuration file based on your existing settings:

1. If necessary, download and install the ClearPath Forward Hardening Tool for Windows on your target operating system.

   Note: *The latest version of the hardening tools are available from the Unisys Product Support website: Locate the ClearPath Forward Product Support page, and then browse to the Software tab on the Drivers and Downloads page.*

2. Set your Windows PowerShell execution policy to RemoteSigned.

3. Run the tool (a Windows PowerShell script named **Apply-Hardening.ps1**) to apply any level of hardening other than level 0. For example,

   ```
   C:\ProgramData\Unisys\Hardening\Apply-Hardening.ps1 -level 1
   ```

   Note: *Be sure to not include the –norollback option.*

4. If desired, apply the level 0 of hardening to rollback any changes. For example,

   ```
   C:\ProgramData\Unisys\Hardening\Apply-Hardening.ps1 –level 0
   ```

For detailed help and more information on the syntax, enter the following command at a Windows PowerShell prompt:

```
get-help C:\ProgramData\Unisys\Hardening\Apply-Hardening.ps1 -detailed
```

For more information on using the tool, see 13.3 Using the ClearPath Forward Hardening Tool for Windows.

Linux Operating Systems

To save a copy of the current state of the security settings of the operating system, do the following to create a configuration file based on your existing settings:

1. If necessary, download and install the ClearPath Forward Hardening Tool for Linux on your target operating system.

   Note: *The latest version of the hardening tools are available from the Unisys Product Support website: Locate the ClearPath Forward Product Support page, and then browse to the Software tab on the Drivers and Downloads page.*

2. Run the tool (available at **/usr/bin/harden**) with the **–o** parameter. For example,

   ```
   harden -o /tmp/my_initial_settings.cfg
   ```

For more information on using the tool, see 13.4 Using the ClearPath Forward Hardening Tool for Linux.

13.6. Identifying the Security Settings on Your Operating System

You can use the ClearPath Forward Hardening Tools to audit your current operating system security settings. This may be useful when planning how you wish to configure your operating systems in support of specific application workloads.

Windows Operating Systems

To generate a report that compares the current security settings of your operating system (for example, a Windows Server 2012 operating system commissioned with Unisys-supplied blueprints) to the recommended settings for a hardening level recommended by Unisys (for example, level 1), do the following:

1. If necessary, download and install the ClearPath Forward Hardening Tool for Windows on your target operating system.

   Note: *The latest version of the hardening tools are available from the Unisys Product Support website: Locate the ClearPath Forward Product Support page, and then browse to the Software tab on the Drivers and Downloads page.*

2. Set your Windows PowerShell execution policy to RemoteSigned.
3. Run the tool (a Windows PowerShell script named **Apply-Hardening.ps1**) with the **–reportOnly** option.

For detailed help and more information on the syntax, enter the following command at a Windows PowerShell prompt:

```
get-help C:\ProgramData\Unisys\Hardening\Apply-Hardening.ps1 -detailed
```

For more information on using the tool, see 13.3 Using the ClearPath Forward Hardening Tool for Windows.

Linux Operating Systems

To audit the current state of the security settings of your operating system (for example, a SUSE Linux Enterprise Server 11 SP3 operating system commissioned with Unisys-supplied blueprints), and generate a report describing areas that could be hardened to further improve security, do the following:

1. If necessary, download and install the ClearPath Forward Hardening Tool for Linux on your target operating system.

   Note: *The latest version of the hardening tools are available from the Unisys Product Support website: Locate the ClearPath Forward Product Support page, and then browse to the Software tab on the Drivers and Downloads page.*

2. Run the tool (available at **/usr/bin/harden**) with the **–r** parameter.

For more information on using the tool, see 13.4 Using the ClearPath Forward Hardening Tool for Linux.

Note: *As some recommendations may conflict with application needs, be sure to consider the requirements of applications on the partition before modifying any settings.*

Section 14

Backing Up and Restoring Fabric Management Platform, Fabric Manager, and Application Operating Environments on PEPPs

This section provides information on backup and restore procedures in the following topics:

14.1. FMP Server Backup

The FMP Manager allows you to take an FMP server backup. You can perform activities such as backing up and restoring the FMP server.

For information on how to access the FMP Manager user interface, see the *ClearPath Forward Administration and Operations Guide*.

Note: *You should not restore the FMP server information when a cluster is active. It may reset the network and other vital system configuration parameters.*

The following sections provide details on how to perform these activities:

14.1.1. Backing Up and Downloading FMP Server Information

This tab allows you to take a backup of the FMP server information and downloads it to your local computer.

To backup and download the FMP server information,

1. From the FMP Manager user interface, select the **Utilities** menu, and then on the Utilities page, select the **FMP Server Backup** tab.
2. Click **Backup & Download**.

   A confirmation message appears.
3. Click **Yes**.

   The FMP Server Backup Status window displays the operation status.
4. After the process is complete, click **Download** to download the file.

   The FMP server information is backed up and downloaded. Along with the FMP Server information, additional files (md5 and log files) are also downloaded.

For more information on the various utilities provided by the ClearPath Forward Fabric Management Platform Manager, refer to the associated help.

14.1.2. Uploading and Restoring FMP Server Information

You can upload and restore the FMP server information. Using the **Upload & Restore** button you can browse your local system for a backup, or choose a file that has already been uploaded to the FMP, and upload the required backup file. It is recommended to use this feature on non-clustered FMPs.

To upload and restore FMP server information,

1. From the FMP Manager user interface, select the **Utilities** menu, and then on the Utilities page, select the **FMP Server Backup** tab.
2. Click **Upload & Restore**.

   The Upload & Restore FMP Server Information window appears.
3. Enter or choose the appropriate values for the following:
   - Select from
   - Archive File
   - MDSUM File
4. Click **Ok**.

   The Uploading FMP Server Information Backup window displays the status of the operation.
5. Click **Close** to exit.

   The FMP server information is uploaded and restored.

For more information on the various utilities provided by the ClearPath Forward Fabric Management Platform Manager, refer to the associated help.

14.2. Fabric Manager Backup

The Fabric Manager database and configuration files should be backed up after completing initial configuration and whenever the configuration is changed so that the server can be quickly restored in case of reinstallation or a catastrophic failure. Unisys also recommends that backups be taken at suitable intervals to capture any possible changes. These backups contain information about all the platforms and partitions in the fabric, and are critical to system operations.

To ensure that no ongoing updates cause integrity issues during the backup process, the backup utility automatically stops all Fabric Manager services, backs up the database and configuration files, and then starts all services when the backup is complete. To minimize the impact of stopping the Fabric Manager services, take the backups according to the site policy and schedule.

If you have two Fabric Management Platforms and they are configured as a high availability cluster, be sure to take the backup from the master node (that is, the Fabric Management Platform running the Fabric Manager services workload).

Depending on the configuration, backing up the Fabric Manager database and configuration files can take up to 10 minutes.

You can create and manage FFM database backups from the **FFM Backup** tab under **Utilities**.

Note: *The following Call Home security files are not included in the Fabric Manager database backup for security reasons:*

- */etc/ssl/certs/callhome.key*
- */etc/ssl/certs/ callhome.key.sig*

These files contain Call Home security information such as the user name and password that is used for connecting your ClearPath Forward Fabric to the Unisys Support Center. After restoring a Fabric Manager database backup, to enable the Call Home feature, you should either restore a backup of the Call Home security files or generate a new set of files.

14.2.1. Generating Fabric Manager Database Backup

You can create a new backup of the Fabric Manager database. The backup contains information about all the platforms and partitions in the fabric and are critical to the operations. It is recommended to take a Fabric Manager database backup every time the composition of your Forward fabric changes, such as commissioning or decommissioning partitions.

To generate a backup,

1. From the FMP Manager user interface, select the **Utilities** menu, and then on the Utilities page, select the **FFM Backup** tab.
2. Click **Generate BackUp**.

   A confirmation message appears.
3. Click **Yes**.

   The FFM Backup page displays the generated backup.

Note: *You can limit the number of backups. Once the limit is reached, the older backups are deleted to accommodate the new backups.*

For more information on the various utilities provided by the ClearPath Forward Fabric Management Platform Manager, refer to the associated help.

14.2.2. Restoring Fabric Manager Database Backup

You can restore a Fabric Manager database backup on the current node.

To restore a backup,

1. From the FMP Manager user interface, select the **Utilities** menu, and then on the **Utilities** page, select the **FFM Backup** tab.
2. Select the backup file that you want to restore.
3. Click **Restore**.

   A confirmation message appears.
4. Click **Yes**.

   The backup file is restored.

Note: *It is recommended to restore the Fabric Manager database backup on the master node.*

For more information on the various utilities provided by the ClearPath Forward Fabric Management Platform Manager, refer to the associated help.

14.3. Backing Up Application Operating Environments on Partitionable Enterprise Partition Platforms

You may use standard operating system or third party datacenter tools to back up the Windows or Linux operating environments that contain your applications according to your site policy.

The ClearPath Forward fabric does not support bare-metal restore of partition images. If the original partition image no longer exists, you commission a new partition image, and then recover the environment of the previous partition image onto the new partition image. When backing up your Windows or Linux operating environments, you do not need to back up the EFI system partition since it is automatically created when you commission a new partition image. For more information on backup and restore tools, see 14.5 Examples of Tools for Backing Up and Restoring Application Operating Environments.

Note: *The EFI system partition is a disk partition on the boot volume used by ClearPath Forward partition images and other machines that adhere to the Unified Extensible Firmware Interface (UEFI). It contains the boot loader, device drivers, system utilities, and other information specific to the current environment of the particular partition image.*

If you intend to restore your operating environment on a different partition image, be sure that you do not include the EFI system partition from the previous partition image (if it was backed up) as part of the restore process. It may contain invalid information for the new partition image.

Note: *If you previously made changes to files on the Linux /boot/efi partition of the original partition image (for example, operating system kernel changes, initrd and efi configuration file changes, or driver updates), you may need to reapply the changes to the new partition image after the restore process.*

14.4. Restoring Application Operating Environments on Enterprise Partition Platforms

The ClearPath Forward fabric does not support bare-metal restore of partitions. If the original partition no longer exists, you commission a new partition image, and then recover the environment of the previous partition into the new partition. When restoring your operating environment, ensure that you do not include the EFI system partition (if it was backed up) as part of the restore process. For more information on backup and restore tools, see 14.5 Examples of Tools for Backing Up and Restoring Application Operating Environments.

To restore the Windows or Linux operating environment containing your applications

1. Commission a new partition on the desired platform using the same blueprint that was used to create the original partition, or a similar blueprint.

   The new partition must be the same operating system type as the original partition, but may be different in size.

2. Use the backup image captured from the original partition to recover the saved operating system and application environment onto the new partition.

3. For the Linux operating environment, if you previously made changes to files on the Linux /boot/efi partition of the original partition image (for example, operating system kernel changes, initrd and efi configuration file changes, or driver updates), you may need to reapply the changes on the new partition image after the restore process.
4. Verify the network configuration for your restored partition:
   - If your partition participated in a secure fabric, manually reassociated the partition with the secure fabric. For more information on associating a partition after commissioning, refer to the *ClearPath Forward Administration and Operations Guide*.
   - If you restored your backup to a replacement partition image with a different platform number or partition number than the original partition, be sure to modify the IP addresses of the partition (on the FM LAN, the IP-LAN secure fabric, other secure fabrics, and so on) from what was captured during the backup to the current values used by Fabric Manager for the replacement partition image. Refer to the summary page of the partition in Fabric Manager for the IP addresses assigned to the partition image on the various LANs and secure fabrics. If your application environment has the old IP addresses configured within it, be sure to reconfigure so that your application can communicate properly with the new partition.
   - If the backup was restored to a different physical environment—for example, to a different physical platform or NIC port configuration—be sure to examine the operating system settings for all network interfaces, and, if necessary, reconfigure for the new environment.

14.5. Examples of Tools for Backing Up and Restoring Application Operating Environments

The EFI system partition on the boot volume of a partition image contains the boot loader, device drivers, system utilities, and other information specific to the current environment of the particular partition image, and may contain invalid information for a new partition image if included as part of the restore process. If the EFI system partition from a previous partition image is restored onto a new partition, the restore process may fail.

You may exclude the EFI system partition when backing up the application operating environment or when restoring the environment. Depending on your choice of backup and restore tool, the exact mechanism for excluding the EFI system partition varies. For example,

- Windows Server Backup

  For Windows Server 2008 R2 partition images, backup or restore the system state and disk volumes you want to restore.

  For Windows Server 2012 and Windows Server 2012 R2 partition images, be sure to back up the disk volumes you want to restore. You do not need to back up the system state separately. For more information on restoring, see 14.6 Restoring Windows Server 2012 or Windows Server 2012 R2 Using Windows Server Backup.

- SLES YaST System Backup

  Exclude /boot/efi in the set of files to be backed up.

- EMC NetWorker

  Before backing up a partition, create a directive to exclude **/boot/efi** for Linux, or **C:\Windows\boot** for Windows, and be sure to add the new directive while configuring client properties.

- Symantec Backup Exec

  Ensure the EFI system partition selection box is not selected when recovering a partition.

- Symantec NetBackup

  Ensure the EFI system partition selection box is not selected when recovering a partition.

14.6. Restoring Windows Server 2012 or Windows Server 2012 R2 Using Windows Server Backup

If you previously backed up a Windows Server 2012 or Windows Server 2012 R2 partition image using the Windows Server Backup application, and the partition image has been decommissioned, do the following to restore the backed up disk volumes onto a replacement partition image.

1. Ensure the backup file is available on the network.
2. Obtain the worksheet for commissioning for the original partition image.
3. Commission a replacement partition image with the same parameters used during commissioning of the original partition image, and configure its internal LUN to be the same as the original partition.

   For more information, see 14.6.1 Commissioning a Replacement Partition Image.
4. Boot the replacement partition image into recovery mode, and configure networking for accessing the backup files on the network.

   For more information, see 14.6.2 Booting Partition with Recovery Option and Configuring Networking.
5. Restore the backed up volumes to the internal LUN of the replacement partition image.

   For more information, see 14.6.3 Restoring Backed Up Volumes To Internal LUN.
6. Verify or set time and time zone for the replacement partition image.

   For more information, see 14.6.4 Verifying Time and Time Zone.
7. Boot into the restored partition image, and verify drive letter assignments.

   For more information, see 14.6.5 Booting the Restored Partition Image and Checking Drive Letter Assignments.

8. Reapply any previous changes made to the EFI system partition.

   For more information, see 14.6.6 Restoring Changes to the EFI System Partition.

9. If necessary, adjust the network configuration settings for the restored partition image.

   For more information, see 14.6.7 Verifying Network Configuration.

14.6.1. Commissioning a Replacement Partition Image

Referring to the commissioning worksheet for your original partition image, use the Fabric Manager user interface to commission a replacement partition image with as many of the parameters of the original partition as possible.

If you do not use the same platform and partition number as the original partition image, or if the backup is restored to a different physical environment than the original environment (for example, a different platform or NIC port configuration), you may have to adjust the network configuration settings in the Windows operating system after restoring the partition from your backup.

If you reconfigured the internal LUN on the original partition image after it was originally commissioned (for example, you changed the size of the C: volume, or created additional volumes), repeat any configuration before proceeding to the next step.

14.6.2. Booting Partition with Recovery Option and Configuring Networking

1. To monitor the boot progress during the next two steps, ensure you are viewing the partition desktop through a partition image console window.
2. From the partition desktop, restart the partition.
3. When the Windows Boot Manager screen displays, select the **Windows Recovery** option, and then press **Enter**.
4. On the Choose an Option screen, click **Troubleshoot**.

   The Advanced Options screen appears.
5. On the Advanced Options screen, click **Command Prompt**.
6. If prompted, select the administrator account, and enter the password that was specified when commissioning the replacement partition.

   A command prompt window appears.
7. Initiate the networking stack: At the command prompt, type the following command, and then press **Enter**.

   ```
   wpeutil initializenetwork
   ```
8. If the IP address for a network interface was not configured using DHCP, use the following command to configure for access to the backup file on the network:

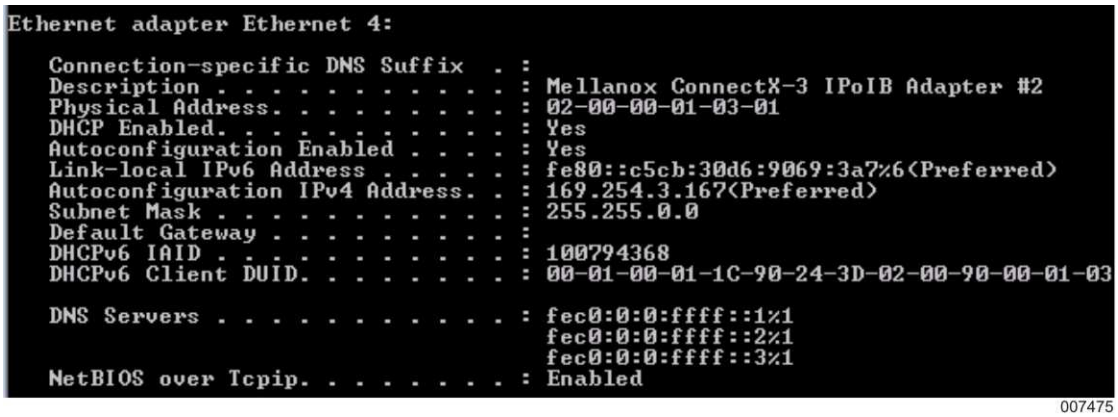
   ```
   netsh interface ip set address <interface name> static
   <IP address> <net mask> [<gateway>]
   ```

Note: *To list all network interfaces (adapters), use the following command:*

```
ipconfig /all
```

For example, in the following graphic, to set the IP address of the Ethernet adapter Ethernet 4 to 172.31.1.133 with an address mask of 255.255.255.0 and no gateway, type in the command

```
netsh interface ip set address "Ethernet 4" static 172.31.1.133 255.255.255.0
```



007475

14.6.3. Restoring Backed Up Volumes To Internal LUN

For each volume you want to restore onto the replacement partition image, use the **wbadmin start recovery** command to restore from the backup files:

```
wbadmin start recovery -ItemType:Volume -Items:<original drive letter>
-BackupTarget:<backup share> -Machine:<original machine name>
-Version:<date and time of backup> -RecoveryTarget:<new drive letter>
```

Note: *When prompted, enter appropriate credentials for accessing the backup files on the network.*

Example

```
wbadmin start recovery -ItemType:Volume -Items:C:
-BackupTarget:\\172.31.1.11\BackupShare -Machine:W12R2Test1
-Version:02/05/2015-21:17 -RecoveryTarget:C:
```

If you backed up volumes other than the C: volume, the drive letters in the recovery environment might be different from the letters under the Windows Server operating system. If that is the case, the –Items parameter specifies the letter at the time the backup was done, and the –RecoveryTarget parameter specifies the drive letter to which the volume should be restored in the Windows Recovery Environment (Windows RE). If needed, you can correct the volume letters later, after booting into the restored C: drive.

To identify the volumes currently associated with drive letters, do one of the following in the recovery environment:

- Run **mountvol** to list the currently mounted drive letters.
- Run **diskpart**, and then use the **list volume** command to list the current drive letters and corresponding volume sizes. To exit diskpart, type **exit**, and then press **Enter**.
- Use the **dir <drive letter>:** command to see the directory listings of the volumes.

14.6.4. Verifying Time and Time Zone

When the replacement partition image was commissioned, the time zone was set to UTC by default. If the partition image that is being restored used a different time zone, set the time zone so that it will be correct when you boot the restored partition.

The time zone is specified as a quoted string. Use the following command to list possible values for the time zone specification:

```
C:\Windows\System32\tzutil /l
```

To set the time zone to match the restored partition:

```
C:\Windows\System32\tzutil /s <time zone>
```

Example

```
C:\Windows\System32\tzutil /s "Pacific Standard Time"
```

Use the **time** and **date** commands to verify that the system clock is set correctly.

14.6.5. Booting the Restored Partition Image and Checking Drive Letter Assignments

1. In the command prompt window, type the following command at the command prompt to restart the system:

   ```
   wpeutil reboot
   ```

2. When the Windows Boot Manager screen displays in the partition image console window, select the Windows operating system, and then press **Enter**.
3. From the desktop of the partition, click **Server Manager**, expand the **Storage** node if needed, and then click **Disk Management**.
4. Verify that the drive (volume) letter assignments are correct. Modify the assignments if needed.

14.6.6. Restoring Changes to the EFI System Partition

The state of the EFI system partition at this point is the initial configuration created during commissioning. Typically, you should not make any changes to the EFI system partition. However, you may have been previously directed by your service representative to copy certain files to the original partition image. If you made changes to EFI system partition of the original partition image, reapply those changes to the replacement partition image.

14.6.7. Verifying Network Configuration

If you restored your backup to a replacement partition image with a different platform number or partition number than the original partition, be sure to modify the IP addresses of the partition (on the FM LAN, the IP-LAN secure fabric, other secure fabrics, and so on) from what was captured during the backup to the current values used by the Fabric Manager for the replacement partition image. Refer to the summary page of the partition in the Fabric Manager user interface for the IP addresses assigned to the partition image on the various LANs and secure fabrics. If your application environment has the old IP addresses configured within it, be sure to reconfigure so that your application can communicate properly with the new partition.

If the backup was restored to a different physical environment—for example, to a different physical platform or NIC port configuration—be sure to examine the operating system settings for all network interfaces, and, if necessary, reconfigure for the new environment.

14.7. Using the Rescue Environment to Back Up, Repair, and Restore a Linux Partition on an Internal Drive

Note: *This section provides information for a Linux administrator so that he or she can apply his skills in the ClearPath Forward environment; it is not intended to be a guide for repairing or restoring Linux environments.*

Occasionally a Linux boot LUN (disk) may be corrupted to the point where it fails to boot.

If the LUN is on an external disk drive, such as a storage array on the storage area network (SAN), you may be able to repair it by mounting it under a different partition, or use storage array tools to restore a correct image onto the LUN from a backup source.

If the LUN is on the internal disk of the enterprise partition platform (EPP), you can refer to the following topics for some options for repairing or restoring the boot disk.

- 14.7.1 Starting a Linux Partition Image in Rescue Mode
- 14.7.2 Accessing the Linux Partition Boot Disk in the Rescue Environment
- 14.7.3 Configuring the Network Adapter in the Rescue Environment
- 14.7.4 Backing Up the Linux Partition Boot Disk in the Rescue Environment
- 14.7.5 Restoring the Linux Partition Boot Disk While in the Rescue Environment
- 14.7.6 Adjusting Settings for a Restored Linux Partition

14.7.1. Starting a Linux Partition Image in Rescue Mode

If your Linux system on a partition image has become non-bootable or is suffering from critical system errors, you can use Rescue Mode option to recover your system data.

The Fabric Manager provides an option to start the Linux partition image in rescue mode so that you can access the Linux partition from the outside in the event of an emergency. You can use the Rescue Mode to troubleshoot and repair the Linux partition image that has become non-bootable or is suffering from critical errors.

Prerequisites:

- The desired partition image is in stopped state.

  If the partition image is not in stopped state and not responding to the Soft Shutdown option, then point to Advanced and click Force Halt.
- The partition image should be running a Linux operating system supported by ClearPath Forward. For example, RHEL x.x or SLES x.x.
- The platform on which the partition image resides should have the supporting image LinEZInstall 1.1.00016 or higher.

To start the Linux partition image in rescue mode

1. On the Fabric Manager user interface, point to **System Administration**, and then click **CPF System**.
2. Click **Platforms and Partitions**.

   The **Details: Platforms and Partitions** screen appears.
3. Click **Partitions** tab.

   The list of partition images appears.
4. Double-click the partition image that you want to start in rescue mode.

   The **Summary** tab displays the information about the selected partition image.
5. Point to **Advanced** and click **Start – Rescue Mode**.

   A message alerting you that this action should be performed only on a Linux partition image and the platform with at least LinEZInstall 1.1.0.0016, or newer.
6. Click **Yes**.

   The Linux partition image starts in the rescue mode. In the rescue mode, using the standard Linux commands, you can troubleshoot and repair your Linux system. After troubleshooting, reboot the partition image. The partition image will attempt to boot back into the installed operating system.

14.7.2. Accessing the Linux Partition Boot Disk in the Rescue Environment

To boot the partition into the Linux rescue environment, refer to 14.7.1 Starting a Linux Partition Image in Rescue Mode.

In the rescue environment, the partition boot disk is accessible via /dev/sda. Use the following command to list the partitions:

```
parted /dev/sda p
```

You can make repairs to the boot disk by mounting the required partition, and then create or modify files. For example, if the bootloader was damaged, you can mount the boot partition, and then copy a good bootloader to it.

If you need access to the network to read files from another machine or partition, refer to 14.7.3 Configuring the Network Adapter in the Rescue Environment.

14.7.3. Configuring the Network Adapter in the Rescue Environment

To boot the partition into the Linux rescue environment, refer to 14.7.1 Starting a Linux Partition Image in Rescue Mode.

After booting into the rescue environment, you can configure a network adapter that is connected to the machine or partition containing the backup file. The names of the network adapters are in the **/sys/class/net** directory and can be viewed using the following command:

```
ls /sys/class/net
```

The PCI adapters have names in the form **ens*<adapter number>*f*<port number>***. For example, ens1f0.

If there is a DHCP server on the network, and you want it to configure the network adapter automatically, use the following command to start the DHCP client on the partition

```
dhclient
```

If you want to manually configure the adapter and routing, use the **ipconfig** and **route** commands:

```
ifconfig <adapter name> <IP address>/<network prefix length>
route add default gw <gateway address>
```

For example,

```
ifconfig ens1f0 122.59.240.21/24
route add default gw 122.59.240.250
```

14.7.4. Backing Up the Linux Partition Boot Disk in the Rescue Environment

When the rescue environment, you can make an offline backup of the entire boot disk, or of some of the partitions on it. This backup file can then be used to restore a partition whose boot disk has become corrupted to the point where it will not boot and is too badly corrupted to repair by manipulation of the file systems from the rescue environment. The backup and restore process takes advantage of the fact that the rescue environment is not stored on the partition boot disk, but instead runs in RAM and thus does not depend on any files on the boot disk.

The following tools are available in the *<path>* of the rescue environment:

- **dd** – Sector level backup or restore
- **fsarchiver** – File system level backup or restore
- **tar** – File level backup or restore
- **cpio** – File level backup or restore
- **zip** – pkzip compressor
- **gzip** – gzip compressor (typically the fastest)
- **pigz** – Multithreaded gzip compressor
- **bzip2** – bzip2 compressor
- **xz** – xz compressor (typically the smallest file size)
- **pixz** – Multithreaded xz compressor (similar to xz -T0)

If you prefer a tool that not present, install the tool of your choice.

Example

A simple example for making a full backup of the boot disk:

1. Boot the partition into the Linux rescue environment and access the partition boot disk.

   For more information, see 14.7.1 Starting a Linux Partition Image in Rescue Mode and 14.7.2 Accessing the Linux Partition Boot Disk in the Rescue Environment.

2. Configure the rescue environment for accessing the network to read or write files.

   For more information, see 14.7.3 Configuring the Network Adapter in the Rescue Environment.

3. Mount the remote directory to which you want to write the backup file. For example, to mount a Windows share named BackupShare located at 192.59.240.12, use the following command:

   ```
   mount //192.59.240.12/BackupShare /mnt –o user=foo,domain=bar
   ```

   Or to mount an exported NFS directory named BackupExport located at 192.59.240.18, use the following command:

   ```
   mount.nfs 192.59.240.18:/BackupExport /mnt
   ```

4. Write the contents of the boot disk to the remote directory:

   ```
   dd if=/dev/sda | xz –czT 0 > /mnt/backup-1.xz
   ```

14.7.5. Restoring the Linux Partition Boot Disk While in the Rescue Environment

Use the appropriate tool to restore from your backup file. The following tools are available in the *<path>* of the rescue environment:

- **dd** – Sector level backup or restore
- **fsarchiver** – File system level backup or restore
- **tar** – File level backup or restore
- **cpio** – File level backup or restore
- **zip** – pkzip compressor
- **gzip** – gzip compressor (typically the fastest)
- **pigz** – Multithreaded gzip compressor
- **bzip2** – bzip2 compressor
- **xz** – xz compressor (typically the smallest file size)
- **pixz** – Multithreaded xz compressor (similar to xz -T0)

If you prefer a tool that is not present, install the tool of your choice.

Example

To restore from a backup file made using the full disk backup example in 14.7.4 Backing Up the Linux Partition Boot Disk in the Rescue Environment:

1. Boot the partition into the Linux rescue environment and access the partition boot disk.

   For more information, see 14.7.1 Starting a Linux Partition Image in Rescue Mode and 14.7.2 Accessing the Linux Partition Boot Disk in the Rescue Environment.

2. Configure the rescue environment for accessing the network to read or write files.

   For more information, see 14.7.3 Configuring the Network Adapter in the Rescue Environment.

3. Mount the remote directory where the backup file is located. For example, to mount a Windows share named BackupShare located at 192.59.240.12, use the following command:

   ```
   mount //192.59.240.12/BackupShare /mnt –o user=foo,domain=bar
   ```

   Or to mount an exported NFS directory named BackupExport located at 192.59.240.18, use the following command:

   ```
   mount.nfs 192.59.240.18:/BackupExport /mnt
   ```

4. Write the contents of the backup file to the boot disk:

   ```
   xz -dc /mnt/backup-1.xz | dd of=/dev/sda
   ```

Note: *In this example, the disk's GPT PartitionGUID is overwritten by the restore process. If you restored a backup taken from a different partition, the EFI boot option stored in NVRAM will not refer to the correct disk. To rectify, you need to clear the EFI boot options so that s-Par rebuilds the boot options to reference the new disk's GUID.*

The rescue environment includes a script to erase all the boot options; to run it, enter the following command:

```
wipe-efi-boot
```

Proceed to 14.7.6 Adjusting Settings for a Restored Linux Partition to configure or verify settings.

14.7.6. Adjusting Settings for a Restored Linux Partition

If you restored a backup file to a different partition than the one that was backed up, the time may be incorrect. Use the **date** command to verify the setting, and to correct if necessary.

If you restored your backup to a replacement partition image with a different platform number or partition number than the original partition, be sure to modify the IP addresses of the partition (on the FM LAN, the IP-LAN secure fabric, other secure fabrics, and so on) from what was captured during the backup to the current values used by the Fabric Manager for the replacement partition image. Refer to the summary page of the partition in the Fabric Manager user interface for the IP addresses assigned to the partition image on the various LANs and secure fabrics. If your application environment has the old IP addresses configured within it, be sure to reconfigure so that your application can communicate properly with the new partition.

If the backup was restored to a different physical environment—for example, to a different physical platform or NIC port configuration—be sure to examine the operating system settings for all network interfaces, and, if necessary, reconfigure for the new environment.

Changes described in this section are probably most easily made using the tools in your partition operating system; however, if you are familiar with how to make these changes in the network initialization scripts on the partition operating system disks, you can make these changes before booting to the partition operating system to avoid possible network conflicts resulting from booting the partition operating system with old configuration information.

When you complete restoring and adjusting settings for the partition, use the Fabric Manager user interface to reboot the partition.

Section 15
Handling Events

An event is any activity that takes place in the fabric that is of sufficient importance that it is stored in the event log. Events are the system's way of informing you of what is happening. They may be vitally important, or they may not be important at all. The Fabric Manager identifies the event's criticality, for example, Critical, Warning, Informational, and so on.

This section describes the typical way in which you will want to handle events. However, the system includes more functionality than is described here. For complete information, such as how to filter events, re-open events, and edit the event log retention period, see the *ClearPath Forward Administration and Operations Guide*.

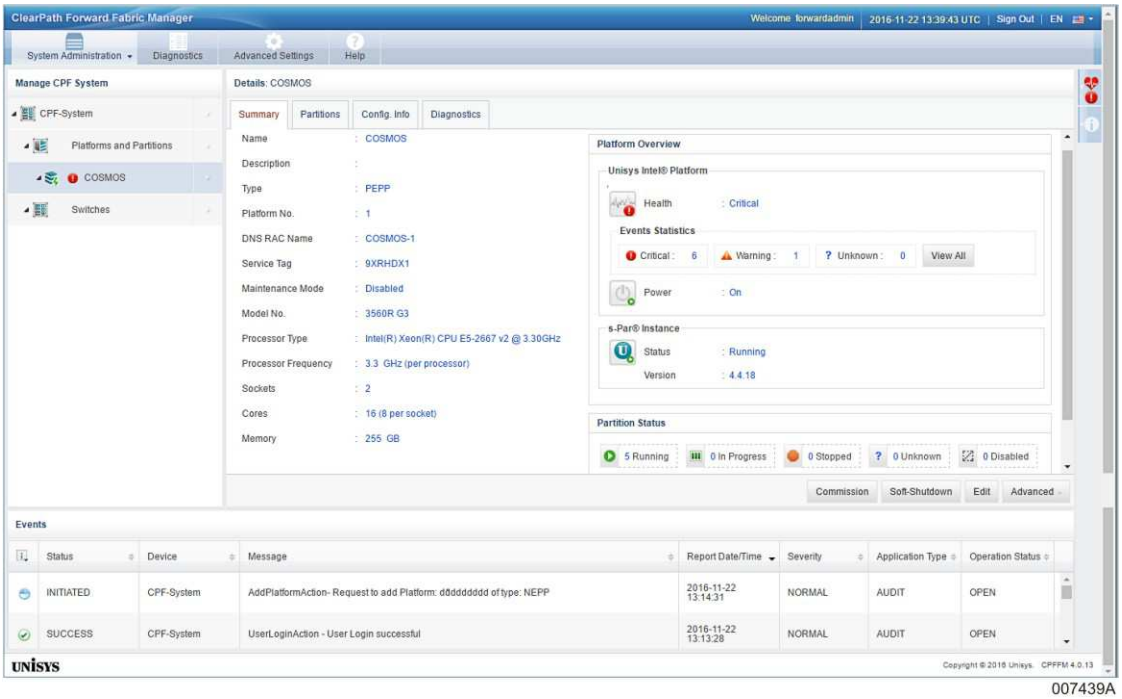
15.1. The Event Log

The Fabric Manager maintains a single consolidated event log for all events occurring in all platforms and partitions in the fabric. By default, events are retained for 90 days. You can set the event log retention period for anywhere from 30 to 180 days.

15.2. How Events Are Made Known to You

Rolling Event Log

Many Fabric Manager screens include a frame at the bottom that displays events in real-time as they occur. For example, in the following screen, the platform COSMOS is highlighted; a portion of the rolling event log appears at the bottom. Scrolling down shows the rest of the frame.



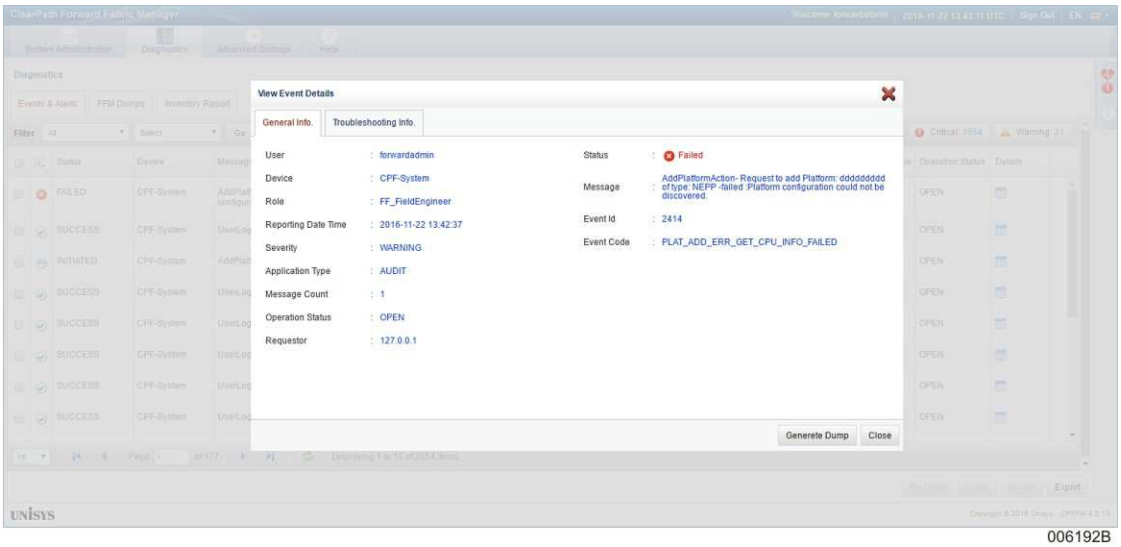
007439A

As more events occur, older ones scroll upward and thus may no longer be visible. However, they remain in the event log for the duration of the event log retention period.

Event Console

You can get full details about events by clicking **Diagnostics** on the Fabric Manager user interface or selecting the **Diagnostics** tab, and then selecting the **Events & Alerts** tab on the Diagnostics page.

For specific information about a particular event, locate the event on the **Events & Alerts** tab on the Diagnostics page, and then click the  icon in the **Details** column. In the following example, the user has called up the Event Console, and clicked the **Details** icon for the first event, which happens to be a failed event. This causes general information about the event to be displayed in the **View Event Details** pop up window. Because the event is a failed event, the **View Event Details** window also displays the **Troubleshooting Info.** tab that displays the possible reasons that might have caused the failure, as well as probable solutions for fixing the failure.



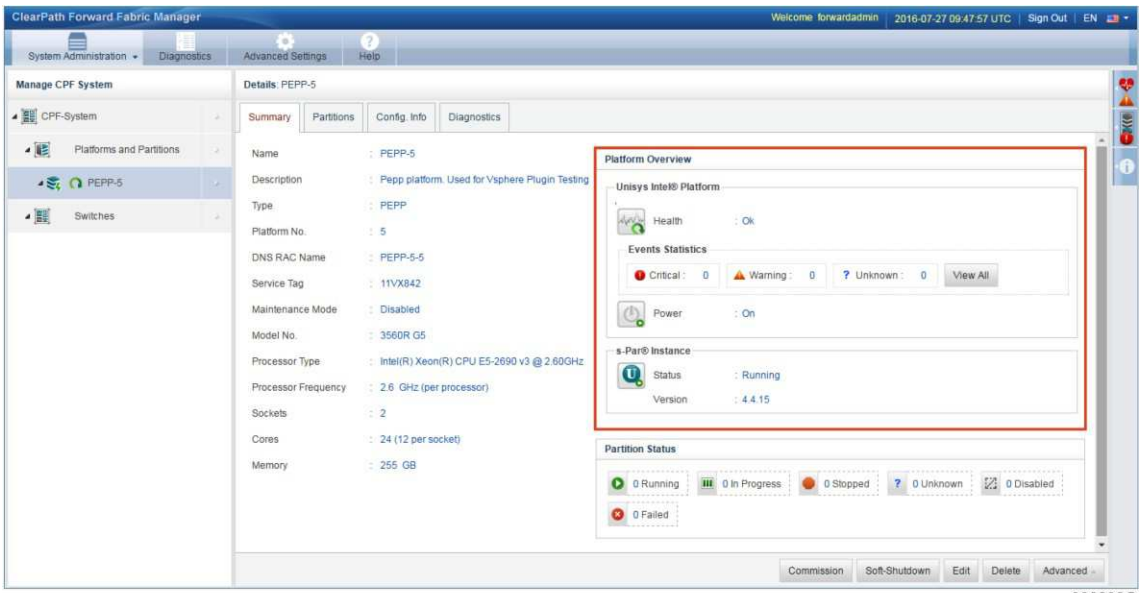
006192B

For complete information on the **Events & Alerts** tab, refer to the ClearPath Forward *Administration and Operations Guide*.

Event Status and Status Icons

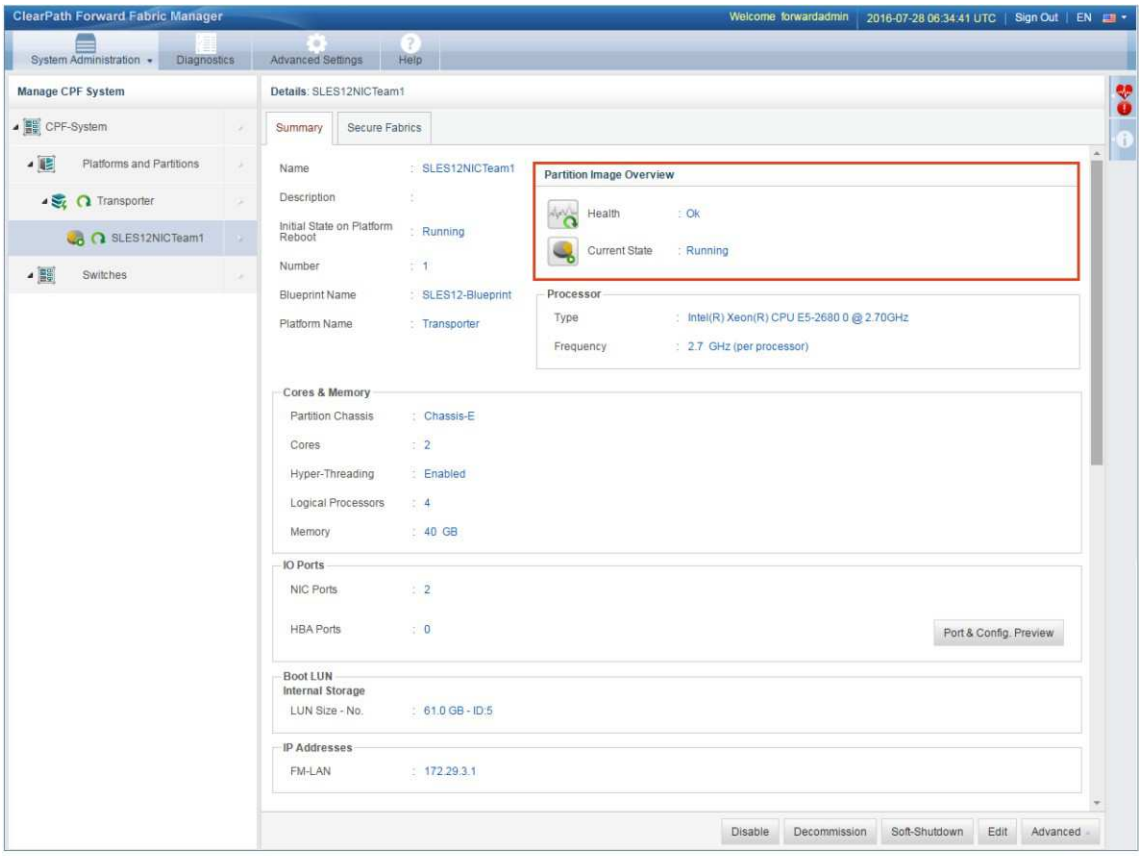
Events in the rolling event log might scroll off the screen before you notice them; and the Event Console is not visible unless you click the **Events** tab. The Fabric Manager draws your attention to some events by using status icons. Many events are not important enough to warrant alerting you via status icons, for example, events with a Status of Ok, Success, Initiated, or Informational.

However, events with a Status of Critical, Warning, or Failed result in a change to the status icons displayed in the Platform Summary display or Partition Summary display (depending on which of the two the event applies to). The following screen example shows the location of the icon in the Platform Summary.



006202G

The following screen example shows the location of the icon in the Partition Summary.



006203G

15.3. How to Handle Events

The recommended procedure for handling events is as follows.

1. You become aware of the event, either via the rolling event log or status icons.
2. Access the Event Console (by clicking the **Events** tab at the top of the Fabric Manger user interface) and find the event that you are interested in.
3. Select the event by clicking anywhere on the row containing the event. Examine the information about the event given in the **Event Details** region.
4. If the Status of the event is OK, Running, Success, Initiated, or Informational, you can safely close the event. (An event with a Status of Stopped can usually also be safely closed.) Closing an event removes it from the Event Console display. However, the event remains in the event log for the duration of the event log retention period.

   Procedure:

   a. Select the event by clicking on the event row.

   b. Click the **Close** button appearing between the list of events and the **Event Details** region.

No more handling of the event is necessary.

However, if the Status of the event is Critical, Unknown, Warning, or Failed (or in some cases Stopped), proceed to the next step.

5. If the Severity of the event is Critical, Unknown, Warning, or Failed (or in some cases Stopped), proceed as follows:

   a. Inform the Fabric Manager that you are aware of the event by accepting the event.

      Procedure:

      - Select the event by clicking on the event row.
      - Click the **Accept** button appearing between the list of events and the **Event Details** region.

      Note that accepting the event does nothing to solve the problem (or non-problem) represented by the event. It merely informs the Fabric Manager that you are aware of the event and intend to do something about it. However, as a result of accepting the event, the Fabric Manager does change status icons back to a normal state.

   b. Solve the problem represented by the event. That is, take whatever corrective action is required.

   c. Inform the Fabric Manager that you have corrected the problem by closing the event.

      Procedure:

      - Select the event by clicking on the event row.
      - Click the **Close** button appearing between the list of events and the **Event Details** region.

      No more handling of the event is necessary.

If you close an event without actually correcting the problem

- The Fabric Manager might prevent you from taking certain actions. For example, it may continue to not monitor a given partition.
- The Fabric Manager issues the event again.

Appendix A
Worksheet for Commissioning

During catastrophic failures, you might lose the partition parameters that you entered while commissioning the partition image and you might not be able to reconstruct the partition environment.

Unisys recommends you to take a printout of worksheet, and manually fill the parameters before setting up the partition environment as part of your planning. As you commission a partition image, make notes or corrections on the worksheet. Store the hard copy in a safe place (and/or scan it and store it on a separate device) as part of a disaster recovery plan.

Table A–1. Worksheet for commissioning

Platform Number:		
Platform Name:		
Tab	**Write the selected parameter details**	**Example**
Blueprint		
Blueprint		V2V-5-GoldImage
Partition Attributes		
Partition Image Name		Partition1
Host Computer		Partition1
Initial State on Platform Reboot		Running
Description		Partition image for finance databases
Cores & Memory		
Partition Chassis		Chassis -B
Cores		2
Enable Hyper-Threading (HT)		Unchecked
Memory		8GB
I/O Ports		
Ports		
NIC Ports		Port A, Slot 2

Table A–1. Worksheet for commissioning (cont.)

HBA Ports		Port 1, Slot 3
Secure Fabric		
Select Secure Fabric		IP-LAN
Storage		
Internal Storage		
LUN Selection		20 GB
External Storage		Selected
Target WWPN		11:22:33:44:AB:CD:EF:AD
Target LUN No.		15
Primary Boot Path		Slot 5 – Port 2

Appendix B
Transferring Files Between Linux and Windows

There may be occasions when you want to transfer files between the Fabric Management Platform (FMP) and external environments. Following are the common file transfer scenarios that you might come across:

- Routine transfer of files such as blueprints, images, and dumps between the ClearPath Forward and external environments using the Fabric Manager user interface.
- Transferring non-routine files between the FMP, which runs Linux operating system, and the external Windows systems.

This section discusses various methods that enables you to transfer files between the Linux and Windows systems in the following sections:

Note: *If the Windows system is running on VMware environment, see https://kb.vmware.com/kb/1918 to know more about transferring files to or from an ESXi host.*

B.1. Transferring Files through the Network Using a Windows Share

The FMP has the capability to mount a Windows share and hence it can support file transfer in both the directions.

Perform the following operations on the FMP to mount a Windows share on it:

1. Create a directory using the following command:

   ```
   mkdir <mountdir>
   ```

   where, <mountdir> is the name of the directory that you want to create.

2. Mount a Windows share on the directory using the following command:

```
mount //<sharehost>/<share> <mountdir> -o user=<account>,domain=<domain>
```

where,

- <sharehost> is the name or IP address of the Windows host on which the share is located
- <share> is the name of the share on the Windows system
- <account> is the name of the user account that has access to the Windows share. If the user account is a domain account, then specify the name of the domain, else, provide only the user name.
- <domain> is the name of the domain to which <account> belongs to. If the <account> account is an account on <sharehost> and not a domain account, then do not include ",domain=<domain>"

Notes:

- *Use forward slash (/). This is in contrast to Windows naming convention where backward slash (\ ) is used.*
- *Do not use space next to a comma (,) or an equal (=) sign.*

For example,

```
mount //192.169.12.2/WinShare /anydir –o user=Administrator,domain=corp
```

When you run this command, you will be prompted to enter the password associated with the specified user account.

3. View the content of the Windows share using the following command:

   ```
   ls <mountdir>
   ```

4. Copy files between the Windows share and Linux using the following commands:

   - To copy files from Linux to the Windows share use the command

     ```
     cp <source> <destination>
     ```

     For example, after mounting a Windows share on the /MyMount directory, use the following command to copy a file named FileA from the current directory to the share.

     ```
     cp FileA  /MyMount
     ```

   - To copy files from the Windows share to Linux, use the command

     ```
     cp <source> <destination>
     ```

     For example, use the following command to copy a file named FileB from the Window share mounted on /MyMount to the current directory on a Linux system.

     ```
     cp /MyMount/FileB
     ```

5. After copying the files, unmount the Windows share using the following command:

   ```
   umount <mountdir>
   ```

   where, <mountdir> is the name of the directory on which the share is mounted.

B.2. Transferring Files through the Network Using SSH

The Secure Socket Shell (SSH) daemon runs by default on the FMP. Hence, it can be used to transfer files to or from an external Windows system, provided that an SSH client is installed on the Windows system.

The Windows operating system does not support SSH. However there are many SSH client software with user friendly graphical user interface that are available for free. For example, FileZilla from filezilla-project.org and WinSCP from winscp.net are some of the popular SSH client software. You can download and install any one of the free SSH client software on the Windows system, and then transfer the files by referring to the documentation associated with the SSH client software.

Note: *The FMP supports SFTP and SCP on port 22.*

B.3. Exchanging Files Using a USB Drive

You can transfer files between the FMP and Windows system using an USB drive.

Prerequisites:

- Physical access to the system cabinet for the administrator or the Unisys representative.
- USB drives that are formatted for FAT or FAT32 file systems.

Transferring files using an USB drive involves the following tasks:

1. B.3.1 Mounting the USB Drive
2. B.3.2 Mounting a Partition on a Directory
3. B.3.3 Copying Files

B.3.1. Mounting the USB Drive

Perform the following procedure to mount the USB drive:

1. Insert the USB drive into the USB port on the FMP and run the following command:

   ```
   dmesg | tail
   ```

   A message is displayed similar to the following:

```
sd 5:0:0:0: [sdb] Write cache: disabled, read cache: enabled sdb: sdb1
   sd 5:0:0:0: [sdb] Attached SCSI removable disk
```

   where, sbd is the drive designation of the USB drive.

2. Verify that the USB drive is displayed in the list of drives using the following command:

   ```
   ls /dev/sd*
   ```

The USB drive is displayed as /dev/sdb and the partitions on the USB drive are displayed as /dev/sdb*n*

where, *n* is the partition number. Typically there will be one partition numbered as 1.

B.3.2. Mounting a Partition on a Directory

Before using a partition that is on the USB drive, you must mount it on a directory. You can use the /mnt directory for this purpose. If the /mnt directory is already being used and not available, then you should create a new directory.

Use the following commands to create a new directory and then to mount partition 1 of the sdb on it:

```
mkdir <mountdir>
mount /dev/sdb1 <mountdir>
```

where, <mountdir> is the name of the directory that you want to create and on which you want to mount the partition.

After the drive is mounted on the directory, you can view it using the following command:

```
ls <mountdir>
```

B.3.3. Copying Files

To copy the files from the USB drive to the FMP or from the FMP to the USB drive use the following command:

```
cp <source> <destination>
```

Examples:

- To copy a file named **FileA** from the current directory on the FMP to the USB drive partition mounted on the /MyMount directory, use the following command:

  ```
  cp FileA /MyMount
  ```

- To copy a file named **FileB** from the USB drive partition mounted on the /MyMount directory to the current directory, use the following command:

  ```
  cp /MyMount/FileB .
  ```

Note: *Before removing the USB drive from the port, you should unmount it using the following command:*

```
umount <mountdir>
```

where, <mountdir> is the name of the directory on which the USB partition is mounted.

B.4. Transferring Files Using a DVD

Prerequisite: Physical access to the system cabinet for the administrator or the Unisys representative

To transfer files from a DVD to the FMP,

1. Insert the DVD in the FMP.

   If the X graphical environment is running on your FMP, then it automatically mounts the DVD as /media/<disk label>, where, <disk label> is the name of the DVD.

   If the X graphical environment is not running on your FMP, then do the following:

   a. Create a directory using the following command:

      ```
      mkdir <mountdir>
      ```

      where, <mountdir> is the name of the directory that you want to create.

   b. Mount the DVD on the directory using the following command:

      ```
      mount /dev/sr0 <mountdir>
      ```

      Note: *<mountdir> is the directory on which the DVD is mounted. If the X graphical environment is running on your FMP, then <mountdir> is /media/<disk label>. If the X graphical environment is not running, then <mountdir> is the directory that you create using the mkdir command.*

2. List the contents of the DVD using the following command:

   ```
   ls <mountdir>
   ```

3. Copy a file from the DVD using the following command:

   ```
   cp <mountdir>/<myfile> .
   ```

4. After copying a file from the DVD, unmount the DVD using the following command:

   ```
   umount /<mountdir>
   ```

8231 0913-005