NO WARRANTIES OF ANY NATURE ARE EXTENDED BY THIS DOCUMENT. Any product or related information described herein is only furnished pursuant and subject to the terms and conditions of a duly executed agreement to purchase or lease equipment or to license software. The only warranties made by Unisys, if any, with respect to the products described in this document are set forth in such agreement. Unisys cannot accept any financial or other responsibility that may be the result of your use of the information in this document or software material, including direct, special, or consequential damages.

You should be very careful to ensure that the use of this information and/or software material complies with the laws, rules, and regulations of the jurisdictions with respect to which it is used.

The information contained herein is subject to change without notice. Revisions may be issued to advise of such changes and/or additions.

Notice to U.S. Government End Users: This is commercial computer software or hardware documentation developed at private expense. Use, reproduction, or disclosure by the Government is subject to the terms of Unisys standard commercial license for the products, and where applicable, the restricted/limited rights provisions of the contract data rights clauses.
Contents

Section 1. Introduction
1.1. Documentation Updates .............................................. 1–1
1.2. What’s New? ......................................................... 1–1
1.3. Audience ............................................................ 1–3
1.4. Purpose .............................................................. 1–3
1.5. Media and Documentation .......................................... 1–3

Section 2. Fabric Architecture
2.1. Summary of the Fabric Architecture ......................... 2–1

Section 3. Planning Your Fabric Implementation
3.1. Partition Planning .................................................. 3–1
3.1.1. Overview of Commissioning a Partition .................. 3–1
3.1.2. Overview of Partition Planning ............................... 3–3
3.1.3. Partition Sizes .................................................. 3–7
3.1.4. Partition Chassis ................................................. 3–8
3.1.5. How the Fabric Manager Guides Partition Design ...... 3–11
3.1.6. How to Choose Partition Sizes and Chassis .......... 3–13
3.1.7. Sizes and Chassis for a 2-Socket, 8-Core EPP .... 3–18
3.1.8. Sizes and Chassis for a 2-Socket, 10-Core EPP ....... 3–19
3.1.9. Sizes and Chassis for a 4-Socket, 12-Core EPP ....... 3–21
3.1.10. Sizes and Chassis for a 4-Socket, 15-Core EPP ...... 3–23
3.2. Planning a Partitionable EPP’s Storage ................. 3–25
3.2.1. Internal and External Data Storage ..................... 3–26
3.2.2. Virtual Disks (LUNs) for Internal Storage ............. 3–27
3.2.3. RAID Configurations and RAID Groups ............... 3–28
3.2.4. Allocating Internal Storage Among Partitions .......... 3–30
3.3. Operating System Licensing .................................. 3–30
3.4. Customer Responsibilities for Operating Environments ... 3–33
3.5. Customer-Supplied Hardware ................................ 3–34

Section 4. Getting Started with User Interface
4.1. Forward! Fabric Manager User Interface .................. 4–1
4.1.1. Understanding the Forward! Fabric Manager User Interface ........................................ 4-2
4.1.2. Signing into Forward! Fabric Manager User Interface ........................................ 4-3
4.1.3. Selecting Preferred Language in Fabric Manager User Interface ............................... 4-4
4.1.4. Understanding the Info Pane .................................................................................. 4-5
4.2. Viewing Software Update Information ......................................................................... 4-6
4.3. Forward! Fabric Management Platform (FMP) ............................................................ 4-7
4.3.1. Signing into Forward! Fabric Management Platform ............................................... 4-7
4.3.2. Changing User Password ...................................................................................... 4-7
4.3.3. Viewing Forward! Fabric Manager Server Health .................................................... 4-8
4.3.4. Viewing Fabric Manager High Availability Status .................................................... 4-9

Section 5. Completing Initial Installation and Configuration

5.1. Cabling the Forward! Fabric Management Platform to Your Network ........................... 5-1
5.2. Cabling Enterprise Partition Platforms to Your Network ............................................. 5-2
5.2.1. Mapping HBA and NIC Ports in OS to Physical Ports ............................................ 5-5
5.3. Installing Operating Systems for Windows and Linux Partitions .................................. 5-6
5.4. Updating the Forward! Fabric Manager Certificate ..................................................... 5-6
5.5. Commissioning a Partition Image .............................................................................. 5-7
5.6. Starting a Partition Image ......................................................................................... 5-12
5.7. Implementing Security Best Practices ........................................................................ 5-12
5.8. Backing Up Your Configuration ................................................................................. 5-12

Section 6. Installing and Configuring Operating Systems

6.1.1. Completing Windows OS Installation ....................................................................... 6-2
6.1.2. Changing Credentials for Default Windows Administrator Account .......................... 6-2
6.1.3. Configuring Your Windows Boot Disk ..................................................................... 6-2
6.1.4. Configuring Customer Corporate LAN (Public LAN) Connections for Enterprise Partition Platforms ........................................... 6-3
6.1.5. Configuring Storage Area Network Connections for Enterprise Partition Platforms ................................................................. 6-3
6.1.6. Completing Windows Configuration ......................................................................... 6-4
6.2. Completing Installation and Configuration of a Unisys-supplied Linux Partition Image ........................................................... 6-4
6.2.1. Completing Linux OS Installation ............................................................................ 6-4
6.2.2. Configuring Customer Corporate LAN (Public LAN) Connections for Enterprise Partition Platforms ............................................. 6-5
## Contents

6.2.3. Configuring Storage Area Network Connections for Enterprise Partition Platforms .......................... 6–5
6.2.4. Completing Linux Configuration .............................................. 6–6
6.3. Installing a Customer-Supplied Windows or Linux OS on a Partitionable Enterprise Partition Platform ........ 6–6

6.3.1. Customer-Supplied Windows or Linux Operating System Images on Partitionable Enterprise Partition Platforms .............................................. 6–6
6.3.2. Understanding Customer-Supplied Windows Operating System Images .............................................. 6–7
6.3.3. Understanding Customer-Supplied Linux Operating System Images .............................................. 6–8
6.3.4. Creating a Customer-Supplied Windows Operating System Image .............................................. 6–9
6.3.5. Creating a Customer-Supplied Linux Operating System Image .............................................. 6–10
6.3.6. Uploading Customer-Supplied Operating System Images to Fabric Manager .............................................. 6–15

6.4. Installing a Customer-Supplied OS on a Non-Partitionable Enterprise Partition Platform ......................... 6–16

6.4.1. Obtaining and Installing Drivers and Firmware .............................................. 6–16
6.4.2. Making Operating System Installation Media Image Available for Installation .............................................. 6–17
6.4.3. Installing and Configuring Windows Server ....................... 6–18

Installing Windows Server .............................................. 6–18
Installing and Configuring Intel PROSet and NIC Network Adapters .............................................. 6–21
Installing and Configuring Mellanox InfiniBand Adapters .............................................. 6–22
Configuring the Windows Firewall .............................................. 6–23
Configuring NMI Memory Dumps for Windows Server 2008 R2 .............................................. 6–24

6.4.4. Installing and Configuring SUSE LINUX 11 Service Pack 3 .............................................. 6–24

Installing SUSE LINUX 11 Service Pack 3 .............................................. 6–24
Configuring SUSE LINUX Kernel Crash Dumps .............................................. 6–28
Configuring the IP LAN (InfiniBand) Connection for SUSE LINUX .............................................. 6–28
Configuring the FM LAN Connection for SUSE LINUX .............................................. 6–29
Updating the UDEV Persistent Rules for SUSE LINUX .............................................. 6–30
Configuring OS Support of NMI Generated Kdumps for SUSE LINUX .............................................. 6–30

6.4.5. Installing and Configuring Red Hat Enterprise Linux .............................................. 6–31

Installing Red Hat Enterprise Linux .............................................. 6–31
Configuring Red Hat Linux Kernel Crash Dumps .............................................. 6–33
Configuring the IP LAN (InfiniBand) Connection for Red Hat Linux ........................................... 6–34
Configuring the FM LAN Connection for Red Hat Linux ......................................................... 6–35
Updating the UDEV Persistent Rules for Red Hat LINUX ....................................................... 6–36
Configuring OS Support of NMI Generated Kdumps for Red Hat LINUX ............................... 6–36

6.5. Configuring Partition Images to Boot From an External Storage Device ................................. 6–37

6.5.1. Booting from Internal or External Storage ................................................................. 6–37

6.5.2. Configuring Windows Partition Image to Boot From External Storage Device ................. 6–38

6.5.3. Configuring Linux Partition Image to Boot From External Storage Device .................. 6–66

6.6. Configuring and Maintaining Operating Environments on Enterprise Partition Platforms ......................................................... 6–71

6.7. Obtaining and Installing Interim Corrections (ICs) ............................................................ 6–71

Section 7. Administering Users

7.1. Role-based Access Control ................................................................. 7–1

7.2. Understanding User Roles ................................................................. 7–2

7.3. Creating a User .................................................................................. 7–4

7.4. Setting-Up User Password ................................................................. 7–5

7.5. Assigning a User Role ....................................................................... 7–6

7.6. Assigning Permissions to a Role ........................................................ 7–6

7.7. Adding Organizations ....................................................................... 7–7

7.8. Assigning Organizations to Users ....................................................... 7–8

7.9. Changing Default Email Address ........................................................ 7–9

7.10. Deactivating a User ........................................................................ 7–9

7.11. Activating User ................................................................................ 7–10

7.12. Setting up User Password Lockout Preferences ............................................... 7–10

7.13. Unlocking User ................................................................................ 7–11

7.14. Deleting User .................................................................................. 7–11

Section 8. Managing the Fabric as a Whole

8.1. Understanding the Relationship Between System and Fabric ................................................ 8–1

8.2. Editing the System Attributes .................................................................. 8–1

8.2.1. Editing Sys Style ........................................................................... 8–4

8.3. Setting the Fabric Under Maintenance Mode ......................................................... 8–6

8.4. Setting Up Call Home .......................................................................... 8–7

8.4.1. Understanding Call Home ................................................................... 8–7

8.4.2. Viewing Call Home Configuration ....................................................... 8–8
### Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.3.</td>
<td>Configuring Call Home</td>
<td>8–8</td>
</tr>
<tr>
<td>8.4.4.</td>
<td>Verifying Call Home Configuration</td>
<td>8–9</td>
</tr>
<tr>
<td></td>
<td>Testing Call Home Connectivity Using</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Communication Test Packet Option</td>
<td>8–9</td>
</tr>
<tr>
<td></td>
<td>Testing Call Home Connectivity Using Ready for Use Test Packet Option</td>
<td>8–10</td>
</tr>
<tr>
<td>8.5.</td>
<td>Adding a Platform to the Fabric</td>
<td>8–11</td>
</tr>
</tbody>
</table>

#### Section 9. Managing High Availability in Your Fabric

| 9.1.    | Redundant Fabric Management Platform for High Availability            | 9–1  |
| 9.2.    | Overview of Fabric Manager Clustering                                 | 9–3  |
| 9.3.    | Understanding Data Replication in Clustering                          | 9–4  |
| 9.4.    | Understanding High Availability Fencing                               | 9–6  |
| 9.5.    | Understanding Cluster Groups                                          | 9–7  |
| 9.6.    | Accessing the Fabric Manager Cluster                                  | 9–8  |
| 9.7.    | Managing the Fabric Manager Cluster                                   | 9–8  |
| 9.7.1.  | Connecting to a Specific Fabric Management Platform                   | 9–10 |
| 9.7.2.  | Identifying All Access Points for the Cluster                         | 9–10 |
| 9.7.3.  | Managing the Cluster Service                                          | 9–12 |
| 9.7.5.  | Performing Routine Maintenance and Updates                            | 9–14 |
| 9.7.6.  | Viewing Current Failure Status and Limits for the Fabric Manager Resources | 9–15 |
| 9.7.7.  | Cleaning Up and Manually Resetting a Resource Failcount               | 9–16 |
| 9.7.8.  | Manually Migrating the Forward! Fabric Manager Workload               | 9–17 |
| 9.7.9.  | Interpreting OCF Return Codes                                         | 9–19 |

#### Section 10. Controlling Power for Each Platform

| 10.1.   | Understanding Status of Platforms                                     | 10–2 |
| 10.2.   | Powering-On a Platform                                                | 10–3 |
| 10.3.   | Performing Soft Shutdown on a Platform                                | 10–3 |
| 10.4.   | Powering-Off a Platform                                               | 10–4 |
| 10.5.   | Performing Hard Restart on a Platform                                 | 10–4 |
| 10.6.   | Performing Soft Restart on a Platform                                 | 10–5 |
| 10.7.   | Performing Power Cycle on Platform                                    | 10–5 |
| 10.8.   | Performing Force Dump on a Platform                                   | 10–6 |
Section 11. Managing Platforms

11.1. Viewing the Platform Summary ........................................ 11–1
11.2. Viewing Configuration Information of a Platform .............. 11–5
11.2.1. Partition Chassis List .............................................. 11–6
11.2.2. Configuration Details Section ................................. 11–7
11.3. Editing Platform’s Name and Description ....................... 11–9
11.4. Launching the Platform Management Card (PMC) Virtual
       Console .............................................................. 11–10
11.5. Deleting Partitionable EPP ......................................... 11–10
11.6. Deleting Nonpartitionable EPP ..................................... 11–11

Section 12. Bringing a Partition into Production

12.1. Understanding Partitions .............................................. 12–1
12.2. Managing the Blueprints ............................................ 12–2
12.2.1. Blueprints, Gold Images, and Commissioning ............. 12–2
12.2.2. Adding a Blueprint ............................................... 12–3
12.2.3. Deleting Blueprints .............................................. 12–5
12.2.4. Filtering Blueprints .............................................. 12–5
12.3. Managing a Gold Image .............................................. 12–7
12.3.1. Understanding a Gold Image .................................. 12–7
12.3.2. Adding a Gold Image ............................................ 12–8
12.3.3. Deleting Gold Images ........................................... 12–9
12.3.4. Filtering Images .................................................. 12–10
12.4. Overview of Commissioning a Partition ......................... 12–11
12.5. Commissioning a Partition Image ................................. 12–13
12.6. Starting a Partition Image ........................................... 12–17

Section 13. Managing Partitions

13.1. Understanding Status of Partition Images ......................... 13–1
13.2. Viewing the Partition Summary ..................................... 13–3
13.3. Accessing a Partition Desktop ..................................... 13–6
13.4. Changing the User/Password of the Partition Image
       Console .............................................................. 13–8
13.5. Deleting the User/Password of the Partition Image
       Console .............................................................. 13–9
13.6. Starting and Shutting down the Partition Images .............. 13–10
13.6.1. Starting a Partition Image ..................................... 13–10
13.6.2. Performing a Soft Restart of a Partition Image ............ 13–10
13.6.3. Performing a Hard Restart of a Partition Image ............ 13–11
13.6.4. Gracefully Shutting Down a Partition Image ................. 13–11
13.6.5. Shutting Down Multiple Partition Images .................... 13–11
13.6.6. Performing a Force Halt of a Partition Image ............... 13–12
16.6. Adding Additional DataNodes to a Hadoop Cluster . . . . . . . 16–8
16.7. Configuring Oozie . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 16–9
16.8. Specifying the Location of Secondary NameNode Data . . . . 16–9

Section 17. Shutting Down and Starting Up the Entire Fabric

17.1. Shutting Down the Entire Fabric . . . . . . . . . . . . . . . . . . . . . . . 17–1
17.2. Restarting the Fabric . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 17–2

Section 18. Backup and Restore

18.1. Backing Up Fabric Manager . . . . . . . . . . . . . . . . . . . . . . . . . 18–1
18.1.1. Preparing to Back Up Fabric Manager . . . . . . . . . . . . . 18–1
18.1.2. Backing up Fabric Manager Database and
        Configuration Files . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 18–2
18.2. Restoring Fabric Manager Database and Configuration
        Files . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 18–3
18.3. Backing Up Application Operating Environments on
        Enterprise Partition Platforms . . . . . . . . . . . . . . . . . . . . . . . . 18–3
18.4. Restoring Application Operating Environments on
        Enterprise Partition Platforms . . . . . . . . . . . . . . . . . . . . . . . . 18–4
18.5. Examples of Tools for Backing Up and Restoring
        Application Operating Environments . . . . . . . . . . . . . . . 18–4

Section 19. Time Management

19.1. Understanding Time Management . . . . . . . . . . . . . . . . . . . 19–1
19.2. Setting Time for Your Platform . . . . . . . . . . . . . . . . . . . . . . . 19–1

Section 20. Security Management

20.1. Understanding Security Management . . . . . . . . . . . . . . . 20–1
20.2. Using the Unisys Stealth Solution . . . . . . . . . . . . . . . . . . . 20–2
20.2.1. Understanding Stealth Security . . . . . . . . . . . . . . . . . . 20–2
20.2.2. Stealth Architecture . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 20–2
20.2.3. Required Knowledge and Documentation . . . . . . . . . . 20–4
20.2.4. General Networking Guidelines . . . . . . . . . . . . . . . . . . 20–4
20.2.5. General Installation and Configuration Guidelines . . . . 20–7

Section 21. Diagnostic Management

21.1. Managing Fabric Management Platform Dumps . . . . . . . . 21–1
21.1.1. Generating FMP Dumps . . . . . . . . . . . . . . . . . . . . . . . . . . . 21–1
21.1.2. Downloading FMP Dump File . . . . . . . . . . . . . . . . . . . . . . 21–2
21.1.3. Deleting FMP Dump File . . . . . . . . . . . . . . . . . . . . . . . . . . 21–3
21.2.1. Generating Platform Dump ................................. 21–3
21.2.2. Downloading Platform Dump ............................. 21–4
21.2.3. Deleting Platform Dump ................................. 21–5

Section 22. Troubleshooting

22.1. Troubleshooting Fabric Management Platform Problems .... 22–1
22.1.1. Troubleshooting Fabric Management Platform Problems ............................. 22–2
22.1.2. Unable to Generate Call Home Events for Fabric Management Platform ............................. 22–4
22.1.3. Unable to Launch Partition Image Console: Browser Settings Problem ............................. 22–5
22.1.4. Unable to Launch Partition Desktop: Installation Problem ............................. 22–6
22.2. Troubleshooting FFM User Problems .......................... 22–8
22.2.1. Unable to Search Users ........................................ 22–8
22.2.2. Fabric Manager User Forgot Password .................... 22–8
22.2.3. Resetting Password ........................................... 22–8
22.2.4. Unable to Edit Customer Identifier Information .......... 22–9
22.3. Troubleshooting Image Problems .............................. 22–9
22.3.1. Unable to view the recently added image in Fabric Manager ........................................ 22–10
22.3.2. Unable to Add a Blueprint or an Image ..................... 22–10
22.3.3. Unable to Shut Down the Partition Image .................. 22–10
22.4. Troubleshooting Commissioning Failure ...................... 22–11
22.4.1. Identifying the s-Par® IP Address ........................... 22–12
22.4.2. Determining the Universal Unique Identifier (UUID) of a Partition Image ............................. 22–12
22.4.3. Deleting a Partition Image .................................... 22–12
22.4.4. Cleaning the FFM Environment ............................. 22–13
22.5. Troubleshooting Dump Problems .............................. 22–13
22.5.1. Unable to Generate the Dump ............................. 22–14
22.5.2. Unable to download the dump .............................. 22–14
22.5.3. Unable to view the downloaded dump ........................ 22–14
22.5.4. Unable to Delete the Dump ................................. 22–15
22.5.5. Unable to Display the Dumps ................................ 22–15
22.6. Troubleshooting Platform Problems .......................... 22–16
22.6.1. Unable to add the platform .................................. 22–17
22.6.2. Unable to view recently added platform .................... 22–18
22.6.3. Platform Health is shown as Unknown, Critical or Warning ......................... 22–18
22.6.4. Unable to delete the partitionable EPP .................... 22–19
22.6.5. Unable to get the Chassis Details of partitionable EPP .................................................. 22–19
22.7. Troubleshooting Hardware Failures ................................. 22–20
22.7.1. Fabric Management Platform Suffers a Repairable Failure ........................................ 22–20
22.7.2. Fabric Management Platform Suffers a Catastrophic Failure ........................................ 22–20
22.8. Troubleshooting Info Pane Problems ............................ 22–21
22.8.1. Info Pane Content does not Get Refreshed ................. 22–21
22.9. Troubleshooting Fabric Manager Services Problems .......... 22–22
22.9.1. Fabric Manager Services are not functional. .............. 22–22
22.10. Reporting Problems to Unisys ................................. 22–24

Appendix A. User Roles and Privileges

Appendix B. Worksheet for Commissioning

Appendix C. Call Home Configuration Parameters
Figures

3–2. Two Examples of Valid Partition Combinations ......................................................... 3–15
3–3. NIC Ports and HBA Ports Owned by a Given Partition ................................................ 3–16
3–4. NIC Ports and HBA Ports Owned by a Given XS Partition ......................................... 3–16
3–5. A Small Partition that Can Grow to Medium, Large, and Max ..................................... 3–17
3–6. A Small Partition that Can only Grow to Medium ....................................................... 3–17
3–7. Sizes and Chassis for a 2-Socket, 8-Core EPP ............................................................. 3–18
3–8. Sizes and Chassis for a 2-Socket, 10-Core EPP ........................................................... 3–20
3–9. Sizes and Chassis for a 4-Socket, 12-Core EPP ........................................................... 3–22
3–10. Sizes and Chassis for a 4-Socket, 15-Core EPP .......................................................... 3–24

5–1. Physical Location of Ports for 2-Socket EPP with 3 Quad-Port 1GbE NICs and 3 Dual-Port 8Gb Fibre Channel HBAs .............................................................. 5–2
5–2. Physical Location of Ports for 2-Socket EPP with 3 Quad-Port 1GbE NICs and 3 Quad-Port 8Gb Fibre Channel HBAs .............................................................. 5–2
5–3. Physical Location of Ports for 2-Socket EPP with 3 Dual-Port 10GbE NICs and 3 Dual-Port 8Gb Fibre Channel HBAs ............................................................... 5–3
5–4. Physical Location of Ports for 2-Socket EPP with 3 Dual-Port 10GbE NICs and 3 Quad-Port 8Gb Fibre Channel HBAs ............................................................... 5–3
5–5. Physical Location of Ports for 4-Socket EPP with 4 Quad-Port 1GbE NICs and 4 Dual-Port 8Gb Fibre Channel HBAs ............................................................... 5–3
5–6. Physical Location of Ports for 4-Socket EPP with 4 Quad-Port 1GbE NICs and 4 Quad-Port 8Gb Fibre Channel HBAs ............................................................. 5–4
5–7. Physical Location of Ports for 4-Socket EPP with 4 Dual-Port 10GbE NICs and 4 Dual-Port 8Gb Fibre Channel HBAs ............................................................... 5–4
5–8. Physical Location of Ports for 4-Socket EPP with 4 Dual-Port 10GbE NICs and 4 Quad-Port 8Gb Fibre Channel HBAs ............................................................. 5–5

7–1. Portal and Fabric Manager Roles .................................................................................... 7–2

9–1. YaST Control Center with the Other Group Open ....................................................... 9–11
9–2. Example of Unisys Cluster Application Window Displaying IP Access Points ............. 9–12
9–3. Typical Cluster Status Screen using HAWK Interface ............................................... 9–14
9–4. Cluster Status with Failures Highlighted ....................................................................... 9–16
9–5. Moving the Workload .................................................................................................. 9–18

15–1. General Event Lifecycle ............................................................................................... 15–3
15–2. Call Home Event Lifecycle ......................................................................................... 15–4
15–3. Filtering Events .......................................................................................................... 15–9
Figures

22-1. Fabric Manager Service commands and their output. . . . . . . . . . . . . . . . . . . . 22-24
Tables

2–1. Definitions of Components in the Fabric ........................................ 2–2
4–1. Fabric Manager User Interface Components ................................. 4–2
5–1. Partition Chassis and Partition Size Fields and Description .......... 5–9
9–1. Common OCF Return Codes ...................................................... 9–19
12–1. Partition Chassis and Partition Size Fields and Description ......... 12–14
A–1. User Roles and Privileges ....................................................... A–1
B–1. Worksheet for commissioning ................................................... B–1
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) 19006085. To obtain a copy of the PLE, contact your service representative or access the current PLE from the product support Web site:

http://www.support.unisys.com/all/ple/19006085

Note: If you are not logged into the product support site, you will be asked to do so.

1.2. What’s New?

The following are the new features supported for Forward! by Unisys 2.0 release.

<table>
<thead>
<tr>
<th>New Feature</th>
<th>Link to Introductory Discussion</th>
</tr>
</thead>
</table>
| The Fabric Manager user interface is enhanced to provide more flexibility during commissioning in order to take advantage of the new EPP types. For example | 3.1.3 Partition Sizes
3.1.4 Partition Chassis
3.1.1 Overview of Commissioning a Partition
5.5 Commissioning a Partition Image
11.2 Viewing Configuration Information of a Platform |
- There are additional partition sizes, allowing a finer granularity of control over the number of processor cores dedicated to a given partition. |
- You can now specify the amount of memory dedicated to a given partition. |
- New UI displays graphically represent partition configurations so that you can commission partitions wisely. For example, you can display which NIC and HBA ports are available and which are already allocated. |
<table>
<thead>
<tr>
<th>New Feature</th>
<th>Link to Introductory Discussion</th>
</tr>
</thead>
<tbody>
<tr>
<td>The following partition operating systems are now supported, in addition to the previous ones:</td>
<td></td>
</tr>
<tr>
<td>• Windows 2012 R2</td>
<td>(not applicable)</td>
</tr>
<tr>
<td>• Red Hat Enterprise Linux 6.5</td>
<td></td>
</tr>
<tr>
<td>• SUSE Linux Enterprise Server (SLES) 11 SP3 for SAP Applications</td>
<td></td>
</tr>
<tr>
<td>You can now install Operating Systems for Windows and Linux partitions.</td>
<td>5.3 Installing Operating Systems for Windows and Linux Partitions</td>
</tr>
<tr>
<td>You can now view the Fabric Manager software version information.</td>
<td>4.2 Viewing Software Update Information</td>
</tr>
<tr>
<td>You may now order a redundant Fabric Management Platform for high availability.</td>
<td>Section 9, Managing High Availability in Your Fabric</td>
</tr>
<tr>
<td>The Forward! fabric now supports Apache Hadoop 2.0.</td>
<td>(not applicable)</td>
</tr>
<tr>
<td>You may now administer and control the user actions in the Portal with more options.</td>
<td>Section 7, Administering Users</td>
</tr>
<tr>
<td>The Fabric Manager now supports monitoring the Fabric Management Platform events.</td>
<td>(not applicable)</td>
</tr>
<tr>
<td>You can now view the status of Fabric Manager High Availability.</td>
<td>4.3.4 Viewing Fabric Manager High Availability Status</td>
</tr>
<tr>
<td>You can now resize a partition image and allocate the required memory.</td>
<td>13.12 Resizing Partition Images</td>
</tr>
<tr>
<td>You can now collect the diagnostic information for a platform by collecting the platform dumps.</td>
<td>21.2 Managing Platform Dumps</td>
</tr>
<tr>
<td>A Forward! fabric now supports up to 16 enterprise partition platforms (EPPs).</td>
<td>(not applicable)</td>
</tr>
<tr>
<td>For internal storage on EPPs, you can now choose Self-Encrypting Drives (SED) or Solid-State Drives (SSD), in addition to Hard Disk Drives (HDD). In addition, the size of HDD drives has been increased.</td>
<td>3.2.1 Internal and External Data Storage</td>
</tr>
<tr>
<td>Multiple RAID groups are now supported on EPPs.</td>
<td>3.2.3 RAID Configurations and RAID Groups</td>
</tr>
<tr>
<td>Upgrades from Release 1.1 to Release 2.0 are supported with assistance from Unisys. Contact your Unisys service representative to discuss upgrade options.</td>
<td>(not applicable)</td>
</tr>
</tbody>
</table>
1.3. Audience

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

• System administrators
• Network administrators
• System operators
• Unisys service representatives

1.4. Purpose

This document

• Describes the architecture and various Forward! Fabric user interface elements.
• Provides operational instructions to do the following:
  – Planning your fabric implementation
  – Completing initial product installation
  – Installing and configuring software
  – Administering users
  – Managing platforms
  – Controlling power for the platform
  – Managing partitions
  – Bringing a partition into production
  – Managing the events

1.5. Media and Documentation

The following documents are required or referenced in this document.

• Forward! by Unisys Product Documentation website
• Forward! by Unisys Information Center
• Forward! by Unisys Overview and Planning Guide (8222 4528)
• Forward! by Unisys Installation and Configuration Guide (8222 4536)
• Forward! by Unisys Fault Isolation and Servicing Guide (8222 4205)
• Forward! by Unisys Glossary (8222 4502)
Section 2
Fabric Architecture

This section summarizes the architecture of the Forward! by Unisys™ product, which is a fabric computing environment in which applications can run in multiple operating environments and on multiple Unisys Intel computers, all interconnected by a high-speed interconnect. All devices and operating environments in a given Forward! fabric are managed by a single instance of the Forward! Fabric Manager and can function as a single entity.

This section includes the following summary:

- **2.1 Summary of the Fabric Architecture**

For detailed information on the Forward! fabric architecture, see the Forward! Product Documentation Web Site on the Unisys Product Support web site.

### 2.1. Summary of the Fabric Architecture

The following figure shows the major components of the Forward! fabric, which are defined in the table that follows.
### Table 2–1. Definitions of Components in the Fabric

<table>
<thead>
<tr>
<th>Component</th>
<th>Definition</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer corporate LAN</td>
<td>Your enterprise’s Ethernet intranet. It allows your enterprise to communicate with each enterprise partition platform, with the Forward! Fabric Management Platform, and with other computers in your enterprise.</td>
<td>Note: The DVD drive in the enterprise partition platform is for Unisys maintenance use only. Customers should not use it.</td>
</tr>
<tr>
<td>Enterprise partition platform (EPP)</td>
<td>The computer that is the basic building block of a Forward! by Unisys™ 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.</td>
<td></td>
</tr>
<tr>
<td>Forward! fabric</td>
<td>A fabric computing environment from Unisys Corporation in which applications can run in multiple operating environments and/or on multiple Unisys 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 Forward! Fabric Manager) and can function as a single entity.</td>
<td>Note: A Forward! fabric is also referred to as a “Forward! system.”</td>
</tr>
<tr>
<td>Component</td>
<td>Definition</td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>------------</td>
<td></td>
</tr>
<tr>
<td>Forward! Fabric Management Platform</td>
<td>A computer equipped with Intel Xeon instruction processors that runs the Linux operating system and communicates with the enterprise partition platforms over the Forward! Management LAN. It provides the Web browser-based management user interface to the fabric, called the Forward! Fabric Manager.</td>
<td></td>
</tr>
<tr>
<td>Forward! Fabric Manager</td>
<td>Management software running on the Forward! 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 re-provisioning an entire server with alternate operating environments and software stacks, based on pre-existing partition templates called blueprints.</td>
<td></td>
</tr>
<tr>
<td>Forward! Management LAN</td>
<td>An Ethernet LAN for managing the enterprise partition platforms and partitions within the fabric. It enables the Forward! Fabric Management Platform to communicate with the enterprise partition platforms and partitions.</td>
<td></td>
</tr>
</tbody>
</table>
| 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 |
| Inter-Partition LAN | A LAN implemented using the high-speed Interconnect infrastructure and TCP/IP communications protocols. It enables the following to communicate with each other:  
  - Partitions residing on the same enterprise partition platform  
  - Partitions residing on different enterprise partition platforms |
| Operating systems | The operating systems providing the partition operating environments. The following operating systems are currently supported in the fabric: Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server 2012 R2, SUSE Linux SLES 11 SP3, SUSE Linux SLES 11 SP3 for SAP Applications, RedHat Linux RHEL 6.4, and RedHat Linux RHEL 6.5. |
| Partitions | A portion of a computer system 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. |
### Table 2–1. Definitions of Components in the Fabric (cont.)

<table>
<thead>
<tr>
<th>Component</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services</td>
<td>Service software provided with the <em>Forward!</em> fabric that an application can invoke, such as ePortal services, Enterprise Output Manager (EOM) print services, or Hadoop distributed file system services. All of these services have been sized and configured by Unisys to provide optimal support for your applications.</td>
</tr>
<tr>
<td>Unisys Secure Partitioning (s-Par®)</td>
<td>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.</td>
</tr>
<tr>
<td>User application</td>
<td>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 <em>Forward!</em> 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.</td>
</tr>
</tbody>
</table>
Section 3
Planning Your Fabric Implementation

This section provides the information on:

- 3.1 Partition Planning
- 3.2 Planning a Partitionable EPP’s Storage
- 3.3 Operating System Licensing
- 3.4 Customer Responsibilities for Operating Environments
- 3.5 Customer-Supplied Hardware

3.1. Partition Planning

A partition is a portion of a computer system that is supported by its own dedicated hardware resources (such as processors, memory, and input/output) and runs its own operating system. That is, partitions are the operating environments in which virtually all processing on a Forward! platform takes place.

A partition image is a bootable operating system (and optionally other software) to which partition hardware resources have been assigned. You create partition images using the Forward! Fabric Manager user interface during a process called commissioning. After the commissioning process is complete, the partition image is enabled (that is, it has been assigned hardware resources).

It is vital that you understand the factors that control the creation and running of partition images, so that you do not inadvertently create one partition image in a manner that interferes with your ability to create and/or run another at a later time.

3.1.1. Overview of Commissioning a Partition

Commissioning is the process of creating a partition image by using the Forward! 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; then you specify values for any additional required attributes, such as the partition image’s

- Name
- Partition chassis
- Size: Extra Small, Small, Medium, Large, Extra Large, Extra Extra Large, or Maximal
- Memory size (a default value is provided which you may change)
• Boot disk storage space (LUN size)

The Fabric Manager then creates the partition image. As a result of the commissioning process, the partition image appears in the left navigation pane of the Fabric Manager, is enabled, and is in a running state. 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 commissioning screen where you select the chassis, size, and so forth.
3.1.2. **Overview of Partition Planning**

The following information describes planning that you should do before your *Forward!* product arrives and even before you order it, to ensure that your fabric environment meets the needs of your applications.

**Planning Prior to Ordering**

Before ordering your *Forward!* fabric, plan your fabric environment as follows.

1. Identify the mission-critical enterprise applications or portions of applications that you will be running on Unisys Intel platforms in your *Forward!* fabric.  
   
   (Formally, a Unisys Intel platform is called an enterprise partition platform.)

2. Determine what internal storage type you want on your Unisys Intel platform: hard disk drive (HDD), solid state drive (SSD), or self-encrypting drive (SED).

3. Determine the total number of partitions needed to implement the applications or portions of applications.
   
   (Each partition is one operating environment; that is, each partition hosts one operating system and its software stack.)

4. Determine if any two (or more) partitions need to be on separate Unisys Intel platforms (enterprise partition platforms) for resiliency purposes. That is, if you have two partitions that you do not want to be simultaneously unavailable, then for added resilience you should assign them to different Unisys Intel platforms.

5. For each partition, do as follows.
   
   a. Determine the type of operating system that will run on the partition.
      
      - Windows Server 2008 R2 SP1
      - Windows Server 2012
      - Windows Server 2012 R2
      - SUSE Linux Enterprise Server 11 SP3
      - SUSE Linux Enterprise Server (SLES) 11 SP3 for SAP Applications
      - Red Hat Enterprise Linux 6.4
      - Red Hat Enterprise Linux 6.5

   b. Determine what hardware resources—instruction processor cores, memory, network interface card (NIC) ports, and host bus adapter (HBA) ports—will be needed by the partition.

   c. Determine the partition size needed to meet the hardware resource needs: Extra Small (XS), Small (S), Medium (M), Large (L), Extra Large (XL), Extra Extra Large (XXL), or Maximal (Max).

   d. Determine the size of the LUN needed by the partition.
**Note:** You should do this for all enabled partitions that run concurrently, regardless of whether those partitions are running or stopped. But you should also do it for any disabled partitions that will be dormant, because disabled partitions also occupy a LUN.

The overall physical storage of a platform’s **SAS disks** is divided into logical virtual disks, in order to provide flexibility in allocating storage space. These virtual disks can then be assigned to the various partitions on the platform as desired. Virtual disks are identified by logical unit numbers (LUNs). Different LUNs represent different instances of storage space for use by different partitions.

At minimum, the required size of the partition’s LUN is the storage size of the operating system itself. However, instead of using external storage for application data, you might want to associate the application data with the partition by configuring the LUN’s space as multiple disk drives (for example C: and K:). In this case, you must also include this application data storage size in the partition LUN along with the operating system size. So the LUN size calculation is as follows:

\[
\text{Required OS size} + \text{additional optional application data size}
\]

Note that the size of the partition LUN for gold images supplied by Unisys must be at least 60 GB for a Windows partition and 10 GB for a Linux partition. The size of customer-supplied gold images may differ.

e. Determine whether the partition will be running all of the time or only part of the time (that is, always enabled, or sometimes disabled in favor of another partition executing in the same space).

f. Do both of the following:

- Determine whether the partition’s hardware resource needs—processor cores, memory, NICs, and HBAs—will conflict with the needs of other partitions.
- Determine whether the partition’s hardware resource needs will conflict with the needs of other partitions if you must change the size of the partition.

See **3.1.6 How to Choose Partition Sizes and Chassis** to understand how the hardware resource needs of one partition may conflict with another.

If you do find conflicts, consider whether the partitions in conflict have to run at the same time. If a partition will only run part of the time, perhaps another partition that uses the same hardware resources can run at a different time, so that there is no conflict for resources.

6. For each platform:

a. Add up all of the LUN storage sizes for all of the platform’s partitions. (Remember to include partitions that will not be simultaneously enabled.) This gives you a total required LUN storage size for the platform.

b. Determine how many SAS disk drives the platform needs in order to accommodate the total required LUN storage size for the platform.

See **3.2.2 Virtual Disks (LUNs) for Internal Storage** for detailed information on LUN planning, including how much LUN storage space is available when different numbers of SAS disks are ordered.
Note the following:

- The total storage size of all of the partition LUNs on a platform affects the number of possible partitions that the platform can support. Having too many partitions with large LUN storage sizes might exceed the capacity of the number of SAS disks that you have purchased for a given platform.

- Regardless of the total LUN size, there is a maximum of 11 customer LUNs in the base configuration EPP RAID group and 16 customer LUNs in additional RAID groups.

7. Determine what RAID type (level) you want, for example RAID 5; and how many RAID groups you want. (See 3.2.3 RAID Configurations and RAID Groups.)

Flow Chart

The following figure summarizes the preceding information in flow chart form.
At Ordering Time

Based on the preceding planning, you will be able to provide the required information when you order your Forward fabric or set it up initially:
• How many Unisys Intel platforms (partitionable enterprise partition platforms) do you need?
• For each platform, what operating systems will be run?
• For each platform, how many internal SAS disk drives do you need, and of what type?
• For each platform, what type (level) of RAID do you want for data protection, and how many RAID groups?

3.1.3. Partition Sizes

A partitionable enterprise partition platform (EPP)—that is, a platform hosting s-Par® firmware—can host partitions of different sizes. "Size" means the relative amount of total EPP physical resources that the partition consumes. The size is most directly related to the number of processor cores in the partition.

*Note:* The 1-socket EPP is nonpartitionable, that is, it does not run s-Par® firmware.

The partition sizes and the corresponding number of processor cores are as follows. Apart from Maximal partitions, each size has double the number of processor cores of the next smaller size.

<table>
<thead>
<tr>
<th>Size</th>
<th>Abbreviation</th>
<th>Number of Processor Cores, 2-Socket EPP</th>
<th>Number of Processor Cores, 4-Socket EPP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extra Small</td>
<td>XS</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Small</td>
<td>S</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Medium</td>
<td>M</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Large</td>
<td>L</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>Extra Large</td>
<td>XL</td>
<td>n/a</td>
<td>16</td>
</tr>
<tr>
<td>Extra extra large</td>
<td>XXL</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Maximal</td>
<td>Max</td>
<td>14</td>
<td>18</td>
</tr>
</tbody>
</table>

Relative Sizes

2-socket EPP, 8 cores per socket

Note that for this platform type (two sockets, eight cores per socket), the number of cores in size Max (14) is less than the total number of cores on the platform (16), because Unisys Secure Partitioning (s-Par®) requires cores to do its work.
2-socket EPP, 10 cores per socket

Note that for this platform type (two sockets, ten cores per socket), the number of cores in size Max (18) is less than the total number of cores on the platform (20), because Unisys Secure Partitioning (s-Par®) requires cores to do its work.

4-socket EPP, 12 or 15 cores per socket

Note that the Max partition size is not supported for 4-socket EPPs. XXL is the largest (32 cores).

3.1.4. Partition Chassis

A partition chassis (“chassis,” for short) is a logical container representing the location into which the partition’s software (that is, the partition image) is to be loaded. A given partitionable enterprise partition platform (EPP) includes up to twelve partition chassis, depending on whether an EPP has two processor sockets or four. Chassis are named Chassis-A, Chassis-B, Chassis-C, and so forth.
There is one and only one chassis per partition.

During commissioning, you use the Forward! Fabric Manager user interface to select the chassis for the partition image. You also select the partition size. Together, the partition chassis and partition size determine which specific processor cores, NIC ports, and HBA ports are allocated to the partition.

You are not able to alter which processor cores, NIC ports, and HBA ports are assigned to a given chassis of a given size. If the number of cores or ports is not acceptable for the partition, you must pick a different partition size.

There is a relationship between chassis and size: A partition with a given chassis can only be of certain sizes. For example

- A Maximal partition must always use Chassis-A.
- An Extra Large partition must always use Chassis-A, Chassis-B, or Chassis-C.

The following figure represents

- All the hardware resources of an EPP, that is, all the processor cores, NIC ports, and HBA ports on an EPP
- A Maximal partition commissioned on the EPP

As the figure represents, all the hardware resources (cores, NIC ports, and HBA ports) on the EPP are consumed by a Maximal partition. A Maximal partition always uses Chassis-A.
Contrarily, the following figure represents an EPP with one Large partition, two small partitions, and two Extra Small partitions. The size of each partition determines the amount of hardware resources (cores, NIC ports, and HBA ports) consumed by each partition. And each partition uses a different chassis.
The following are rules for chassis:

- A partition image is permanently anchored to the chassis that was chosen during commissioning. That is, the partition image is always associated with that chassis. Once you assign a particular chassis to a particular partition image, the association is permanent.

- Multiple partition images can share the same chassis, as long as only one of the partition images is enabled at a time.

Partition images are automatically enabled after commissioning. But using the Fabric Manager, you can disable them. Disabling all partition images that share the same chassis except one enables you to commission multiple partition images that use the same chassis. (Disabling a partition image frees up its hardware resource blocks; however, the partition image content is persisted on mass storage for possible future use. That means you can enable the partition image later.)

### 3.1.5. How the Fabric Manager Guides Partition Design

The Fabric Manager enforces rules for constructing partitions and prevents you from defining invalid partitions. For example, during commissioning, when you select a chassis, the Fabric Manager then lets you select only partition sizes that are valid for that chassis.

The Fabric Manager user interface also provides displays that enable you to do “what-if” explorations when designing partitions. The following screens are an example.
1. When you highlight an enterprise partition platform (PEPP0, in this case), then select the **Config. Info** tab, and then under **Details: Chassis-A** select the **Small** tab, you see the following display. It presents information about that chassis (Chassis-A) for that size (Small). In this case, the resulting partition would have

- Two processor cores
- Two to 511 GB of memory (the user can specify the desired size)
- One NIC port (port 0 in slot 3)
- One HBA port (port 0 in slot 7)

2. If you then select the **Medium** tab, you can see what system resources you would receive if you commissioned your Chassis-A partition as size Medium rather than size Small. In this case, the resulting partition would have

- Four processor cores
- Two to 128 GB of memory (the user can specify the desired size)
- One NIC port (port 0 in slot 3)
- One HBA port (port 0 in slot 7)
3.1.6. How to Choose Partition Sizes and Chassis

Understanding Partition Design Better

For many users, relying on the Fabric Manager to guide partition design, as described in the previous subsection, will be sufficient. However, if you commission a partition and find out later that it does not meet your needs—for example, it does not have enough processor cores or NIC ports—you need to decommission the partition and then recommission it.

The better you understand how physical resources are allocated to a partition, the easier it will be to avoid having to decommission and recommission. To commission a partition most effectively, you should understand how much of the enterprise partition platform’s (EPP’s) physical resources will be consumed by the partition, and how your choices for one partition might be dependent on your choices for other partitions.
Visual Aid for Partition Planning

**Figure 3-1** is a visual aid for understanding and planning
- Partition sizes, chassis, and NIC and HBA ports
- How to combine different partitions on the same EPP
- The extent to which you will be able to increase the size of a partition in the future

(Specifically, this figure represents the 2-socket, 8-core EPP, but guidelines for using the figure and others like it are the same regardless of which EPP type you have.)

![Figure 3-1: Visual Aid for Choosing Partition Sizes and Chassis](image)

**Choosing Partition Sizes and Chassis**

A partition’s size and chassis determine which of the EPP’s physical resource are consumed by the partition. In **Figure 3-1**, the XS, S, M, L, and Max columns represent the amount of physical resources consumed by a partition of that size. They also specify the chassis that you can use when commissioning a partition of that size. For example:
- A Max partition and a Large partition must use Chassis A.
- A Medium partition could use Chassis A, but it could also use B or C.
- An Extra Small (XS) partition can use Chassis E, J, F, C, H, G, L, D, or I.
Combining Partitions on the Same EPP

When placing multiple partitions on the same EPP, only certain combinations of sizes and chassis are allowed. No two enabled partitions can simultaneously use the same chassis, because a given chassis represents a specific set of physical resources (for example, processor cores), and two different enabled partitions cannot own the same physical resources.

In Figure 3–1, a given partition of a given size, commissioned using a given chassis, consumes all of the physical resources to the left of it. So for example if you commission a Large partition (always on Chassis A), you cannot commission the following partitions to the left of it in Figure 3–1:

- Medium partitions on Chassis A or B
- Small partitions on Chassis A, E, B, or F
- Extra Small partitions on Chassis E, J, F, or K

To construct a valid combination of partition sizes and chassis, make sure no partition is to the left of another in Figure 3–1. For example, both of the following in Figure 3–2 are valid combinations:

Figure 3–2. Two Examples of Valid Partition Combinations

NICs and HBAs Owned by a Given Partition

In Figure 3–1, a partition of a given size, commissioned using a given chassis, includes all of the NIC ports and HBA ports (columns 1 and 2) to the left of the partition. For example, a Large partition (always Chassis A) includes the following:
Figure 3–3. NIC Ports and HBA Ports Owned by a Given Partition

Whereas an Extra Small partition commissioned using Chassis I includes only NIC slot 2, port 2; and HBA slot 6, port 2:

Figure 3–4. NIC Ports and HBA Ports Owned by a Given XS Partition

Caution

For HBAs, ports 2 and 3 are only available with the quad-port HBA; the dual-port HBA is limited to ports 0 and 1. If you desire many partitions with storage I/O, then you should order quad-port HBAs for your enterprise partition platform.

Ensuring a Partition Can Grow in the Future

You might decide that your current needs are met by a relatively small-sized partition, but suspect that in the future you may want to increase the size of this partition. Figure 3–1 once again helps you understand which partitions can grow in size and which cannot. A partition of a given size, commissioned using a given chassis, can grow in the future if that same chassis appears in a partition of a larger size (that is, appears to the right of the first chassis).
Example 1: A Small partition commissioned on Chassis A can grow to Medium, Large, or Max, because Chassis A appears in a partition of size Medium, Large, and Max.

![Figure 3-5. A Small Partition that Can Grow to Medium, Large, and Max](image)

Example 2: On the other hand, a Small partition commissioned on Chassis C can only grow to Medium, because there is no Large or Max partition commissioned using Chassis C.

![Figure 3-6. A Small Partition that Can only Grow to Medium](image)

Example 3: A Small partition commissioned on Chassis E cannot grow at all, because there is no Medium, Large, or Max partition commissioned using Chassis E.
### 3.1.7. Sizes and Chassis for a 2-Socket, 8-Core EPP

*Figure 3–7* shows the chassis and NIC and HBA ports consumed by a partition of a given size on an EPP with two sockets and 8 cores per socket.

<table>
<thead>
<tr>
<th>Dedicated NICs (Slot:Port)</th>
<th>Shared NICs (Slot:Port)</th>
<th>Dedicated HBAs (Slot:Port)</th>
<th>XS (1 core)</th>
<th>S (2 cores)</th>
<th>M (4 cores)</th>
<th>L (8 cores)</th>
<th>Max (14 cores)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4:0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2:0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2:1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4:2*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4:1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2:0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:3*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4:3*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:2*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2:1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2:2*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Ports 2 and 3 are only available with the quad-port adapters

*Figure 3–7. Sizes and Chassis for a 2-Socket, 8-Core EPP*

The following are two examples of valid combinations of partitions.
3.1.8. Sizes and Chassis for a 2-Socket, 10-Core EPP

Figure 3–8 shows the chassis and NIC and HBA ports consumed by a partition of a given size on an EPP with two sockets and 10 cores per socket.
### Partition Planning

**Figure 3–8. Sizes and Chassis for a 2-Socket, 10-Core EPP**

The following are two examples of valid combinations of partitions.
3.1.9. Sizes and Chassis for a 4-Socket, 12-Core EPP

Figure 3–9 shows the chassis and NIC and HBA ports consumed by a partition of a given size on an EPP with four sockets and 12 cores per socket.
Figure 3–9. Sizes and Chassis for a 4-Socket, 12-Core EPP

The following are two examples of valid combinations of partitions.

<table>
<thead>
<tr>
<th>Dedicated NICs (Slot:Port)</th>
<th>Shared NICs (Slot:Port)</th>
<th>Dedicated HBAs (Slot:Port)</th>
<th>XS (1 core)</th>
<th>S (2 cores)</th>
<th>M (4 cores)</th>
<th>L (8 cores)</th>
<th>XL (16 cores)</th>
<th>XXL (32 cores)</th>
</tr>
</thead>
<tbody>
<tr>
<td>7:0</td>
<td></td>
<td></td>
<td>3:0</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Chassis A</td>
<td></td>
</tr>
<tr>
<td>7:1</td>
<td></td>
<td></td>
<td>3:0</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Chassis A</td>
<td></td>
</tr>
<tr>
<td>8:0</td>
<td></td>
<td></td>
<td>3:0</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Chassis A</td>
<td></td>
</tr>
<tr>
<td>8:1</td>
<td></td>
<td></td>
<td>3:0</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Chassis A</td>
<td></td>
</tr>
<tr>
<td>9:0</td>
<td></td>
<td></td>
<td>3:0</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Chassis A</td>
<td></td>
</tr>
<tr>
<td>9:1</td>
<td></td>
<td></td>
<td>3:0</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Chassis A</td>
<td></td>
</tr>
<tr>
<td>10:0</td>
<td></td>
<td></td>
<td>3:0</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Chassis A</td>
<td></td>
</tr>
<tr>
<td>10:1</td>
<td></td>
<td></td>
<td>3:0</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Chassis A</td>
<td></td>
</tr>
<tr>
<td>1:0</td>
<td></td>
<td></td>
<td>8:0</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Chassis C</td>
<td></td>
</tr>
<tr>
<td>1:1</td>
<td></td>
<td></td>
<td>8:1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Chassis D</td>
<td></td>
</tr>
<tr>
<td>2:3* 6:2*</td>
<td></td>
<td></td>
<td>7:3*</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Chassis K</td>
<td></td>
</tr>
<tr>
<td>3:1</td>
<td></td>
<td></td>
<td>7:1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Chassis B</td>
<td></td>
</tr>
<tr>
<td>4:0 6:1</td>
<td></td>
<td></td>
<td>9:0 10:1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Chassis E</td>
<td></td>
</tr>
<tr>
<td>4:3* 6:0</td>
<td></td>
<td></td>
<td>9:3* 10:0</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Chassis G</td>
<td></td>
</tr>
<tr>
<td>4:1 4:2*</td>
<td></td>
<td></td>
<td>9:1 10:2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Chassis F</td>
<td></td>
</tr>
<tr>
<td>6:3*</td>
<td></td>
<td></td>
<td>10:3*</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Chassis M</td>
<td></td>
</tr>
</tbody>
</table>

* Ports 2 and 3 are only available with the quad-port adapters.
3.1.10. Sizes and Chassis for a 4-Socket, 15-Core EPP

Figure 3–10 shows the chassis and NIC and HBA ports consumed by a partition of a given size on an EPP with two sockets and 15 cores per socket.
The following are two examples of valid combinations of partitions.

Figure 3–10. Sizes and Chassis for a 4-Socket, 15-Core EPP
3.2. Planning a Partitionable EPP’s Storage

You must consider the disk storage space needs of your application and ensure that when you commission a partition image, it includes enough internal storage space.
The Forward! fabric supports a variety of external storage devices.

### 3.2.1. Internal and External Data Storage

#### Internal Data Storage Drive Types

Enterprise partition platforms (EPPs) include internal Serial Attached SCSI (SAS) storage drives in a variety of customer-orderable types.

<table>
<thead>
<tr>
<th>Hard disk drive (HDD)</th>
<th>HDD is a low-cost storage technology relying on magnetic rotating disks and a moving actuator arm.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• 300 GB drives are the base configuration; customers can order larger disk drives as an option.</td>
</tr>
<tr>
<td></td>
<td>• 1-socket EPP: Supports 300 GB, 600 GB, and 1.2 TB disks.</td>
</tr>
<tr>
<td></td>
<td>• 2-socket EPP: Supports 300 GB, 600 GB, and 1.2 TB disks.</td>
</tr>
<tr>
<td></td>
<td>• 4-socket EPP: Supports 300 GB, 600 GB, and 1.2 TB disks.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Solid state drive (SSD)</th>
<th>SSD is a high-speed storage technology using circuit boards rather than mechanical components.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• SSD is a customer-orderable option.</td>
</tr>
<tr>
<td></td>
<td>• 1-socket EPP: Supports 200 GB and 400 GB disks.</td>
</tr>
<tr>
<td></td>
<td>• 2-socket EPP: Supports 200 GB and 400 GB disks.</td>
</tr>
<tr>
<td></td>
<td>• 4-socket EPP: Supports 200 GB, 400 GB, 800 GB, and 1.6 TB disks.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Self-encrypting drive (SED)</th>
<th>SED is a storage technology in which data on the drive is automatically encrypted.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• SED is a customer-orderable option.</td>
</tr>
<tr>
<td></td>
<td>• 1-socket EPP: Supports 1.2 TB disks.</td>
</tr>
<tr>
<td></td>
<td>• 2-socket EPP: Supports 300 GB and 1.2 TB disks.</td>
</tr>
<tr>
<td></td>
<td>• 4-socket EPP: Supports 300 GB and 1.2 TB disks.</td>
</tr>
</tbody>
</table>

#### Rules for Ordering Internal Data Storage Drives

- HDD is the base configuration. Each order includes a minimum of four 300 GB HDD disks. (The 1-socket nonpartitionable EPP requires a minimum of three 300 GB HDD disks.)

- Maximum number of internal storage drives per EPP
  - 1-socket nonpartitionable EPP: 8 drives maximum
  - 2-socket EPP: 16 drives maximum
  - 4-socket EPP: 24 drives maximum
• All SAS storage drives are in RAID pairs. Drives are purchased in increments that support the type of RAID that you order. For example, RAID 10 requires at least 4 drives. RAID 1 requires at least 2 drives.

• You may have multiple types of storage drives (HDD, SSD, SED) on a given EPP, but they must be in separate RAID groups.

• You may order field upgrades to add additional storage devices. Upgrades are installed by a Unisys service representative.

• Note that the Forward! Fabric Management Platform is an appliance configured by Unisys Corporation. You cannot access the internal storage drives.

External Storage

The Forward! fabric supports a variety of external storage devices. Access to external storage from enterprise partition platforms is provided via standards-based connection methods such as

• Fibre Channel (FC)
• Fibre Channel Over Ethernet (FCOE)
• iSCSI

For details on supported external storage devices, see your Unisys sales representative.

You can boot a partition’s operating system from an external storage device. See 6.5.1 Booting from Internal or External Storage for more information.

3.2.2. Virtual Disks (LUNs) for Internal Storage

When you order a Forward! fabric, you choose how many SAS disk drives you want each enterprise partition platform (EPP) to include.

The overall physical storage of a partitionable EPP’s SAS disks is divided into logical virtual disks, in order to provide flexibility in allocating storage space. These virtual disks can then be assigned to the various partitions on the platform as desired. Virtual disks are identified by logical unit numbers (LUNs).

Each partition (both enabled and disabled) can have a maximum of one virtual disk (LUN) assigned to it from a RAID group of internal disks.

The base configuration consists of four 300 GB HDD storage drives configured as a single RAID group. There are 11 user LUNs in this RAID group (and another 5 dedicated to usage by s-Par® firmware).

(Because the 1-socket EPP does not run s-Par® firmware, all 16 LUNs are available to its RAID group.)
When the *Forward!* product is first installed at your site, the Unisys service representative will consult with you to determine how you want to divide up each partitionable EPP’s available physical disk storage space into virtual disk storage space for your partitions. That is:

- How many LUNs you desire, one per partition image boot volume
- The size of each LUN

Note that the size of the partition image virtual disk (LUN) must be an absolute minimum of 60 GB for a Windows partition image and 10 GB for a Linux partition image. Depending on the planned usage of the partition, significantly more may be required. See 3.1.2 Overview of Partition Planning for information on how to determine LUN size.

The storage size available for user virtual disks (LUNs) varies depending on the number of physical disks, as described in the following table. This table assumes that all disks are 300 GB drives configured as RAID 10. The information in the table changes based on disk capacity and RAID type.

<table>
<thead>
<tr>
<th>Number of Physical Internal Disk Drives</th>
<th>Approximate Maximum Virtual Disk (LUN) Size for Users (11 Virtual Disks)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>~433GB</td>
</tr>
<tr>
<td>6</td>
<td>~713GB</td>
</tr>
<tr>
<td>8</td>
<td>~992GB</td>
</tr>
<tr>
<td>10</td>
<td>~1.24TiB</td>
</tr>
<tr>
<td>12</td>
<td>~1.55TiB</td>
</tr>
<tr>
<td>14</td>
<td>~1.79TiB</td>
</tr>
<tr>
<td>16</td>
<td>~2.11TiB</td>
</tr>
</tbody>
</table>

This release supports up to 12 enabled partition images. However, there are only 11 user LUNs available in the base configuration RAID group. Therefore, to support 12 enabled partition images (or any combination of enabled and disabled partition images exceeding 11), you must have at least two RAID groups. Two RAID groups provide 27 user partition LUNs:

- 11 from the first RAID group (because 5 are used for s-Par firmware)
- All 16 from the second RAID group (since s-Par firmware’s needs have been met)

### 3.2.3. RAID Configurations and RAID Groups

#### Supported RAID Types

Supported and default RAID types are as follows:
• RAID 0, 1, 5, 6, 10, 50, or 60
  The 1-socket nonpartitionable EPP does not support RAID 6 or 60.
• For 1-socket EPPs, the base configuration is three 300 GB disks. There is no default RAID type.
• For 2-socket and 4-socket EPPs, the base configuration is four 300 GB disks configured as RAID 10.

**RAID Groups**

A RAID group is a set of associated storage drives having a single RAID type. One or more LUNs (virtual disks) are assigned to the RAID group. All LUNs in the RAID group are distributed equally across all the storage drives. The RAID group type determines how many storage disks you can have in a RAID group.

This release supports up to 12 enabled partition images. However, there are only 11 user LUNs available in the base configuration RAID group. Therefore, to support 12 enabled partition images (or any combination of enabled and disabled partition images exceeding 11), you must have at least two RAID groups.

**How RAID Groups Are Established**

The desired number of RAID groups are established as follows:

1. During the ordering process, the customer specifies the number of RAID groups that are desired.
2. For each RAID group, the customer specifies
   • The internal storage drive type
   • The number of internal storage drives that are desired (in increments that support the defined RAID type)
   • The RAID type (RAID 0, 1, 5, 6, 10, 50, or 60)
     The 1-socket EPP does not support RAID 6 or 60.
3. The Unisys factory sets up EPPs with the desired type and number of SAS drives, with the desired RAID configuration.
4. When your Forward! fabric is installed, the Unisys service representative works with the customer to configure
   • The number of LUNs (partition image virtual disks) that you desire per RAID group
   • The size of each LUN
5. If in the future you wish to make any changes to RAID groups, these changes are performed by the Unisys service representative.

**Rules for RAID Groups**

Rules for RAID groups are as follows:
All SAS storage drives are configured in RAID pairs. Storage drives are purchased in increments that support the type of RAID that you order. For example, RAID 10 requires at least four drives. RAID 1 requires at least two drives.

The base configuration includes one RAID group (RAID 10) consisting of four 300GB HDD storage drives and 11 user LUNs.

The 1-socket EPP includes one RAID group consisting of three 300GB HDD storage drives and 16 user LUNs.

Each RAID group (excluding the RAID group in the base configuration) is configured with up to 16 LUNs that are available for partitions.

All storage drives in a RAID group must be the same type and disk capacity.

You may have multiple types of storage drives (HDD, SSD, SED) on a given EPP, but they must be in separate RAID groups.

### 3.2.4. Allocating Internal Storage Among Partitions

You allocate partitionable enterprise partition platform (EPP) internal disk storage space as follows:

1. The partitionable EPP arrives from the factory with the number of SAS disks that you ordered and with five LUNs devoted to s-Par® use.
2. As part of your planning, you should consider the storage needs of your applications and have this information available when your Forward! product is installed.
3. As part of installing the Forward! product, the Unisys service representative will work with you to configure LUNs according to your needs, as well as create LUNs having the sizes you desire, based on your needs.
4. When you commission a partition image, the LUNs created by the service representative will be available in the Forward! Fabric Manager user interface. You merely select the LUN size that you want for that particular partition image.

### 3.3. Operating System Licensing

Regardless of whether you purchased an operating system license from Unisys Corporation or from a third party, in general operating system suppliers

- Will not allow a license purchased for one enterprise partition platform to be used on another enterprise partition platform.
- Will allow a license purchased for one of the partitions on an enterprise partition platform to be used for a different partition on that same enterprise partition platform, provided both partitions do not simultaneously reside on the enterprise partition platform. (That is, only one can be enabled at a time.)

For precise licensing requirements, see your operating system vendor.
- Each Windows Server 2012 or Windows Server 2012 R2 license supports two partitions, including downgrades to Windows Server 2008 R2 SP1. Customers supplying licenses for Windows Server 2008 R2 SP1 must adhere to Microsoft virtualization rights for that product.
- Unisys Corporation offers licenses supporting 2, 4, 6, 8, 10, or 12 Windows operating systems per enterprise partition platform.
- Customers cannot purchase add-on licenses from Unisys Corporation.
- No license renewal is required.
- Customers who want the option of installing new releases of Windows operating systems must purchase Software Assurance from a third party within the time limit specified by Microsoft (typically 90 days).
- It is the customer’s responsibility to meet licensing requirements and to track:
  - Which types of licenses they possess (OEM licenses from Unisys Corporation versus customer-supplied licenses)
  - How many of each type they have
- Customers must review the Microsoft Software License Terms document provided with their order, and adhere to the terms.
Subscriptions may be purchased through Unisys Corporation, SUSE, or a SUSE distributor/reseller.

For subscriptions purchased through Unisys Corporation:

- Each SUSE Linux Enterprise Server (SLES) 11 subscription supports one of the following:
  - Two sockets with up to 12 SLES partitions
  - Four sockets with up to 16 SLES partitions (only 12 simultaneously-enabled partitions are supported at this time)
- Unisys Corporation sells subscriptions with 1-, 3-, or 5-year terms.
- A subscription requires management between SUSE and the customer.
- Subscription renewal is required at the end of the term and is the customer’s responsibility.
- You can renew your subscription through Unisys Corporation.

Subscriptions are purchased through Red Hat Corporation or a Red Hat distributor/reseller.

- Each Red Hat subscription supports a single partition. Each partition running Red Hat requires its own subscription.
- Subscriptions are based on the number of sockets allocated to the partition.
- A subscription requires management between Red Hat and the customer.
- Subscription renewal is required at the end of the term and is the customer’s responsibility.
- You can renew your subscription through Red Hat Corporation or a Red Hat distributor/reseller.
3.4. Customer Responsibilities for Operating Environments

Operating Environments for EPPs

• Once it has been commissioned, an enterprise partition platform (EPP) partition is yours to do with as you please. For example, you may install applications, operating system patches, anti-virus software, and so forth, as you see fit.

• You are responsible for the following:
  – Installing and maintaining anti-virus software
  – Determining what Windows or Linux operating system patches to install, and installing them
  – Adhering to operating system license requirements
  – Performing regular backup of the partition operating environments after initial commissioning

• Forward! firmware (for example, s-Par® firmware) supports the enterprise partition platform as a whole. When necessary, a Unisys service representative will apply updates and patches to the Forward! firmware. You should not make any changes to the firmware unless explicitly instructed to do so by Unisys Corporation.

Operating Environment of the FMP

• You should back up the Fabric Manager database and configuration files after completing initial configuration and whenever the configuration is changed. For more information, see 18.1 Backing Up Fabric Manager.

• You should not install any other applications on the Forward! Management Platform.

• When necessary, a Unisys service representative will apply updates to the Forward! Fabric Management Platform’s firmware (for example, updates to the Forward! Fabric Manager).

• If updates and patches to the Fabric Management Platform’s operating system are necessary, a new level of the Fabric Manager will be created, and you will be instructed to upgrade to it.

  If you choose to apply operating system patches (such as security patches) yourself, this is at your own risk.

• You may install and run anti-virus software on the Fabric Management Platform.

• If you make other changes to the Fabric Management Platform operating environment than the ones described above, such changes are at your own risk.

Service Partitions

A service partition is a pre-populated, pre-configured partition whose only role is to provide a service to other partitions. A service partition is manufactured and delivered as an appliance from Unisys Corporation. You do not need to alter the software on the service partition in any way, and you should not do so.
3.5. Customer-Supplied Hardware

The Forward! fabric hardware does not include keyboard, video and mouse. Typical Forward! fabric administration and operations tasks are performed remotely by accessing the Forward! Fabric Manager (FFM) on the Forward! Fabric Management Platform (FMP) through the network, and keyboard, video and mouse hardware is not supplied by Unisys with the customer order.

For installation occasions, the customer will need to permit use of the Unisys service representative’s laptop. For servicing occasions that need a physical connection with the cabinet complex, the customer will need to either permit use of the service representative’s laptop, or provide keyboard, video and mouse hardware, an external personal computer, or a laptop for the service representative.

Notes:

- The customer may implement a LAN-based keyboard, video and mouse solution.
- Older video monitors may not support the video resolution of the graphical interface of the FMP.
Section 4
Getting Started with User Interface

This section provides the information on Forward! Fabric Manager user interface and Fabric Management Platform in following topics:

- 4.1 Forward! Fabric Manager User Interface
- 4.2 Viewing Software Update Information
- 4.3 Forward! Fabric Management Platform (FMP)

4.1. **Forward! Fabric Manager User Interface**

The Forward! Fabric Manager (FFM) is designed to both simplify and centralize nearly all of your day-to-day management tasks. The user interface allows operators and administrators to manage components of a fabric. The Fabric Manager has the following capabilities:

- **Managing Platforms**: Fabric Manager allows you to efficiently configure and manage enterprise partition platforms in the fabric. Using the Fabric Manager, you can do the following:
  - Discover the platform.
  - Set and edit initial configuration of the platform.
  - Perform operations on the platform such as powering-on, powering off, shutting down, and so on.
  - Configure the console settings, which include network settings, user authentication, configuring and managing the console directory services, and firmware updates.
  - View the platform health status.

- **Managing Partitions**: Fabric Manager allows you to manage partition images on a platform. Using the Fabric Manager, you can do the following:
  - Commission a partition image. The commissioning process checks the availability of resources, installs the OS image on the selected partition image, and starts the partition image.
  - View the partition image summary.
  - Start and stop the partition images.
  - Add multiple OS images to a partition chassis.
  - Edit the partition image summary.
- Resize the partition image size.
- Decommission a partition image.

- **Managing Events:** Fabric Manager logs the events that occur from different components of the fabric and management operations performed by the user. Using the Fabric Manager, in the Events console, you can do the following:
  - View the events.
  - Filter the events.
  - Accept, close, and reopen the events.
  - Resend failed Call Home events.
  - Edit the event log retention period.

### 4.1.1. Understanding the *Forward!* Fabric Manager User Interface

*Table 4–1. Fabric Manager User Interface Components*

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Forward!</em> fabric</td>
<td>It is a set of all the platforms (EPPs) and associated partition images. All the partitionable EPPs and nonpartitionable EPPs that are part of the fabric are listed under the system. Fabric Manager displays <em>Forward!</em> Fabric as the default name for the fabric. <strong>Note:</strong> Based on your needs, you can change the default system (fabric) name. The “<em>Forward</em>-System” is synonymous to the default system name you define.</td>
</tr>
</tbody>
</table>
Table 4–1. Fabric Manager User Interface Components (cont.)

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform</td>
<td>Displays the type of the platform and its current state.</td>
</tr>
<tr>
<td>Partition image</td>
<td>Displays all the partition images and their current state.</td>
</tr>
<tr>
<td>Server Health Status</td>
<td>Displays health status of Fabric Management Platform.</td>
</tr>
<tr>
<td>Info Pane</td>
<td>Displays the help based on the context.</td>
</tr>
<tr>
<td>High Availability Status</td>
<td>Displays the status of the High Availability cluster.</td>
</tr>
</tbody>
</table>

4.1.2. Signing into Forward! Fabric Manager User Interface

You can sign in to the Fabric Manager user interface by using the credentials provided by the administrator.

The supported browsers for accessing the Fabric Manager user interface are
- Firefox version 29 and later
- Internet Explorer 9, Internet Explorer 10, and Internet Explorer 11
- Google Chrome version 35 and later

The minimum screen resolution supported to view the Fabric Manager user interface is 1280 x 1024.

**Caution**

Multiple site administrators or operators attempting to issue simultaneous partition or platform commands against the same set of resources by using the separate Fabric Manager browser instances can lead to undesirable results. Activities must be coordinated to avoid the undesirable results.

**Prerequisite:**
- The FMP public LAN IP address on the customer corporate LAN—recorded during fabric installation—is available. If you have two Fabric Management Platforms configured as a high availability cluster, be sure to use the floating FMP public LAN IP address so that you are connecting to FFM on the active FMP.
- Your account is activated by the Field Engineer.

To sign in to the Fabric Manager user interface...
1. Type the Fabric Manager IP address in a browser.
   The Fabric Manager sign in page appears.

2. Type the email address and password and then click **Sign In**.
   The Fabric Manager sign in page appears.

**Notes:**

- **It is not recommended to access the Fabric Manager and its features on multiple browser tabs in a single user session.**
- **The Forward! Fabric Manager user interface will prompt you to change the password when you login to the Fabric Manager the first time. The default user credentials are as follows:**

<table>
<thead>
<tr>
<th>User ID</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:forwardadmin@unisys.com">forwardadmin@unisys.com</a></td>
<td>Forwardadmin@1</td>
</tr>
<tr>
<td><a href="mailto:administrator@unisys.com">administrator@unisys.com</a></td>
<td>Administrator@1</td>
</tr>
<tr>
<td><a href="mailto:operator@unisys.com">operator@unisys.com</a></td>
<td>Operator@1</td>
</tr>
<tr>
<td><a href="mailto:observer@unisys.com">observer@unisys.com</a></td>
<td>Observer@1</td>
</tr>
</tbody>
</table>

**Note:** By default, all the default users are deactivated except the user forwardadmin@unisys.com.

- **User account gets locked automatically on five consecutive login failures. It gets unlocked automatically after 30 minutes. On or after the sixth login attempt within lock-in period (30 minutes), a lock message appears. If you want to unlock the account before this lock-in period, contact Administrator.**
- **If the Fabric Manager application browser session is left unattended for 30 minutes, it automatically gets terminated. A warning message is displayed in the browser, providing you an option to extend the session for another 30 minutes.**

To log out from the user interface, click **Sign Out** at the right corner.

### 4.1.3. Selecting Preferred Language in Fabric Manager User Interface

The FFM UI supports English (US) and Japanese languages. By default, the language is set to English (US).

To change the language

1. Logon to the Fabric Manager user interface. See **4.1.2 Signing into Forward! Fabric Manager User Interface** for instructions.

2. Click and select the required language, for example, Japanese.
   The Fabric Manager user interface is displayed in the selected language.
4.1.4. Understanding the Info Pane

Info Pane is an embedded help system available in the Fabric Manager user interface. The content of the Info Pane displays help content about the tab that you are currently working on and the possible tasks that you can perform here. It also displays any particular best practice or recommendation that might be useful to you.

Following are the advantages of Info Pane:

- It minimizes navigation in the UI and helps you to fetch appropriate information.
- The content of Info Pane changes dynamically as you navigate through the tabs.
- It provides information about the specific UI page that you are on.

To launch the Info Pane, click in any tab of Fabric Manager user interface.

Info Pane slides out and displays the information relevant to the selected UI page.
4.2. Viewing Software Update Information

You can view the following parameters of the Fabric Manager software:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FFM Current Version</td>
<td>Current version of the Fabric Manager.</td>
</tr>
<tr>
<td>ISO version</td>
<td>ISO version of the Fabric Manager.</td>
</tr>
<tr>
<td>Last Updated on</td>
<td>Date on which the Fabric Manager software was installed on a HA node in the MM-DD-YYYY-HH:MM:SS format.</td>
</tr>
<tr>
<td>Operating System</td>
<td>OS version running on a HA node; for example, SLES 11 SP3.</td>
</tr>
<tr>
<td>HA Extension</td>
<td>Information about the HA extension provided by the OS; for example, SLEHA 11 SP3 or SLES HA SP3.</td>
</tr>
</tbody>
</table>

To view the update information for the Fabric Manager software:

1. Click **Manage System**.
   - The **Manage System** and **Details** panes appear.

2. Under **Details**, click the **Software** tab.
   - The **Version Info.**, **Images**, and **Blueprints** tabs appear.

3. Click the **Version Info.** tab.
A list of parameters for both Master and Slave FMPs appears. To know more about Master, Slave and High Availability, see Section 8, Managing the Fabric as a Whole.

4.3. **Forward! Fabric Management Platform (FMP)**


- Is a computer equipped with Intel Xeon (E5-2407 2.2GHz 4c) instruction processors
- Runs the Linux operating system
- Communicates with the enterprise partition platforms over the Forward! Management LAN (Ethernet)
- Provides the Web browser-based management user interface to the Forward! fabric, called the Forward! Fabric Manager. This user interface enables you to manage every enterprise partition platform and partition in the fabric.

4.3.1. **Signing into Forward! Fabric Management Platform**

There might be situations where you may need to login to the Fabric Management Platform.

**Prerequisite:** IP address of the Fabric Management Platform is known.

You can access and sign in to the Fabric Management Platform by using Remote Desktop Protocol (RDP) client software; for example, Remote Desktop Connection on a Windows computer. The credentials are administrator/Administer4me.

4.3.2. **Changing User Password**

You must change the default user password of Partition Desktop.

To change the password

1. Logon to the Fabric Management Platform desktop, and open a new terminal session as a root user.
   (If you are connecting remotely, use a tool like PuTTY or the remote desktop function of the Fabric Management Platform, and logon as root user. The root user login is root/Administer4Me. Similarly you can login as administrator or operator.)

2. Type `passwd`.
   The prompt appears.

3. Type the required password.

   **Note:** The new password must contain at least one uppercase and one lower case character, one number and one special character as per the following list:
   - **Characters:** Lowercase “a” to “z” and uppercase “A” to “Z”.
   - **Numbers:** 0 to 9
The password is changed successfully.

### 4.3.3. Viewing Forward! Fabric Manager Server Health

The Fabric Manager server health pane displays the health status of the Fabric Management Platform itself. Health status of the following resources are displayed:

- **CPU**
- **Memory**
- **Swap**: It is the memory space used when the physical memory (RAM) is full. If the system needs more memory resources and the RAM is full, inactive space from memory is moved to the swap space.
- **Disk**

This pane provides information such as the health status, percentage utilization, and whether the resource is running or in a stopped status.

To view the Fabric Manager server health:

1. On the Fabric Manager user interface, click **Manage System** on the left pane and expand `<Forward-System>`.
   
   The **Details** screen appears on the right pane.
   
2. On the **Details** pane, click

   The **FFM Server Health** pane slides out and health information appears.
The following table provides various states of the Fabric Management Platform and their threshold values.

<table>
<thead>
<tr>
<th>FFM Server Health Status Icon</th>
<th>Server Health Status</th>
<th>Parameters</th>
<th>Description</th>
<th>Threshold Value (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Normal</td>
<td>CPU (Used)</td>
<td>CPU usage</td>
<td>1–69</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Memory (Used)</td>
<td>Memory usage</td>
<td>1–94</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Swap (Free)</td>
<td>Swap space</td>
<td>&gt;20</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Disk (Free)</td>
<td>Disk space</td>
<td>&gt;15</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Warning</td>
<td>CPU (Used)</td>
<td>CPU usage</td>
<td>70–79</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Memory (Used)</td>
<td>Memory usage</td>
<td>95–98</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Swap (Free)</td>
<td>Swap space</td>
<td>11–20</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Disk (Free)</td>
<td>Disk usage</td>
<td>11–15</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Critical</td>
<td>CPU (Used)</td>
<td>CPU usage</td>
<td>&gt;80</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Memory (Used)</td>
<td>Memory usage</td>
<td>&gt;99</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Swap (Free)</td>
<td>Swap space</td>
<td>&lt;10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Disk (Free)</td>
<td>Disk usage</td>
<td>&lt;10</td>
</tr>
</tbody>
</table>

### 4.3.4. Viewing Fabric Manager High Availability Status

In a *Forward!* Enterprise configuration, two Fabric Management Platform nodes are configured as high availability (HA) cluster. One of the Fabric Management Platforms in a cluster serves as master node and the other serves as slave node. You can view the status of master node and slave node on the Fabric Manager user interface.

The following figure displays the high availability status displayed for each of the platforms.
The following table describes the HA-related information displayed on the Fabric Manager user interface.

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FMP 1</strong></td>
<td>First node of the HA cluster. Second node is indicated as <strong>FMP 2</strong>.</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>Name of the HA node. This is configured while setting up the HA cluster.</td>
</tr>
</tbody>
</table>
### Status

Status of the HA node. This can be **Master**, **Slave**, or **Unknown** based on the node configuration. Master is indicated by ⭐ and Unknown is indicated by ?.

### Cluster Service

Status of the cluster services. This can be one of the following:

- **Online** (✔) – All the services on both the nodes are running.
- **Offline** (❌) – All the services or resources on the node are stopped.
- **Unreachable** – Node is unreachable.
- **Maintenance** (🛠️) – The node is set to maintenance mode. In this state, the Fabric Manager allows you to only edit the node configurations. You cannot manage any of the node resources.
- **Standby** – All the resources are stopped and moved to another node.

### Replication Status

The status of the failover operation. This can be one of the following:

- **Up-to-date** (✔) – The data is successfully moved to another node.
- **Disk State Unknown** – Status of the disk to which data needs to be transferred is unknown.
- **Unknown** (❓) – Status of the data transfer is unknown
- **Unreachable** – Other node is not accessible for data transfer.
UI Element Description

(Displaying the health status of nodes)

Displays the health status of nodes based on the severity. The status can be one of the following:

- Critical
- Warning
- Unknown
- OK

*Note:* The slider icon changes based on all health status severity conditions, that is, Critical, Warning, Unknown, and Ok.

To view the Fabric Manager HA status:

1. Click **Manage System**.
   
The Manage System and Details panes appear.

2. On the Details pane, click .
   
The FFM High Availability Status pane slides out and the status information appears.

The following table describes the different statuses of the FFM HA:

<table>
<thead>
<tr>
<th>FFM High Availability Status Icon</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="icon" /></td>
<td>Ok</td>
<td>Both the FMP nodes are running properly.</td>
</tr>
<tr>
<td><img src="image" alt="icon" /></td>
<td>Warning</td>
<td>Status of one of the nodes is <strong>Ok</strong> or <strong>Unknown</strong> and the other node is <strong>Warning</strong>.</td>
</tr>
<tr>
<td><img src="image" alt="icon" /></td>
<td>Critical</td>
<td>One of the nodes is in <strong>Critical</strong> state.</td>
</tr>
</tbody>
</table>
### FFM High Availability Status

<table>
<thead>
<tr>
<th>FFM High Availability Status Icon</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Unknown Icon" /></td>
<td>Unknown</td>
<td>Both the nodes are in <strong>Unknown</strong> state.</td>
</tr>
</tbody>
</table>
Section 5
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.

- 5.1 Cabling the Forward! Fabric Management Platform to Your Network
- 5.2 Cabling Enterprise Partition Platforms to Your Network
- 5.3 Installing Operating Systems for Windows and Linux Partitions
- 5.4 Updating the Forward! Fabric Manager Certificate
- 5.5 Commissioning a Partition Image
- 5.6 Starting a Partition Image
- 5.7 Implementing Security Best Practices
- 5.8 Backing Up Your Configuration

5.1. Cabling the Forward! Fabric Management Platform to Your Network

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

*Note:* PCIe slot 1 port C is named eth-pub0, and PCIe slot 1 port D is named eth-pub1.
5.2. Cabling Enterprise Partition Platforms to Your Network

For non-partitionable 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 Forward! Fabric Manager, 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.

---

**Figure 5–1. Physical Location of Ports for 2-Socket EPP with 3 Quad-Port 1GbE NICs and 3 Dual-Port 8Gb Fibre Channel HBAs**

---

**Figure 5–2. Physical Location of Ports for 2-Socket EPP with 3 Quad-Port 1GbE NICs and 3 Quad-Port 8Gb Fibre Channel HBAs**
Figure 5–3. Physical Location of Ports for 2-Socket EPP with 3 Dual-Port 10GbE NICs and 3 Dual-Port 8Gb Fibre Channel HBAs

Figure 5–4. Physical Location of Ports for 2-Socket EPP with 3 Dual-Port 10GbE NICs and 3 Quad-Port 8Gb Fibre Channel HBAs

Figure 5–5. Physical Location of Ports for 4-Socket EPP with 4 Quad-Port 1GbE NICs and 4 Dual-Port 8Gb Fibre Channel HBAs
Figure 5–6. Physical Location of Ports for 4-Socket EPP with 4 Quad-Port 1GbE NICs and 4 Quad-Port 8Gb Fibre Channel HBAs

Figure 5–7. Physical Location of Ports for 4-Socket EPP with 4 Dual-Port 10GbE NICs and 4 Dual-Port 8Gb Fibre Channel HBAs
5.2.1. Mapping HBA and NIC Ports in OS to Physical Ports

When configuring your enterprise Windows and Linux operating system partitions on partitionable enterprise partition platforms, you may need to identify HBA and NIC slots and ports as displayed in the device manager user interface of the operating systems and map them to the physical slots and ports of the enterprise partition platform. Refer to the information in Client Technical Bulletin (CTB) 6948 or Technical Information Bulletin (TIB) 6919.

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

The Support Site page for the product appears.

3. Click Recent Alerts.

The Recent Alerts page for the product appears.

4. Depending on your user privileges, locate either Client Technical Bulletin (CTB) 6948 or Technical Information Bulletin (TIB) 6919, and then click the link.

The Forward! Errata for v2.0 page appears.

5. Under the Operating Considerations section, locate and expand the headline User needs documentation to map OS visible HBA/NIC slots/ports to physical slots/ports.

6. Refer to the information and link in the Workaround section.
5.3. Installing Operating Systems for Windows and Linux Partitions

For non-partitionable enterprise partition platforms, install one of the supported customer-supplied operating systems. For more information, see 6.4 Installing a Customer-Supplied OS on a Non-Partitionable Enterprise Partition Platform.

For partitionable enterprise partition platforms, depending on the source for your operating system images, do one of the following:

- If you are installing one of the supported customer-supplied operating systems, create the desired operating system images from your own operating system installers to upload to the platform, and then use Forward! Fabric Manager to commission a partition image that uses your operating system on that platform. For more information, see 6.3 Installing a Customer-Supplied Windows or Linux OS on a Partitionable Enterprise Partition Platform.

- If you are installing one of the Unisys-supplied operating systems,
  1. Use Forward! Fabric Manager to commission a partition image with the desired operating system. For more information, see 5.5 Commissioning a Partition Image.
  2. If the status of the partition image is not RUNNING, start the partition image. For more information, see 5.6 Starting a Partition Image.
  3. Complete initial configuration of the operating system. For more information, see 6.1 Completing Installation and Configuration of a Unisys-supplied Windows Partition Image or 6.2 Completing Installation and Configuration of a Unisys-supplied Linux Partition Image.

5.4. Updating the Forward! Fabric Manager Certificate

The Fabric Management Platform is shipped with a self-signed certificate and a default RSA keypair in order for initial operations to be secured by SSL/TLS. Unisys recommends that you generate a new RSA keypair and request a certificate from a trusted authority to replace the default that is shipped with the platform.

*Note:* In the following procedure, `#` is represented as a command prompt. You do not need to type it.

To update the Forward! Fabric Manager (FFM) certificate, refer to the following instructions:

1. Launch a virtual console from the FMP platform management console and log in as root.
2. Navigate to the “ssl” directory, and enter the following command:
   
   ```bash
   # cd /usr/local/ffm/apache2/conf/ssl
   ```
3. 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
```

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 4.*
- *If this step did not require the entry of a passphrase, continue to step 5.*

4. 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
```

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

**Note:** The certificate must be in PEM format in order for step 6 to work. *If the certificate is not in PEM format, use the openssl x509 command to convert the certificate to PEM format.*

6. Enter the following command to export the certificate received from CA or self-signed certificate created in step 3 to “.pfx” format:

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

The localhost.pfx file is created.

7. 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.

8. Enter the following command to restart the FFM services:

```
# rcffmservices restart
```

The FFM services are restarted.

5.5. Commissioning a Partition Image

Ensure that the required resources such as blueprint and gold image are available. See 3.1 Partition Planning for more information. Additionally, the Fabric Manager user interface provides information about the different partition images that you can commission on a particular platform. See 11.2 Viewing Configuration Information of a Platform for more information.
Commissioning a Partition Image

Notes:

• 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 B, Worksheet for Commissioning, to learn more about the worksheet.

• 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, click Manage System on the left pane, expand <Forward-System> and then select the required platform on which you want to commission the partition image.

   Details screen appears on the right pane.

2. On the Details pane, click Commission.

   Alternatively, click the arrow next to the platform and click Commission.

   A message informing that the system is discovering the resources for the commissioning appears.

   After the discovering the required resources to commission a partition image, the Commission window appears.

3. In the Select Blueprint tab, select the desired blueprint and click Next.

   Note: The Next button is enabled only when a blueprint is selected.

4. In the Set Basic Info. tab, provide appropriate information in the following fields:

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

     Note: The maximum length of the partition image name can be up to 15 alphanumeric characters along with “-”. The name cannot start with the character “-“.

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

     Note: The Host Computer Name should be unique across the fabric if partition images are connected within the same customer LAN subnet.

   • Description: Type a description for the partition image.

     Note: Provide a meaningful description for the partition image. The maximum length of the 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.

5. Click Next.
6. In the **Allocate Resource** tab, select the appropriate values in the following fields:

- **Partition Chassis**: Choose the appropriate partition chassis; for example, Chassis-B.

- **Partition Size**: Choose the appropriate partition size; for example, Medium. The available options are based on the value that you have selected in the **Partition Chassis** field.

  For example, if you have selected **Chassis-A** in the **Partition Chassis** field, the available partition size could be **Small**, **Medium**, **Large**, and **Maximal**. If you have selected **Chassis-B** in the **Partition Chassis** field, the available partition size could be **Small** and **Medium**.

- **Configuration of <name of the chassis and partition size value>**: Table **Table 5–1** displays the various fields under this section. These fields are automatically populated based on the values that you have selected in the **Partition Chassis** and **Partition Size** fields:

  **Table 5–1. Partition Chassis and Partition Size Fields and Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cores</td>
<td>Displays the number processor cores assigned for the partition image.</td>
</tr>
<tr>
<td>Memory (&lt;x-y&gt; GB)</td>
<td>Displays the default memory allocated for the partition image. This is an editable field. You can also choose a different memory size. x and y denote the minimum and maximum memory sizes (in GB) that you can choose. Information about the remaining memory in the platform is displayed along with this field. You can use the increment and decrement operator to increase and decrease the memory beyond the default memory. This value changes automatically based on the memory size that you have selected.</td>
</tr>
<tr>
<td>NIC Ports and HBA Ports</td>
<td>Displays information about the NIC and HBA ports. Click the Show Legends tab to learn more about the displayed information.</td>
</tr>
</tbody>
</table>

**Note**: You can view the vendor and the device type details of a particular port. If you click a port, the vendor and device type information of the selected port appears under the **Details: Slot** section.
The following is an example of the **Allocate Resource** tab:

- **LUN Selection**: Choose the desired LUN size.

  **Notes:**
  - A LUN size of at least 60 GB if you are commissioning a Windows partition image from Unisys-supplied images.
  - A LUN size of at least 20 GB if you are commissioning a Linux partition image from Unisys-supplied images.
  - 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. For more information, see 6.3.5 Creating a Customer-Supplied Linux Operating System Image.

- **Enable Hyper-Threading (HT):** If you select this check box, two logical processors per core are selected. By default, the HT option is disabled for 4S platforms and enabled for 2S platforms.

7. Click **Next**.

8. In the **Set State & Credentials** tab, select the appropriate options in the following fields:

   - **Initial State (Platform Reboot):** Enables you to identify whether or not the partition image is started after a platform reboot. The available values are **Running** and **Stopped**. The default value is **Running**.
     
     **Note:** The **Initial State** value does not apply to the partition images that are currently disabled.

   - **Login Credentials:** Enables you to type the appropriate password in the **Password** field and confirm the password in the **Confirm Password** field. These fields are 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 was captured as part of the image you created. Use that information to access your Linux partition image; the input in the host computer name and password fields during commissioning is ignored.

9. Click **Next**.

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

10. Click **Submit**.

   A message informing you that the commissioning process will begin shortly appears.

11. Click **OK**.

   Commissioning of the new partition image begins. After the commissioning is complete, the newly commissioned partition image appears in the Manage System pane under the respective platform. You can also monitor the progress of the commissioning process by referring to the logs being generated under the **Events** tab.

You can set up the Windows and Linux operating environments after Commissioning a partition image. See 6.1 Completing Installation and Configuration of a Unisys-supplied Windows Partition Image and 6.2 Completing Installation and Configuration of a Unisys-
supplied Linux Partition Image for information.

5.6. Starting a Partition Image

**Prerequisite:** The EPP has to be powered on and the desired partition image is in a stopped state.

To start a partition image

1. On the Fabric Manager user interface click **Manage System** on the left pane, expand `<Forward-System>` to view various platforms.
2. Expand the desired platform and then click the partition image that you want to start.
   
   The **Details** pane displays the information about the selected partition image.
3. Click **Start**.
   
   The status of the partition image changes to **RUNNING**.

5.7. Implementing Security Best Practices

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

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

5.8. Backing Up Your Configuration

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 **18.1 Backing Up Fabric Manager**.
Section 6
Installing and Configuring Operating Systems

Depending on the type of enterprise partition platform, the operating system, or the source of the operating system image, refer to the appropriate sections for more information on installing and configuring your operating system.

- 6.1 Completing Installation and Configuration of a Unisys-supplied Windows Partition Image
- 6.2 Completing Installation and Configuration of a Unisys-supplied Linux Partition Image
- 6.3 Installing a Customer-Supplied Windows or Linux OS on a Partitionable Enterprise Partition Platform
- 6.4 Installing a Customer-Supplied OS on a Non-Partitionable Enterprise Partition Platform
- 6.5 Configuring Partition Images to Boot From an External Storage Device
- 6.6 Configuring and Maintaining Operating Environments on Enterprise Partition Platforms
- 6.7 Obtaining and Installing Interim Corrections (ICs)


If 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. 6.1.1 Completing Windows OS Installation
2. 6.1.2 Changing Credentials for Default Windows Administrator Account
3. 6.1.3 Configuring Your Windows Boot Disk
4. 6.1.4 Configuring Customer Corporate LAN (Public LAN) Connections for Enterprise Partition Platforms
5. 6.1.5 Configuring Storage Area Network Connections for Enterprise Partition Platforms
6. 6.1.6 Completing Windows Configuration
6.1.1. 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 Fabric Manager to launch a console for the desired partition. (See 13.3 Accessing a 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 the setup and automatically logs in using the default administrator credentials specified during commissioning.

6.1.2. 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.

6.1.3. Configuring Your Windows Boot Disk

When you commission a Windows partition image, no matter the size of the virtual disk (LUN) you choose, the boot volume where the operating system is installed (C:) is automatically configured to be a single primary partition that is approximately 60 GB. If your virtual disk is larger than 60 GB, use Windows Disk Management to either extend the C: partition or to configure additional disk partitions.

**Note:** In Windows Disk Management, you will see five additional disks—Disk 1 through Disk 5—that are marked as offline. These are virtual disks used by Unisys. Do not alter them.
6.1.4. 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.

**Notes:**

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

- *If your environment includes both Linux and Windows partition images, Unisys recommends using the Host Data LAN when addressing all partition images. If your environment only includes Linux partition images, Unisys recommends using the Inter-partition LAN.*

To identify the ports allocated to your partition image, use the Forward! Fabric Manager 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.

6.1.5. 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 fiber channel HBAs in your Forward! fabric, you may use the Emulex OneCommand Manager (OCM) utility. A qualified version of the utility for the Forward! fabric is available from the Unisys Product Support website.

To identify the ports allocated to your partition image, use the Forward! Fabric Manager 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.
6.1.6. Completing Windows Configuration

Activate Your Windows Operating System License

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

- 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.

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.

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

If 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. 6.2.1 Completing Linux OS Installation
2. 6.1.4 Configuring Customer Corporate LAN (Public LAN) Connections for Enterprise Partition Platforms
3. 6.1.5 Configuring Storage Area Network Connections for Enterprise Partition Platforms
4. 6.2.4 Completing Linux Configuration

6.2.1. 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 Fabric Manager to launch a console for the desired partition. (See 13.3 Accessing a 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.

4. When prompted to change the root password, enter a new password.

### 6.2.2. 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.

**Notes:**

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

- If your environment includes both Linux and Windows partition images, Unisys recommends using the Host Data LAN when addressing all partition images. If your environment only includes Linux partition images, Unisys recommends using the Inter-partition LAN.

To identify the ports allocated to your partition image, use the Forward! Fabric Manager 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.

### 6.2.3. 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 fiber channel HBAs in your Forward! fabric, you may use the Emulex OneCommand Manager (OCM) utility. A qualified version of the utility for the Forward! fabric is available from the Unisys Product Support website.

To identify the ports allocated to your partition image, use the Forward! Fabric Manager 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.
6.2.4. 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.

6.3. Installing a Customer-Supplied Windows or Linux OS on a Partitionable Enterprise Partition Platform

To install a customer-supplied operating system on a partitionable enterprise partition platform,

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

   For more information, see
   - 6.3.1 Customer-Supplied Windows or Linux Operating System Images on Partitionable Enterprise Partition Platforms
   - 6.3.2 Understanding Customer-Supplied Windows Operating System Images
   - 6.3.3 Understanding Customer-Supplied Linux Operating System Images
   - 6.3.4 Creating a Customer-Supplied Windows Operating System Image
   - 6.3.5 Creating a Customer-Supplied Linux Operating System Image

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

   For more information, see 6.3.6 Uploading Customer-Supplied Operating System Images to Fabric Manager.

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

   For more information, see 5.5 Commissioning a Partition Image.

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

If the operating system is supported, you can create operating system 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 images from the Windows operating system installation media that you obtain from your operating system vendor, for example, an ISO image or DVD. The installation media is directly 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 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 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.

6.3.2. Understanding Customer-Supplied Windows Operating System Images

You use the Customer-Supplied OS Toolkit for Windows to create operating system images from your own Windows operating system installation media. The toolkit contains a utility that enables you to create an image that you can copy to the Fabric Management Platform with the required corresponding blueprint image that is included in the toolkit. You then 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.

Supported Windows operating systems are
• Windows Server 2008 R2 SP1, Enterprise Edition, x64, English
• Windows Server 2012, Standard Edition, x64, English
• Windows Server 2012 R2, Standard Edition, English

The toolkit contains the following
• IsoToWinImg.exe
  A command line utility that converts an ISO file of an operating system installer into a GUID Partition Table (GPT) disk image that is compatible with Unisys Secure Partitioning (s-Par®).
• dotnetfx45_full_x86_x64.exe
  The installer for Microsoft .NET Framework 4.5.
• Blueprint images (.img)

Three blueprint images are included:

- A blueprint for Windows Server 2008 R2 (filename starts with `CSO-W2k8r2.sp1.ee-eng-Bp`)
- A blueprint for Windows Server 2012 (filename starts with `CSO-W2k12.std-Eng-Bp`)
- A blueprint for Windows Server 2012 R2 (filename starts with `CSO-W2k12r2.std-Eng-Bp`)

Each blueprint is paired respectively to the operating system image you create using `IsoToWinImg.exe`. When you use the Fabric Manager user interface to add your operating system 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 paired blueprint during commissioning.

### 6.3.3. Understanding Customer-Supplied Linux Operating System Images

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

Supported Linux operating systems are

- SUSE LINUX Enterprise Server 11 Service Pack 3 (SLES 11 SP3)
- SUSE LINUX Enterprise Server 11 Service Pack 3 (SLES 11 SP3) for SAP applications
- Red Hat Enterprise Linux 6.4 (RHEL 6.4)
- Red Hat Enterprise Linux 6.5 (RHEL 6.5)

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—that based on open source Ubuntu software—that helps you modify (prepare) a running Linux operating system for the `Forward!` 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.
6.3.4. Creating a Customer-Supplied Windows Operating System Image

The IsoToWinImg.exe command line utility in the Customer-Supplied OS Toolkit for Windows requires a Windows computer with the following prerequisites:

- Windows 7, Windows Server 2008 R2, or later (32-bit or x64-bit)
- .NET Framework 4.5 or later
  - Version 4.5 is included in the toolkit.
- 1 GB of memory
- 10 GB of hard disk space on the local drive

Be sure to have your operating system installation media available: Copy your OS installation ISO file to your computer. If the installation media is a DVD, convert it to an ISO file using any DVD-to-ISO conversion software (for example, IsoBuster or Roxio Creator) and make sure the ISO file is available on your computer.

To create an operating system image:

1. Copy the Customer-supplied OS Toolkit for Windows to your computer and unzip it into a folder, for example, C:\CSO-Windows-Toolkit.
2. If you do not have the required .NET Framework running on your computer, install it using the .exe provided in the toolkit: Navigate to dotnetfx45_full_x86_x64.exe, double-click it, and then follow the onscreen prompts to install the .NET Framework.
3. On your Windows computer, launch a Command Prompt window.
4. At the prompt, use the cd command to navigate to the directory containing the IsoToWinImg.exe utility. For example, cd c:\CSO-WINDOWS-TOOLKIT
5. Run IsoToWinImg.exe using the following syntax:

   IsoToWinImg inputfile.iso outputfile.img <Win2012|Win2008>

   Where
   - *inputfile.iso* specifies the ISO file of your operating system installation media.
   - *outputfile.img* is the destination .img file.
   - The file name (excluding the .img extension) cannot be longer than 32 characters.
   - Win2012 or Win2008 are optional parameters.
   - The utility automatically detects operating system version; however, for the cases when it cannot find the version information, you can use this optional parameter to specify the version.

   For example:

   IsoToWinImg en_windows_server_2012_x64_dvd_915478.iso Win2012Std.img

   The utility creates the image, and reports the location and filename of the resulting .img file.
Use the Fabric Manager user interface to add the operating system image and its corresponding blueprint image to the desired platform. For more information, see 6.3.6 Uploading Customer-Supplied Operating System Images to Fabric Manager.

### 6.3.5. 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 Forward! 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 one of the following:
  - SUSE LINUX Enterprise Server 11 Service Pack 3 (SLES 11 SP3)
  - SUSE LINUX Enterprise Server 11 Service Pack 3 (SLES 11 SP3) for SAP applications
  - Red Hat Enterprise Linux 6.4 (RHEL 6.4)
  - Red Hat Enterprise Linux 6.5 (RHEL 6.5)
- 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 Forward! Environment

Before using the toolkit to create your image, prepare your Linux operating system for the Forward! 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. Be sure the following packages are installed from your operating system installation media.

   Note: When you run the Unisys-CSO-prep.sh script and it does not detect the packages marked with an asterisk (*), the script installs the missing packages.

   - For SLES
     - gcc
     - gcc-fortran (available on SUSE SDK DVD #1)*
     - gcc43-fortran (available on SUSE SDK DVD #1)*
     - libgfortran3 (available on SUSE SDK DVD #1)*
     - libgfortran43 (available on SUSE SDK DVD #1)*
     - kernel-source
     - libnl-32bit*
     - libnl-devel (available on SUSE SDK DVD #1)*
     - libquadmath0 (available on SUSE SDK DVD #1)*
     - libquadmath46 (available on SUSE SDK DVD #1)*
     - kernel-devel
     - make
     - perl
     - tcl
     - tk

   - For RHEL
     - gcc
     - Make
     - tcl*
     - tk
3. Use the Unisys-CSO-prep.sh script in the toolkit to install additional 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 cursory check for required packages. If dependencies are missing, the script attempts to install them, and reports an error if installation does not succeed.

   *Note: The check is performed at a high level and may not detect all missing dependencies.*

   The script then installs the following:
   - Dynamic Kernel Module Support (DKMS) software
   - Mellanox InfiniBand drivers
   - Unisys Secure Partitioning (s-Par®) drivers
   - Usysreport – a Unisys diagnostic tool
   - **Forward!** Hardening Tool for Linux

### Capturing a Snapshot of the Linux Operating System

After preparing your Linux operating system for the **Forward!** 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 toolkit ISO image or DVD automatically boots into a command line environment. Note that 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.

2. Run the image-capture.sh script to capture a snapshot of your prepared Linux operating system. The script creates files to be used later to create a gold image. The script requires information to create the snapshot files, and interactively prompts for information that was not previously provided through a command line option. If you run the script in quiet mode (by specifying the q|Q option), it uses the default value for any information that was not previously provided through a command line option.

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

To create snapshot files and a directory to contain them, run the image-capture script by entering `image-capture.sh` and providing the following information either interactively, or through command line options:

- **<c|C option>**
  The capture format for how the script captures the device. Valid values are
  - DD – The script performs a byte-to-byte copy of the disk using the Linux dd command.
  - FS – The script capture the file systems on each partition.
  The default is FS.

**Notes:**
- If the operating system you are attempting to capture contains LVM partitions, you must specify the DD format.
- If the operating system you are attempting to capture has selinux set to enforcing, you must specify the DD format.
- If you specify the DD format, during commissioning, you must select a disk of the same size or larger than the size of the disk you are capturing.

- **<d|D option>**
  The kernel name of the device that the script should capture, for example, sdc.

- **<f|F option>**
  The name for files that the script creates. The script appends the partition number to this name. The default is Linux version-version of image.

- **<o|O option>**
Installing a Customer-Supplied Windows or Linux OS on a Partitionable Enterprise Partition Platform

The full path name for the directory the script should use to store the files it creates. The default is /tmp/CapturedImage.

- <qQ option>
  Quiet mode indicates the script should not query for input. If specified, the script uses the default value for required information, unless an alternative value is previously provided with a command line option.

- <vV option>
  The version number for the image. This number will be stored in the /etc/image version file of your operating system. The format must be x.x.x.xxx where x is a numeric digit. The default is 1.0.0.000.

**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, run the mkCSOimage script to convert the snapshot into a customer-supplied operating system image and create the corresponding blueprint.

The script interactively prompts for the information required to create the images. You may run the script non-interactively by specifying command line option parameters to provide the information before the script runs. If you do not specify all needed parameters, the script prompts for the missing information.

To convert the snapshot into an image and create a corresponding blueprint, in the terminal session, enter **mkCSOimage**, followed by the following parameters (if desired):

- <bB option>
  The full path name for the directory containing the blueprint template and associated files. The default is /opt/unisys/CSO-Blueprint.

- <nN option>
  The image number for the image you are creating. The value must be a number from 1 to 6. Duplicate image numbers are not supported on the same enterprise partition platform. The default is 1.

- <dD option>
  The description of the image you are creating and its blueprint. This description is displayed on the Fabric Manager user interface, and must be less than 32 characters. The default is CSO-Linux-Image-x, where x is the image number.

- <iI option>
  The full path name for the directory that you created using the image-capture script when you captured a snapshot of your operating system.
The full path name for the directory to store the image you are creating and its blueprint.

The version number for the image you are creating and its blueprint. The format must be x.x.x.xxxxx where x is a numeric digit. The default is 1.0.0.0001.

The full path name for the directory to temporarily store working files and scripts. The default is /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 6.3.6 Uploading Customer-Supplied Operating System Images to Fabric Manager.

6.3.6. 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 12.3.2 Adding a Gold Image and 12.2.2 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 5.5 Commissioning a Partition Image for more information.
6.4. Installing a Customer-Supplied OS on a Non-Partitionable Enterprise Partition Platform

To install a customer-supplied operating system on a non-partitionable enterprise partition platform:

1. If you do not have credentials with the following parameters for the platform management card of the non-partitionable 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 6.4.1 Obtaining and Installing Drivers and Firmware.

3. Copy your operating system installation media image to the Fabric Management Platform.
   For more information, see 6.4.2 Making Operating System Installation Media Image Available for Installation.

4. Install and configure your operating system.
   For more information, see one of the following:
   - 6.4.3 Installing and Configuring Windows Server
   - 6.4.4 Installing and Configuring SUSE LINUX 11 Service Pack 3
   - 6.4.5 Installing and Configuring Red Hat Enterprise Linux

6.4.1. 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 web site.

Note: The Unisys Product Support web site 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 Forward! if needed, and then click 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 files for.

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 non-partitionable 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 Non-Partitionable Enterprise Partition Platform**

1. Obtain Mellanox firmware 2.30.3110: Download the firmware update package from the Unisys Product Support web site.

   **Note:** All Mellanox cards in partitionable or non-partitionable partition platforms have the correct level of firmware (2.30.3110) installed before shipping from Unisys. All spare cards in the spares depots also have the correct level of firmware (2.30.3110) installed.

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

---

**6.4.2. 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 11.4 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 6.4 Installing a Customer-Supplied OS on a Non-Partitionable Enterprise Partition Platform.

5. On the Attached Media tab, set the Virtual Media Status to Attach.

Note: Remember to set the setting back to Detach when you no longer need to attach media.

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.

6.4.3. 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.

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 6.4.2 Making Operating System Installation Media Image Available for Installation for more information.

2. Ensure the RAID controller is configured with the desired LUNs.

   To view or modify the RAID configuration with the BIOS Configuration Utility: When you start the platform, use the platform management console to monitor the boot progress, and then immediately press the Ctrl and R keys simultaneously when the PowerEdge Expandable RAID Controller BIOS banner displays.

3. For Windows Server 2008 R2, obtain the drivers needed for accessing the RAID controller. See 6.4.1 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 6.4.1 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, 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.

**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**.


   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.

### Installing and Configuring Intel PROSet and NIC Network Adapters

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 **Forward!** management LAN (for example, **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. The subnet mask field is filled out automatically.


17. Click **OK** to close the Local Area Connection Properties dialog.

### Installing and Configuring Mellanox InfiniBand Adapters

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. 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, and then click **Properties**.

The Local Area Connection Properties dialog box opens.

6. 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.

7. Select **Use the following IP address**, and then type in the address the Fabric Manager displays as the IP LAN IP address for the enterprise partition platform on the summary page. The subnet mask field is filled out automatically.

8. Click **OK** to close the Internet Protocol Version 4 (TCP/IPv4) Properties dialog box.

9. Click **OK** to close the Local Area Connection Properties dialog.

10. If there is a connection for a second InfiniBand adapter (Mellanox ConnectX-3 IPoIB Adapter #2), right-click the connection, and then select **Disable**.

**Note:** Only one adapter is used because the Windows drivers do not currently support teaming on IP over InfiniBand.

### Configuring the Windows Firewall

To configure the Windows Firewall to allow ping requests through the **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**.

Configuring NMI Memory Dumps for Windows Server 2008 R2

The *Forward! 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](http://support.microsoft.com/kb/927069).

6.4.4. Installing and Configuring SUSE LINUX 11 Service Pack 3

Use the following procedures to perform a complete, basic installation and configuration of your SUSE LINUX Enterprise Server 11 Service Pack 3 (SLES 11 SP3) operating system.

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 SUSE LINUX Enterprise Server 11 documentation provided in the “docu” directory on the SLES 11 SP3 media.

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.

Installing SUSE LINUX 11 Service Pack 3

To install your SUSE LINUX Enterprise Server 11 Service Pack 3 (SLES 11 SP3) 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 6.4.2 Making Operating System Installation Media Image Available for Installation for more information.

2. 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.

   **Note:** Be aware that the screen displayed in the next step is timed. If you do not make a selection in time, wait for the server to finish booting from hard disk, and then repeat this step.
3. The SUSE LINUX Enterprise Server screen with the boot/installation options appears. Select **Installation**, and then press **Enter**.
   After a few minutes, the **Welcome** screen appears.
4. Select the language and keyboard layout you want to use.
5. Read the license agreement and select **I agree to the License Terms**.
6. Click **Next**.
   The **Media Check** window appears.
7. If you want to test the media, click **Start Check**. If the result is **OK** when the media check is complete, click **Next**; otherwise, insert new media and click **Start Check**.
   If you want to skip the media check, click **Next**.
8. Click **New installation**, and then click **Next**.
   The **Clock and Time Zone** window appears.
9. Perform any of the following steps as appropriate for your situation:
   - Select the desired **Region and Time Zone** options.
   - If you want to set the time to Coordinated Universal Time (UTC), check **Hardware Clock Set To UTC**.
   - If the date or time is incorrect, click **Change**, make the required changes, and then click **Accept**.
10. Click **Next**.
    The Server Base Scenario screen appears.
11. Choose the scenario for your server.
    If you want to install a graphical user interface, select **Physical Machine (Also for Fully Virtualized Guests)**.
    If you do not want to install a graphical user interface, select **Xen Virtualization Host (Local X11 Not Configured by Default)**.
12. Click **Next**.
    The installation continues to analyze your system. When the analysis is finished, the **Installation Settings** screen appears with a list of installer default configurations.
13. 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. Click **Partitioning** on the **Change** menu.
   b. Select **Custom partitioning (for experts)**, and then click **Next**.
   c. Under **Expert Partitioner**, select **Hard disks**, and then expand the hard disks to see the available disks.
d. Select the hard disk from which you want to boot, select the Overview tab, and then check the Disk Label field to see if the disk is labeled correctly.

e. Select the Partitions tab.

f. If the Disk Label (from step d) is not correct, then do the following:
   • Select the Expert tab on the bottom of the screen.
   • Select Create New Partition Table.
   • If a disk drive partition table window appears, select the desired type.
   • If a warning about data loss appears, click Yes.

g. To add new disk drive partitions, click the Add tab.

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.

14. Select Software from the Change menu, and then
   a. Select Infiniband (OFED).
   b. Click Details, and then select the Search tab.
   c. In the Search box, type infiniband, and then click Search.
   d. In the right pane, select infiniband-diags.
   e. Add or remove other software components as appropriate for your environment.

15. Click Accept or OK.

16. If a package that you want installed needs a license, then the appropriate license appears. Click Accept.

17. If you added a package that needs other packages to resolve dependencies, then a Changed Packages window appears. Click Continue.

18. Click Install to complete the installation settings.

A Confirm Installation screen appears.

19. If necessary, click Back to go back and make changes before the installation process begins.

20. Once the installation settings are correct, click Install.

The installation process begins.

When the initial installation phase completes, the following message appears:

   The system will reboot now.

A 10-second countdown occurs.

21. Click OK or wait until the countdown completes.

The server stops and starts.

Allow the boot/installation options menu to default to Boot from Hard Disk.
When the installation process completes, the **Password for the System Administrator** “root” screen appears.

22. Type a password of your choice, confirm it, and then click **Next**.
   
   The **Hostname and Domain Name** window appears.

23. Type the system name and the domain name information, and then click **Next**.
   
   The **Network Configuration** window appears with a list of all detected network devices.

   This screen also provides **Virtual Network Computing (VNC)**, firewall, and proxy options.

24. Configure the network devices and other network options, as necessary, and click **Next**.

   The **Test Internet Connection** window appears; the default action is to test the connection.

25. If you do not want to test the connection, select **No, Skip This Test**, and then click **Next**.

   A **Network Services Configuration** window appears.

26. Set the appropriate configuration values for CA management (a computer management tool) and the Open LDAP server, or click **Skip Configuration**, and then click **Next**.

   The **User Authentication Method** screen appears. This screen defines different methods of authentication. Local (/etc/passwd) is the default and is appropriate for most environments.

27. If necessary, select the appropriate method of authentication, and then click **Next**.

    The **New Local User** window appears.

28. If necessary, type the appropriate values in the **User’s Full Name**, **Username**, **Password**, and **Confirm Password** fields, and then click **Next**.

    The SLES 11 SP3 release notes information appears.

29. Read the release notes, and then click **Next**.

    After checking for devices, such as graphic cards, printers, and sound cards, the Hardware Configuration screen appears with a list of the devices found. If you receive a warning from the screen, click **OK**. If necessary, change the device settings.

30. Click **Next**.

    The **Installation Completed** window appears.

31. If you do not want to save a copy of this configuration for the AutoYaST tool (used to install Linux automatically), clear the **Clone This System for AutoYaST** check box.

32. Click **Finish**.

    The initial installation is now complete. Proceed to configure for SUSE LINUX kernel crash dumps.
Configuring SUSE LINUX Kernel Crash Dumps

Log in as root, and do the following:

1. Verify that the kdump and kexec-tools packages are installed by typing the following commands:
   
   ```bash
   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:
   
   ```bash
   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 and FM LAN connections, and update the UDEV persistent rules.

Proceed to configure the IP LAN connection for SUSE LINUX.

Configuring the IP LAN (InfiniBand) 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:

   ```ini
   BOOTPROTO=none
   MTU="
   STARTMODE='hotplug'
   USERCONTROL='no'
   ```
2. Create a file named `ifcfg-ib1` in the `/etc/sysconfig/network` directory with the following content:

```bash
BOOTPROTO=none
MTU="
STARTMODE='hotplug'
USERCONTROL='no'
```

3. Create a file named `ifcfg-bond0` in the `/etc/sysconfig/network` directory with the following content:

```bash
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.

4. Create a file named `routes` in the `/etc/sysconfig/network` directory with the following content:

```
Note: Do not include an entry for your enterprise partition platform—either comment out the line that references your platform number (third octet of the IP address), or do not include that line.
```

```
172.30.1.0 172.31.1.250 255.255.255.0 bond0
172.30.2.0 172.31.2.250 255.255.255.0 bond0
172.30.3.0 172.31.3.250 255.255.255.0 bond0
172.30.4.0 172.31.4.250 255.255.255.0 bond0
172.30.5.0 172.31.5.250 255.255.255.0 bond0
172.30.6.0 172.31.6.250 255.255.255.0 bond0
172.30.7.0 172.31.7.250 255.255.255.0 bond0
172.30.8.0 172.31.8.250 255.255.255.0 bond0
172.30.9.0 172.31.9.250 255.255.255.0 bond0
172.30.10.0 172.31.10.250 255.255.255.0 bond0
172.30.11.0 172.31.11.250 255.255.255.0 bond0
172.30.12.0 172.31.12.250 255.255.255.0 bond0
172.30.13.0 172.31.13.250 255.255.255.0 bond0
172.30.14.0 172.31.14.250 255.255.255.0 bond0
172.30.15.0 172.31.15.250 255.255.255.0 bond0
172.30.16.0 172.31.16.250 255.255.255.0 bond0
```

Proceed to configure the FM LAN connection for SUSE LINUX.

**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:

```bash
BOOTPROTO=none
MTU="
```
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.

4. If you have a firewall, ensure that your firewall rules allow responses to incoming pings on the FM LAN.

   Proceed to update the UDEV persistent rules for SUSE LINUX.

### 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/pci0000:00/0000:00:1c.4/0000:08:00.0/net*", NAME="eth-fmp3"
SUBSYSTEM=="net", ACTION=="add", DEVPATH=="/devices/pci0000:00/0000:00:1c.4/0000:08:00.1/net*", NAME="eth-fmp4"
```

Proceed to configure OS support of NMI generated kdumps for SUSE LINUX.

### Configuring OS Support of NMI Generated Kdumps for SUSE LINUX

The *Forward!* Fabric Manager and platform management console use a non-maskable interrupt (NMI) to force a server memory dump when you request for a dump. If you wish to use those interfaces when generating a kdump, configure operating system support for the NMI interrupt.

Log in as root, and add the following line to the `/etc/sysctl.conf` file:

```
kerneld.unknown_nmi_panic=1
```

Reboot when you complete all configuration changes.
6.4.5. Installing and Configuring Red Hat Enterprise Linux

Use the following procedures to perform a complete, basic installation and configuration of your Red Hat Enterprise Linux 6.4 (RHEL 6.4) or Red Hat Enterprise Linux 6.5 (RHEL 6.5) operating system.

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 Web site 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.

Installing Red Hat Enterprise Linux

To install your Red Hat Enterprise Linux 6.4 (RHEL 6.4) or Red Hat Enterprise Linux 6.5 (RHEL 6.5) 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 6.4.2 Making Operating System Installation Media Image Available for Installation for more information.

2. 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.

3. On the Welcome to Red Hat Enterprise 6 screen, either select Install or upgrade an existing system and press Enter, or allow the sixty second timer to expire.

4. Perform one of the following when the Welcome to Red Hat Enterprise Linux Server for x86_64 screen appears:
   • If you want to test the media, press the spacebar.
   • If you do not want to test the media, press Tab to select Skip, and then press the spacebar.

5. On the RED HAT ENTERPRISE LINUX 6 screen, click Next.
6. Select the language to use for the installation, and then click Next.
7. Select the appropriate keyboard for the system, and then click Next.
8. Select the type of storage devices involved in the installation, and then click Next.
9. The installation process checks for any previously installed versions of the Red Hat Linux operating system. If one or more versions are found, select Fresh Installation, and then click Next. If you do not see the versions listed, skip this step.
10. Enter the hostname of the computer.
11. If you wish to configure your networking devices at this time, click Configure Network to set up the appropriate networking configuration values, and then click Close when you finish your configuration changes.
12. Click Next.
13. Select the appropriate time zone. Click System clock uses UTC if appropriate, and then click Next.
14. Type and confirm a root password of your choice for the system, and then click Next.
15. On the disk partitioning screen, specify the type of installation:
   a. Select the action that the automatic partitioning process should take regarding existing disk drive partitions.
   b. Select whether you want to review and modify the disk drive partitions that are created by the automatic partitioning process, and then click Next.
   c. If there is more than one drive, select the drives to be used for this installation.
   d. If you selected the Review and modify partitioning layout option during step b, review or modify the disk drive partition configuration, and then click Next.
   e. If a format warning box appears, check the disk and click Format if it is correct.
16. In the Writing storage configuration to disk box, click Write changes to disk.
17. Optionally, select Use a boot loader password, type and confirm a boot loader password of your choice, and then click Next.
18. Select Server type and additional repositories.
19. If you want a graphical user interface, select Desktop.
20. Select Customize now, click Next, and then
   a. Select Infiniband Support.
   b. Select other packages that you want to add.
21. If you want to specify additional packages, select Customize now, and then click Next to select the desired additional packages.
22. Click Next to begin the installation.
23. Wait until a screen appears indicating that the installation is complete, and then click Reboot.
   The server stops, and then restarts.
25. Read the agreement, select **Yes, I agree to the License Agreement**, and then click **Forward**.

26. On the Set Up Software Updates screen, do one of the following:
   - If you want to register at this time, select **Yes, I’d like to register now**, and then click **Forward**.
     Complete the remaining steps to register the product.
   - If you want to register at a later time, select **No, I prefer to register at a later time**, click **Forward**, and then click **No thanks, I’ll connect later**.

27. On the Finish Updates Setup screen, click **Forward**.

28. If desired, type the appropriate information to create a new user account, and then click **Forward**.

29. Verify or modify the date and time, and then click **Forward**.

30. On the Kdump screen, click **Finish**.

31. When queried about reboot, click **No**.

The initial installation is now complete. Proceed to configure for Red Hat Linux kernel crash dumps.

## Configuring Red Hat Linux Kernel Crash Dumps

Before configuring crash dumps, determine a location in which the vmcore file (dump file) can be placed. This location can be another server, a RAW device, or a local file system that is approximately the size of the physical memory of the system.

Log in as root, and do the following:

1. Verify the kexec-tools package is installed by entering the following command:
   ```bash
   rpm -q kexec-tools
   ```
2. If the kexec-tools package is not installed, install it on the server.
3. Run the Kernel Dump Configuration utility by entering the following command:
   ```bash
   system-config-kdump
   ```
4. When the utility starts, do the following:
   a. Select **Automated kdump memory settings**.
   b. Click **Target settings** 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.
   c. Click **Filtering settings** and set the values as required.
   d. Click **Expert settings** and set the values as required.
   e. Click **Apply**.
f. On the system-config-kdump box, click OK.
g. Click File, and then click Quit.
h. Click No in response to the system reboot message.

5. Read through the kdump configuration file, and set the site-appropriate values for various parameters.

Proceed to configure the IP LAN connection for Red Hat Linux.

**Configuring the IP LAN (InfiniBand) Connection for Red Hat Linux**

Log in as root, and do the following:

1. Verify that rdma was brought up when the system booted:
   
   ```bash
   chkconfig rdma on
   ```

2. Stop the Network Manager service, and prevent it from starting during boot:

   ```bash
   service NetworkManager stop
   chkconfig NetworkManager off
   ```

3. Create a file named `ifcfg-ib0` in the /etc/sysconfig/network-scripts directory with the following content:

   ```bash
   DEVICE=ib0
   TYPE=InfiniBand
   ONBOOT=yes
   BOOTPROTO=none
   NM_CONTROLLED=no
   SLAVE=yes
   MASTER=bond0
   USERCTL=no
   HOTPLUG=yes
   ```

4. Create a file named `ifcfg-ib1` in the /etc/sysconfig/network-scripts directory with the following content:

   ```bash
   DEVICE=ib1
   TYPE=InfiniBand
   ONBOOT=yes
   BOOTPROTO=none
   NM_CONTROLLED=no
   SLAVE=yes
   MASTER=bond0
   USERCTL=no
   HOTPLUG=yes
   ```

5. Create a file named `ifcfg-bond0` in the /etc/sysconfig/network-scripts directory with the following content:

   ```bash
   DEVICE=bond0
   IPADDR=172.31.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.

6. Create a file named `/etc/modprobe.d/bonding.conf` and add the following line:
   
   ```
   alias bond0 bonding
   ```

7. Create a file named `route-bond0` in the `/etc/sysconfig/network-scripts` directory with the following content:

   **Note:** Do not include an entry for your enterprise partition platform—either comment out the line that references your platform number (third octet of the IP address), or do not include that line.

   ```
   172.30.1.0/24 via 172.31.1.250
   172.30.2.0/24 via 172.31.2.250
   172.30.3.0/24 via 172.31.3.250
   172.30.4.0/24 via 172.31.4.250
   172.30.5.0/24 via 172.31.5.250
   172.30.6.0/24 via 172.31.6.250
   172.30.7.0/24 via 172.31.7.250
   172.30.8.0/24 via 172.31.8.250
   172.30.9.0/24 via 172.31.9.250
   172.30.10.0/24 via 172.31.10.250
   172.30.11.0/24 via 172.31.11.250
   172.30.12.0/24 via 172.31.12.250
   172.30.13.0/24 via 172.31.13.250
   172.30.14.0/24 via 172.31.14.250
   172.30.15.0/24 via 172.31.15.250
   172.30.16.0/24 via 172.31.16.250
   ```

Proceed to configure the FM LAN connection for Red Hat Linux.

**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/network-scripts` directory with the following content:

   ```
   DEVICE=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=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.

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.

Proceed to update the UDEV persistent rules for Red Hat Linux.

**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/pci0000:00/0000:00:1c.4/0000:08:00.0/net*", NAME="eth-fmp3"
SUBSYSTEM=="net", ACTION=="add", DEVPATH=="/devices/pci0000:00/0000:00:1c.4/0000:08:00.1/net*", NAME="eth-fmp4"
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", ATTR{dev_id}=="0x0", ATTR(type)=="32", NAME="ib0"
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", ATTR{dev_id}=="0x1", ATTR(type)=="32", NAME="ib1"
```

Proceed to configure OS support of NMI generated kdumps for Red Hat Linux.

**Configuring OS Support of NMI Generated Kdumps for Red Hat LINUX**

The Forward! Fabric Manager and platform management console use a non-maskable interrupt (NMI) to force a server memory dump when you request for a dump. If you wish to use those interfaces when generating a kdump, configure operating system support for the NMI interrupt.
Log in as root, and add the following line to the `/etc/sysctl.conf` file:

```
kernel.unknown_nmi_panic=1
```

Reboot when you complete all configuration changes.

### 6.5. Configuring Partition Images to Boot From an External Storage Device

After commissioning a partition image on the internal storage of an enterprise partition platform (EPP), you can configure the partition image to boot from an external storage device.

- [6.5.1 Booting from Internal or External Storage](#)
- [6.5.2 Configuring Windows Partition Image to Boot From External Storage Device](#)
- [6.5.3 Configuring Linux Partition Image to Boot From External Storage Device](#)

#### 6.5.1. 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.

Once you commission the partition image, 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. 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 LUN is accessed has a valid license for running the operating system.

### 6.5.2. Configuring Windows Partition Image to Boot From External Storage Device

After commissioning a Windows operating system partition image on the internal storage of an enterprise partition platform (EPP), you can configure the partition image to boot from an external storage device.

This section provides details for setting up and configuring a previously commissioned Windows partition image to boot from an external storage device. In general, the process is as follows:

1. Prepare the external storage device.
2. Prepare for access to the EFI driver during boot.
3. Install the operating system and drivers, and create the boot environment on the external storage device.
4. Prepare the registry of the boot environment on the external storage device.
5. Determine the path information of the external storage device and update adapter firmware.
6. Configure the HBA adapter to boot from a LUN on the external storage device.
7. Boot your Windows partition image from the external storage device, and complete operating system setup if it is the first boot.
8. Complete post-installation tasks: Configure the FM LAN network connection, and update the registry.
9. Optionally configure the EFI shell for automatic boot to operating system on the external storage device.

**Note:** To boot the partition image from an external storage device, you need to establish the required driver for enabling boot from external storage devices. This is a manual intervention that uses the partition image console window (accessed through the Fabric Manager), and cannot be done through a Remote Desktop Protocol (RDP) session. This applies to all reboots as well.
Prerequisites

- A commissioned Windows Server 2012 or Windows Server 2012 R2 partition image
- Access to the partition image console (through the Fabric Manager user interface on the Fabric Management Platform)
- A functioning external storage device where the disk volume is visible to the operating system on the commissioned partition image
- The following files for accessing and creating a bootable partition on the external storage device:
  - Downloaded from the Unisys Product Support web site:
    (Access the Support site page for the Forward! product, navigate to the Software tab on the Drivers and Downloads page, and then download the SAN Boot Toolkit for the operating system you want to boot from external storage device.)
    - Bcdboot.exe
    - Dism.exe
    - Imagex.exe
    - Elxcli413a6.efi
    - s-Par® drivers for Windows Server 2012 or Windows Server 2012 R2
    - The Emulex OneInstall setup application for installing the Emulex OneCommand suite
    - Emulex adapter firmware file (.prg)
    - Emulex adapter boot code (.prg)
    - bootx64.efi
    - Winboot.nsh
    - Regupdate_remote.reg
    - Regupdate_remote_post_install.reg
    - Regupdate_host.reg
  - Third party drivers, such as Intel Ethernet and chipset drivers
  - Install.wim for Windows Server 2012 or Windows Server 2012 R2, depending on your desired operating system
    - The install.wim file is available from the respective Microsoft Windows operating system installation media, typically in the sources folder.
    - Depending on the operating system, rename the install.wim file to either install_w2k12.wim or install_w2k12r2.wim so that you can choose to use scripts included in the SAN Boot Toolkit.
    - The install_<OS version>.wim from the Microsoft Windows operating system installation media includes various editions of Windows for the operating system, each tagged with an image index number. You will need to enter the image index number later to select the appropriate edition within the
install_<OS version>.wim during installation. To identify the correct image index number for your operating system edition for use later: Place the install_<OS version>.wim file in a known location (for example, C:\temp), and then enter the following command in a Windows PowerShell window to display the contents of the install_<OS version>.wim:

```bash
.\imagex /info c:\temp\install_<OS version>.wim
```

Locate the description for your desired edition of Windows, and note its image index number.

**Preparing Your External Storage Device**

Do the following to prepare the external storage device and create a Windows boot volume:

1. Access the desktop of the partition image you wish to boot from an external storage device: On the Fabric Management Platform, use Fabric Manager to launch a console for the desired partition. (See 13.3 Accessing a Partition Desktop for more information.)

2. Copy the prerequisite files to a temporary location on the partition, for example, C:\temp.

3. Click **Server Manager**, expand the **Storage** node if needed, and then click **Disk Management**.

4. Verify that the external storage device is online and available in the Disk Management pane.

5. Note the characteristics of the external storage device so that you can identify it later in the DiskPart program window.


7. Type `diskpart`, and then press **Enter**.

   The DiskPart program window appears.

8. In the DiskPart program window, type `list disk`, and then press **Enter**.

   A list of available disks appears.

9. Using the characteristics of the external storage device that you previously noted down, determine the disk number for the external storage device.

10. Type **Select disk <number>**, and then press **Enter**.

    Where `<number>` is the displayed disk number.

11. Type **clean**, and then press **Enter**.

12. Type **convert gpt**, and then press **Enter**.

13. Type **create partition efi size=200**, and then press **Enter**.

14. Type **format fs=fat32 label ="<san system>" quick**, and then press **Enter**.

    Where `<san system>` is a valid label.

15. Type **assign letter=<system drive letter>**, and then press **Enter**.
Where `<system drive letter>` is an available drive letter, for example, s:.

16. Type `create partition msr size=128`, and then press Enter.

17. Type `create partition primary`, and then press Enter.

18. Type `format fs=ntfs label = “sanboot” quick`, and then press Enter.
   Where `<san boot>` is a valid label.

19. Type `assign letter= <boot drive letter>;`, and then press Enter.
   Where `<boot drive letter>` is an available drive letter, for example, v:.

20. Type `detail disk`, and then press Enter.
   A resulting summary of details similar to the following appears.

```
DISKPART> detail disk
DGC RAID 5 SCSI Disk Device
Disk ID: (BC4986B3-0FC5-4E18-841D-F98973A5007E)
Type: FIBRE
Status: Online
Path: 0
Target: 0
LUN ID: 0
Location Path: UNAVAILABLE
Current Read-only State: No
Read-only: No
Boot Disk: No
Pagefile Disk: No
Hibernation File Disk: No
Crashdump Disk: No
Clustered Disk: No

+-----------+---+-----------------+-----------------+--------+----------------+---------+----------+
<table>
<thead>
<tr>
<th>Volume ###</th>
<th>Ltr</th>
<th>Label</th>
<th>Fs</th>
<th>Type</th>
<th>Size</th>
<th>Status</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume 2</td>
<td>U</td>
<td>sanboot</td>
<td>NTFS</td>
<td>Partition</td>
<td>64 GB</td>
<td>Healthy</td>
<td>Hidden</td>
</tr>
<tr>
<td>Volume 3</td>
<td>S</td>
<td>SANSYSTEM</td>
<td>FAT32</td>
<td>Partition</td>
<td>200 MB</td>
<td>Healthy</td>
<td>Hidden</td>
</tr>
</tbody>
</table>
```

21. Verify the details for the disk partitions on the external storage device.

22. Refresh the Disk Management pane, and verify details for the disk partitions on the external storage device.
In the following example, Disk 1 is the external storage device.

Preparing for Access to EFI Driver During Boot

The partition image you wish to boot from an external storage device will need to access the external storage device through the Emulex HBA while booting. Thus the Emulex EFI driver needs to be manually loaded within the EFI boot shell of the partition image.

To preload the driver

1. From the desktop of your partition (on the internal storage of the enterprise partition platform), use the Disk Management pane to verify the disk number of your partition. For example, Disk 0.
2. In the DiskPart program window, type `select disk <disk number>`, and then press `Enter`.
   Where `<disk number>` is the disk number of your partition, for example, 0.
3. Type `detail disk`, and then press `Enter`.
4. Identify the volume number for the system volume—it will not have a value in the Ltr column.
5. Type `select vol <system volume number>`, and then press `Enter`.
   Where `<system volume number>` is the number for the system volume you previously identified.
6. Type `assign letter=<drive letter>`, and then press `Enter`.
   Where `<drive letter>` is an available drive letter, for example, h:. 
7. Type exit, and then press Enter to exit the DiskPart program window.

8. In the Windows PowerShell window, type exit, and then press Enter to exit Windows PowerShell.

9. From the desktop of your partition, launch File Explorer, and locate the drive letter for the system volume.

10. Copy the following files to the root directory of the drive:
    - Elxcli413a6.efi
    - winboot.nsh

    For example:

11. Navigate to the EFI folder in the root directory of the drive, rename the bootx64.efi file in there to bootx64.efi_old, and then copy the bootx64.efi file from the set of prerequisite files to the folder.

    **Note:** If desired, you can create a text file with all the diskpart commands—each command on a separate line—and run it in Windows PowerShell. For example,

    `diskpart.exe /s diskpartscript.txt`

**Installing OS and Drivers, and Create Boot Environment on Your External Storage Device**

Do the following to install the operating system, load s-Par® and third-party drivers, and create the boot environment on the external storage device:
1. From the desktop of your partition, copy the prerequisite files to a temporary location on the partition, for example, c:\temp.

   **Note:** The commands in following procedure use c:\temp. Adjust as appropriate to reflect the location where you copied the prerequisite files to.

2. In the Windows PowerShell window, type `cd \temp`, and then press Enter.

3. Type `.\imagex /apply c:\temp\install_<OS version>.wim <image index number><boot drive letter>`, and then press Enter.

   Where
   - `install_<OS version>.wim` is the name you renamed your install.wim to, for example, install_w2k12.wim.
   - `<image index number>` is the number you previously noted for your edition of Windows, for example, 1.
   - `<boot drive letter>` is the letter you previously assigned to the NTFS partition on the external storage device.

   For example:

   ![ImageX Tool for Windows](image)

   006623

4. Depending on your version of operating system, type one of the following, and then press Enter.

   - For Windows Server 2012
     ```
     .\dism\dism.exe /image:<boot drive letter>: /Add-driver /Driver:c:\temp\win8_signed_4.1.17 /recurse /forceunsigned
     ```
   - For Windows Server 2012 R2
     ```
     .\dism\dism.exe /image:<boot drive letter>: /Add-driver /Driver:c:\temp\win81_free_4.1.17 /recurse /forceunsigned
     ```

   Where `<boot drive letter>` is the letter you previously assigned to the NTFS partition on the external storage device.
5. Depending on your version of operating system, type one of the following, and then press Enter.
   - For Windows Server 2012
     \dism\dism.exe /image:<boot drive letter>: /Add-driver /Driver:c:\temp\3rdpartyDriversW2K12 /recurse /forceunsigned
   - For Windows Server 2012 R2
     \dism\dism.exe /image:<boot drive letter>: /Add-driver /Driver:c:\temp\3rdpartyDriversW2K12R2 /recurse /forceunsigned

   Where <boot drive letter> is the letter you previously assigned to the NTFS partition on the external storage device.

   For example:

   ![Command Output](image1)

6. Type \bcdboot <boot drive letter>:\Windows /s <system drive letter>: /f UEFI, and then press Enter.

   Where <boot drive letter> is the letter you previously assigned to the NTFS partition, and <system drive letter> is the letter you previously assigned to the FAT32 partition on the external storage device.

   ![Command Output](image2)
For example:

```
PS C:\temp> .\bedboot v:\Windows /s:\ /f UEFI
Boot files successfully created.
```

**Preparing Registry of Boot Environment on Your External Storage Device**

By default, Windows drivers in the newly created environment on the external storage device are set to not start when the partition starts. Use Registry Editor of the currently running (commissioned) partition image to update the registry of the environment on the external storage device.

1. From the desktop of your partition, run `regedit`.
   The Registry Editor window appears.
2. In the left pane, locate and select `HKEY_LOCAL_MACHINE`, click `File`, and then select `Load Hive`.
   The Load Hive dialog box appears.
3. Locate the NTFS partition on the external storage device, navigate to the `Windows\System32\config` folder, select `SYSTEM`, and then click `Open`.
4. When prompted, enter the name `remote`.
5. Click `File`, locate and select the `regupdate_remote.reg` file from the set of prerequisite files, and then click `Open`.
6. Click `OK`.
7. Close the Registry Editor.

**Determining Port Path Information of External Storage Device and Updating Adapter Firmware**

Use the Emulex OneCommand utility to determine the World Wide Name (WWN) port path information of the external storage device, and update firmware levels of the adapter.

1. From the desktop of your partition, locate and run the Emulex OneInstall setup application.
   The OneInstall window appears.
2. In the OneInstall window, click `Next`, ensure the NIC Driver option is not selected, and then click `Install` to install the Emulex OneCommand suite.
3. Click **Finish**.
4. From the **Start** menu, point to All **Programs**, **Emulex**, and then click **OCManager**.
   The OneCommand Manager window appears.
5. In the OneCommand Manager window, expand the nodes as needed to view details of the LUN on the external storage device where you previously loaded files, and note down the following:

- WWN of the adapter port
  
  For example:

- Port WWN of the target outboard of the adapter port
  
  For example:

- LUN number outboard of the target WWN (SCSI OS LUN)
  
  For example:
6. Update the adapter firmware and bootcode:
   a. In the left pane, click the adapter port number, and then select the **Maintenance** tab in the right pane.
      For example:

   b. Click **Download Firmware**.
The firmware download dialog box appears.

c. Click **Browse**, locate and select one of the .prg files from the set of prerequisite files, click **OK**, and then click **Start Download**.

For example:

![Firmware Download Dialog Box](image)

d. If prompted, click **Yes** to continue.

e. Repeat steps c and d for the other .prg file.

f. Click **Close** to close the firmware download dialog box.

7. Close the OneCommand Manager window.

### Configuring HBA Adapter to Boot From LUN on External Storage Device

**Note:** If you are configuring multiple partition images on the enterprise partition platform to boot from external storage devices, to minimize the number of platform reboots, perform all preparatory tasks detailed in the previous procedures for all desired partition images before rebooting the platform during this procedure.

To define the boot LUN outboard of the HBA adapter to boot from, do the following:

1. From the Fabric Management Platform, use Fabric Manager to gracefully shut down all running partitions on the enterprise partition platform. For more information, see **13.6.4 Gracefully Shutting Down a Partition Image**.

2. From the Fabric Management Platform, use Fabric Manager to launch a console for
the platform so that you can view the boot progress. (See 11.4 Launching the Platform Management Card (PMC) Virtual Console for more information.)

A platform management console window appears.

3. Reboot the platform, and use the platform management console window to monitor the boot progress.

4. When the option becomes available, press F2 to enter System Setup.

   For example:

   ![Platform management console window]

   5. Click System BIOS, click Integrated Devices, and then click Slot Disablement.

   6. Locate the HBA adapters associated with the partition image you are configuring to boot from external storage device, and then select their respective Enabled radio buttons.

      **Note:** Ports associated with a partition are allocated during commissioning. To identify the ports allocated to a partition, use Fabric Manager to view the summary of a partition, and then click Port & Config Preview to display a logical diagram of the ports allocated to the partition.

   7. Click Back, click Back, click Finish, and then click Yes to save changes.

   8. Click OK to acknowledge the message that changes were saved, click Finish, and then click Yes to confirm the exit and reboot.

   The platform reboots.

   9. Use the platform management console window to monitor the boot progress. When the option becomes available during adapter BIOS execution, simultaneously press the Ctrl and E keys or the Alt and E keys to enter the adapter BIOS configuration utility. The status “Emulex FC BIOS configuration utility selected” appears.
For example:

Note: If you see RAID adapter information on the screen, you missed the opportunity to enter the adapter BIOS configuration utility. Complete the platform boot process, and then reboot the platform to try again.

10. In the adapter BIOS configuration utility, use the arrow keys to select (highlight) the entry corresponding to the adapter port WWN you previously noted down, and then press Enter.
For example:

11. Select (highlight) the **Enable/Disable Boot from SAN** option, and press **Enter**.

12. Select (highlight) **Enable** and press **Enter**.
13. Press **Esc** to return to the previous menu, select (highlight) the **Configure Boot Devices** option, and then press **Enter**.

14. From the list of saved boot devices, select (highlight) the first item, and then press **Enter**.

15. In the resulting list, select (highlight) the entry corresponding to the target port WWN you previously noted down, and then press **Enter**.
For example:

16. When prompted, select the LUN number of the drive outboard of the target WWN. If necessary, adjust the value to correspond with information you previously noted down, and then press Enter.

In the following example, the value displayed is 00.

17. In the resulting list of LUN outboard of the target WWN, select (highlight) the entry corresponding to the LUN number you previously noted down, and then press Enter.
For example:

18. In the resulting context menu displaying details on the target WWN and outboard LUN, select (highlight) the **Boot this device via WWPN** option, and then press **Enter**.

For example:

19. Press **Esc**, and then press **Esc** again to return to the list of adapter ports and their WWNs.
20. If you are configuring multiple partition images on the enterprise partition platform to boot from external storage devices, repeat step 10 through 19 as needed to configure the boot LUN paths for other partitions as well.

21. Press Esc to exit the utility, and then press Yes to reboot the platform.

22. Use the platform management console window to monitor the boot progress, and when the option becomes available, press F2 to enter System Setup.

23. Click System BIOS, click Integrated Devices, and then click Slot Disablement.

24. Disable BIOS execution for the adapters you previously enabled.

25. Click Back, click Back, click Finish, and then click Yes to save changes.

26. Click OK to acknowledge the message that changes were saved, click Finish, and then click Yes to confirm the exit and reboot.

The platform reboots and starts partitions on the platform. Depending on the configuration, this can take up to 20 minutes.

27. Sign on to the partition you want to configure to boot from external storage device.

Boot Windows Partition Image From External Storage Device

After loading prerequisite files, partially installing the operating system on the external storage device, setting the registry for environment on external storage device, and configuring the HBA adapter to boot from the LUN of the external storage device, do the following to boot to the external storage device and complete operating system installation:

Notes:

- During the boot process, you will need to interrupt the normal boot process. Use the partition image console to carefully watch for the opportunity—there is only a two second window to interrupt this process. If you do not interrupt the boot in time, wait for the partition image to finish booting, and then restart the partition to try again.

- If you need more time to interrupt the normal boot process, start a command prompt when the partition image is booted from internal storage, and enter the following commands to display the Windows Boot Manager for 60 seconds when booting the platform.

  bcdedit /copy {current} /d "boot delay"
  bcdedit /timeout 60

- You need to repeat steps 2 through 16 whenever the partition reboots (manually invoked or OS-invoked) if you want to boot the partition image from an external storage device.

1. From the desktop of your partition, restart your partition.

The partition proceeds through its reboot process and video is lost.

Note: Be aware that in the next step you will only have two seconds to press a key to interrupt the boot process. If you do not interrupt the boot in time, wait for the partition image to finish booting, and then restart the partition to try again.
2. When the partition starts, the partition image console displays a black screen. Watch the black screen carefully for a progress line at the bottom, with the words “start boot option,” and press any key to interrupt the boot process. The EFI shell menu is displayed.

3. Use your cursor keys to select (highlight) the **Boot Manager** option, and then press **Enter**.

4. Highlight **Support Disk**.

5. Prepare to press **Esc** within five seconds of pressing **Enter** in the next step.

6. Press **Enter**, and then immediately press **ESC** to interrupt the automatic startup process.

   The Shell prompt appears.

7. Type **fs3:**, and then press **Enter**.

8. Type **ls**, and then press **Enter**.
The contents of the directory is listed, including the Elxcli413a6.efi file you previously loaded. For example:

```
Shell> fs3:

fs3:\> ls
Directory of: fs3:\

04/24/14 01:23p <DIR> 2,048 EFI
04/08/14 12:54a 415,232 Elxcli413a6.efi
    1 File(s)    415,232 bytes
    1 Dir(s)

fs3:\> 
```

9. Type `load Elxcli413a6.efi`, and then press `Enter`.

The system reports that the file was loaded. For example:

```
fs3:\> load Elxcli413a6.efi
load: Image fs3:\Elxcli413a6.efi loaded at 7A2E3000 - Success
fs3:\> 
```

**Note:** The hex address shown in the screen capture is an example; your system will display a different address.

10. Type `map –u`, and then press `Enter`.

The system displays several screens of output as it remaps drives, including external storage devices with partitions formatted in FAT32.

11. Review the output to locate the new EFI shell volume name for the FAT32 format partition on the external storage device.
In the following example, the external storage device can be identified by the word “fibre” in the path information, and is mapped to fs4.

12. Type `fs4:`, and then press **Enter**.
13. Type `cd EFI`, and then press **Enter**.
14. Type `cd boot`, and then press **Enter**.
15. Type `ls`, and then press **Enter**.

The contents of the directory are listed, including the `bootx64.efi` file you previously loaded. For example:
16. Type `bootx64.efi`, and then press **Enter** to boot the operating system on the external storage device.

   **Note:** You need to repeat steps 2 through 16 whenever the partition reboots (manually invoked or OS-invoked) if you want to boot the partition image from an external storage device.

   The screen in the partition image console does not display any activity for approximately two minutes, and then video is lost.

   The system checks memory and resets, and video is lost again.

   **Note:** Be aware that in the next step you will only have two seconds to press a key to interrupt the boot process. If you do not interrupt the boot in time, wait for the partition image to finish booting, and then restart the partition to try again.

17. When the partition starts, the partition image console displays a black screen.

   Watch the black screen carefully for a progress line at the bottom, with the words “start boot option,” and press any key to interrupt the boot process.

   The EFI shell menu is displayed.

18. Repeat steps 3 through 16 to reload the Emulex EFI driver and boot the operating system on the external storage device.

   Approximately 30 seconds after entering the `bootx64.efi` command, the Windows initial setup window appears.

19. Step through the on-screen prompts to complete installing your operating system, including entering your registration key.

20. When the operating system completes its set up processes, click **Server Manager**, expand the **Storage** node if needed, and then click **Disk Management**.
Disk 0 is now the boot disk within the external storage device environment, and Disk 1 is the boot disk on the internal storage of the enterprise partition platform. For example:

**Caution**

Do not use Disk 1 for anything else; it is required for the initial booting of the partition.

21. Right-click **Disk 1**, and then select **Offline**.
22. Optionally, close the Server Manager window.

**Completing Post-Installation Tasks**

Perform the following post-installation tasks:
Configure the FM LAN network connection

Use Fabric Manager to view FM LAN details for the partition. From the partition desktop, using Network Settings, locate the network adapter Unisys s-Par Nic6 Ethernet Adapter, access the adapter settings, and then define a static address for the adapter.

The IPv4 IP address should be in the form of 172.29.x.y, where x is the platform number and y is the partition number.

Update the registry

By default, some required boot drivers may be set to not load when the partition next reboots, for example, elxstor and elxfc for the fibre channel HBA. Update the registry to ensure that boot drivers are in the correct state for subsequent booting: Copy Regupdate_host.reg from the SAN Boot Toolkit onto the partition, and execute the file to update the registry.

Your partition is now ready for use.

Configuring EFI Shell for Automatic Boot to Operating System on Your External Storage Device

It may be inconvenient to manually interrupt the boot process to point to the EFI driver, remap the drives, and execute the bootx64.efi shell on the external storage device every time you reboot your partition image. To configure the partition boot manager to automatically boot to the external storage device, do the following:

1. From the desktop of your partition, restart your partition.

   The partition proceeds through its reboot process and video is lost.

   **Note:** Be aware that in the next step you will only have two seconds to press a key to interrupt the boot process. If you do not interrupt the boot in time, wait for the partition image to finish booting, and then restart the partition to try again.

2. When the partition starts, the partition image console displays a black screen.

   Watch the black screen carefully for a progress line at the bottom, with the words “start boot option,” and press any key to interrupt the boot process.

   The EFI shell menu is displayed.

3. Use your cursor keys to select (highlight) the **Boot Maintenance Manager** option, and then press **Enter**.
4. Select (highlight) **Boot Options**, and then press **Enter**.

5. Select (highlight) **Add Boot Option**, and then press **Enter**.

6. Locate and select (highlight) the volume **SYSTEM**, and then press **Enter**.
7. Select (highlight) the **EFI** option, and then press **Enter**.

8. Select (highlight) the **Boot** option, and then press **Enter**.

9. Select (highlight) **bootx64.efi**, and then press **Enter**.

10. Select (highlight) the **Input Description** option, and then press **Enter**.

11. Type in descriptive text for the entry you are creating (for example, SAN Boot), and then press **Enter**.
12. Select (highlight) the **Commit Changes and Exit** option, and then press **Enter**.

13. In the Boot Maintenance Manager screen, select (highlight) **Boot Options**, and then press **Enter**.

14. Select (highlight) **Change Boot Order** and then press **Enter**.

15. Press **Enter** to change the boot order, select the entry you just created (for example, SAN Boot), press + (the plus sign key) to move the entry to the top of the list, and then press **Enter**.

16. Select (highlight) the **Commit Changes and Exit** option, and then press **Enter**.

17. Press **Esc** to go back to the main menu.

18. Verify that **Continue** is selected (highlighted), and then press **Enter**.

   The boot process continues and you boot into the operating system on the external storage device.

19. If desired, restart your partition to verify it automatically boots to the external storage device.

### 6.5.3. Configuring Linux Partition Image to Boot From External Storage Device

After commissioning a Linux operating system partition image on the internal storage of an enterprise partition platform (EPP), you can configure the partition image to boot from an external storage device. Though the `/boot/efi` files need to remain on the internal storage, you can:

1. Copy the operating system files to the external storage device.

2. If necessary, change configuration files to reflect the external storage device.

**Note:** Depending on your configuration and setup, the `/boot` directories may also need to remain on the internal storage.
Prerequisite

You should be an experienced Linux system administrator familiar with the various processes used in this section and the implicit commands needed to execute the processes.

Considerations

When setting up your Linux partition image to boot from external storage, consider the following:

- Since you are copying files from a running operating system, the resultant files can be corrupted if they are in use during the copy process. Therefore,
  - Ensure you are running at single user mode (run level 1) to eliminate some of the possible open file issues.
  - Ensure you have synchronized the disks, and then remount the internal storage as read-only before performing the copy process.
- Since networking is not available in single user mode, you must log on to the Fabric Management Platform and use Fabric Manager to launch a partition image console for accessing the system. For more information, see 13.3 Accessing a Partition Desktop.
- Ensure you know the details for your external device so that you can easily identify it later in the list of controllers for external devices.

Setting Up Linux Partition Image to Boot From External Storage Device

To set up a previously commissioned Linux partition image to boot from an external storage device:

1. Configure your Linux partition image to boot into single user mode:
   a. On the running Linux partition image, edit the `inittab` file, or the `grub.conf` (Red Hat partition image) or `elilo.conf` (SUSE partition image) files so the partition image will boot into single user mode.
      Alternatively, insert the “1” kernel parameter during the boot process to force the partition image to boot into single user mode for a single boot. Subsequent boots will boot with your default run level.
   b. Reboot the partition image.
2. If you edited files in the previous step to change the run level, edit the same file to configure settings back to your default run level so that the partition image will boot into that mode when it next reboots.
3. Identify the internal (storage) boot device that contains your currently running operating system, as well as where the EFI system partition or `/boot/efi` partition is on the device.
Note: For Red Hat guests, you will also need to know which partition is the /boot partition. If /boot is not mounted as a separate partition, you will need to create a /boot partition on the internal boot device, and then copy the /boot files (except /boot/efi) to the new partition.

4. Determine how many partitions the internal boot device contains, and the size of the partitions.

5. Examine the /etc/mtab and /etc/fstab files to determine where various parts of the root file system (/) are mounted. Also note down the file system types.

6. Identify the external storage device that will become the new boot device.

7. Turn off swap.

8. Create a new GPT partition table on the external storage (boot) device.

9. Determine the size of the external storage boot device.

10. Examine the internal storage boot device and create a corresponding partition on the external storage boot device for each partition on the internal boot device, except for the /boot/efi partition, and, for Red Hat partition images, the /boot partition—these partitions remain on the internal boot device.

Depending on the sizes of the two disks, you may need to, or chose to, create partitions on the external storage boot device that are of different sizes than those on the internal storage boot device.

11. Create file systems on each of the newly created partitions on the external storage boot device. The file system type should be the same as the corresponding partition on the internal storage boot device. Refer to file system types on the internal storage boot device that you noted down in step 5.

12. Create a directory on the internal storage boot device that can be used as a mount point for mounting the partitions of the external storage boot device.

13. Create file system labels, and optionally change the UUIDs of the partitions on the external storage boot device.

   a. Identify the UUID and file system label for each of the partitions on the internal storage boot device and the external storage boot device, and then create a file system label for each of the new partitions on the external storage boot device. You can choose to create the file system labels on the external storage boot device using the same values as those on the internal storage boot device, or you can create them with different values.

   You can also choose to change the UUIDs of the partitions on the external storage boot device so they are the same as those on the internal device.

   Note: The file system labels and UUIDs must be unique for all the devices visible to the partition image—ensure no other external storage devices are using the same values.

   b. If you choose new labels or UUIDs, be sure to update any configuration files (such as /etc/fstab, /etc/kdump.conf, and the grub.conf or elilo.conf files) that reference the old labels and UUIDs with the new values.

   c. If you choose to retain the same labels or UUIDs, be sure to change the values on
Configuring Partition Images to Boot From an External Storage Device

14. If you have a Red Hat partition image and it does not have a separate /boot partition, create a partition on the internal storage boot device:
   a. Create a file system on that partition of the same type as your / file system.
   b. Create a file system label for the new partition.
   c. Update any configuration files that reference /boot.

15. Verify that initrd contains a driver for the HBA card that your partition image uses to connect to the external storage device. If the required driver is not in initrd, update initrd with the driver.

   *Note*: On a SLES 11 SP3 partition image, to verify if the required driver is in initrd, look at the list of modules in the INITRD-MODULES keyword in the /etc/sysconfig/kernel file to see if the driver is listed. If the driver is not listed, add the driver name to the list, save the file, and then issue a mkinitrd command.

16. Copy the file systems on each of the internal boot device partitions (except swap, /boot/efi, and, for Red Hat partition images, /boot) to the corresponding partition on the external storage device:
   a. Determine the file system type of the internal boot device partition you are copying.
   b. Mount the external storage boot device partition on the mount point directory you created in step 12.
   c. Synchronize your disks, and then remount the internal boot device partition as read-only.

   *Note*: If the directories or files on that partition are in use, you may not be able to remount the partition.

   d. Copy the directories on the internal storage boot device partition to the external storage mount point directory.

   *Note*: Do not copy subdirectories that are mounted to a different partition. For example, if /tmp is mounted to /dev/sda3, and /is mounted to /dev/sda5, do not copy the /tmp directory when you copy the / directory.

   As needed, create empty directories on the external storage boot device for dynamic directories that are created when the partition image boots, such as /proc or /sys.

   e. Unmount the external storage mount point directory.

   f. Remount the internal storage boot device partition as read-write if you mounted it as read-only.

17. Reboot the partition image.

18. Issue the mount command to verify that the file systems are mounted on the external boot storage device partitions.

19. Delete all the partitions on the internal boot storage device except for the /boot/efi partition, and, for Red Hat partition images, the /boot partition.
20. Reboot the partition image.

**Setting Up Different Linux Partition Image to Boot From Same External Storage Device**

If you wish to boot a different partition image from the external storage device that you set up, do the following:

1. Ensure that the external storage device can be viewed or accessed from the other partition, or will be visible or accessible.
2. If a partition is currently booted from the external storage device, shut down the partition.

**Caution**

Ensure only one partition is booted from the external storage device. Concurrently booting from multiple partitions causes data corruption.

You can choose to decommission or disable the original partition image to prevent concurrent booting.

3. Commission a new partition image using the same blueprint that you used when commissioning the original partition image that was configured to boot from the external storage device.
4. On the new partition image, change the required configuration files (such as `/etc/fstab`, `eliilo.conf`, or `grub.conf`) so they reference the external storage boot device partition file system labels and UUIDs.
5. Update the files on the `/boot/efi` (and for Red Hat partition images, the `/boot` partition) with changes you made to the corresponding files on the original partition.
6. Reboot the new partition.
7. Issue the mount command to see if the file systems are mounted on the external storage device partitions.
8. Delete all the partitions on the internal boot storage device except for the `/boot/efi` partition, and, for Red Hat partition images, the `/boot` partition.
9. Reboot the partition.
10. Change the IP addresses in the networking configuration files to reflect the new partition and platform.

The Forward! internal LANs use the following format:

- **Forward! Management (FM) LAN**: 172.29.x.y
- **Host Data (HD) LAN**: 172.30.x.y
- **Inter-partition (IP) LAN**: 172.31.x.y

Where x is the platform number and y is the partition number.
6.6. Configuring and Maintaining Operating Environments on Enterprise Partition Platforms

Hardening Operating Environments

You can choose to implement best practices recommended by Unisys for securing your Windows and Linux operating systems. For more information, see Section 14, Hardening and Unhardening Application Operating Environments.

Backing Up Operating Environments

According to your site policy and standard processes, schedule and perform backups of the Windows and Linux operating environments that contain your applications. For more information, see 18.3 Backing Up Application Operating Environments on Enterprise Partition Platforms.

6.7. Obtaining and Installing Interim Corrections (ICs)

Interim corrections (ICs), or fixes, are replacement versions of software that contain corrections to software errors. Each interim correction issued for a given software component has a cycle number to distinguish it from previous interim corrections for the same product.

Interim corrections are cumulative, meaning that each one in a series contains all the previous fixes in the same series. For example, suppose that

- Level 1.1 of a given product had interim corrections 1, 2, 3, and 4.
- You had installed interim correction 1, but not 2 or 3.

Interim correction 4 contains all the corrections that were in 1, 2 and 3, plus the new corrections that led to the release of interim correction 4. If you later require the changes made for interim correction 4, you also receive all corrections from 1, 2 and 3 in a single installation when you install interim correction 4.

The latest interim corrections, patches, fixes, and various packages containing new adapter drivers and firmware are available for download from the Unisys Product Support web site.

1. Using a web browser, navigate to www.support.unisys.com and sign in.
2. On the Product Support Home page, expand Forward! if needed, and then click Forward!
   The Support Site page for the product appears.
3. Click Releases.
   The Releases page appears.
4. On the Releases page, locate the section for your release level, and then click the link in the **Fixes** column.

   A Latest Available Interim Corrections page appears.

5. Click the desired IC.

   A download page for the IC appears.

6. Click the desired downloadable file, and then save it to a location of your choice.

7. Review any available comments, read-me files, or installation instructions on the page.

8. If needed, transfer the downloaded files to the appropriate platform, extract the contents from the archive, and then review and perform the included installation instructions.
Section 7
Administering Users

This section provides information about the users who can use the Fabric Manager user interface, and the associated roles in the following topics:

- 7.1 Role-based Access Control
- 7.2 Understanding User Roles
- 7.3 Creating a User
- 7.4 Setting-Up User Password
- 7.5 Assigning a User Role
- 7.6 Assigning Permissions to a Role
- 7.7 Adding Organizations
- 7.8 Assigning Organizations to Users
- 7.9 Changing Default Email Address
- 7.10 Deactivating a User
- 7.11 Activating User
- 7.12 Setting up User Password Lockout Preferences
- 7.13 Unlocking User
- 7.14 Deleting User

7.1. Role-based Access Control

Role-based Access Control (RBAC) is controlling the access based on the user roles. It allows you to create roles for particular job functions and give each role a subset of permissions or privileges that are required to perform a particular task.

Fabric Manager enables you to control which users can use the Fabric Manager, and what capabilities they have, based on what user roles they are assigned. It includes a collection of privileges that you can use to modify the roles. These roles are administrator, field engineer, observer, and operator. The privileges are described in 7.2 Understanding User Roles.
7.2. Understanding User Roles

A role is a set of privileges provided to a user or group of users so that they can perform specific tasks. A user who has been assigned with the administrator role can in turn assign roles to the existing users and add or update privileges associated with those roles. A user can be assigned to multiple roles.

Based on the tasks they perform, the user roles are categorized as Fabric Manager user roles and Portal roles. The Portal allows you to define and edit the permissions for various Fabric Manager and Portal user roles.

You can view all the roles defined for both the Fabric Manager and Portal in the Portal itself. Figure 7–1 displays the different roles available on the Portal.

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
<th>Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>FF_FieldEngineer</td>
<td>A user in this role has administrative privileges to monitor and manage the fabric.</td>
<td>Can perform all the tasks on Fabric Manager. This role has full access to all Fabric Manager features and settings. In this role, the user can perform all operations, including role and user management.</td>
</tr>
</tbody>
</table>

Figure 7–1. Portal and Fabric Manager Roles

Based on their functionality, the roles are classified as:

- **Fabric Manager user roles:**
  These are custom roles defined to access and perform various operations using the Fabric Manager. The following table lists the four predefined roles provided by the Fabric Manager, along with the descriptions, and privileges defined for each role.
**Role Description Privileges**

**Note:** This is not synonymous to Unisys service representative. This is a separate user role for the Fabric Manager.

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
<th>Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>FF_Administrator</td>
<td>A user in this role has administrative privileges to monitor and manage the fabric. The user in this role can perform both Portal administration and all the operations using Fabric Manager user interface.</td>
<td>This role has full access to all Fabric Manager features and settings. In this role, the user can perform all operations, including role and user management. Administrator cannot launch platform management console.</td>
</tr>
<tr>
<td>FF_Operator</td>
<td>A user in this role has controlled privileges to monitor and manage the fabric.</td>
<td>Can perform all operations on Fabric Manager except:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Configuring users</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Configuring platforms (add/delete/edit)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Launching platform management console</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Editing system (fabric) attributes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Deleting diagnostic information</td>
</tr>
<tr>
<td>FF_Observer</td>
<td>A user in this role can only view the operational status information. By default, the user in this role is also assigned with a Power User role.</td>
<td>This role can only view the operational status information. The user in this role cannot modify anything and cannot view or collect the diagnostic information.</td>
</tr>
</tbody>
</table>

See [Appendix A, User Roles and Privileges](#), for more information on various user roles and permissions.

- **Portal administration user roles:** These are default roles available to manage the Portal.

  **Note:** It is recommended not to assign the Portal Administration roles while creating a custom user.

  The following table lists the roles available in the Portal, along with the descriptions and privileges for each role.
Role Description Privileges

**Administrator**
A user in this role has administrative privileges to manage the Portal.
The user in this role cannot perform any Fabric management actions or operations, such as adding a platform.

*Note:* It is recommended not to add the Administrator role for any user.

This role has full access to all portal features and settings. A user in this role can perform all the portal operations, including role and user management.
Except for the operations defined for the Fabric Manager user interface, the user can perform all administrative actions.

**Power User**
A user in this role has the privileges to manage (upload image, blogs and so on) the sites the user has created on the portal.
The user in this role cannot perform any administrative operations on the Portal. The permissions for Power User are restricted by the Administrator.
The user cannot perform any Fabric management actions or operations, such as adding a platform.

The user with the Power User role can be created by an administrator role with some specific permission.

### 7.3. Creating a User

To get access to the Fabric Manager you must be added as a user by the administrator.

To create a user

1. On the Fabric Manager user interface, click ![Control Panel](image).
The Control Panel screen appears on the right pane.
2. On the left pane and under Portal, click Users and Organizations.
The Users and Organization screen appears on the right pane.
3. Click **Add** and then **User**.
The New User form appears.
4. Type the appropriate information in the following mandatory fields.
   
   - **Screen Name**
   - **Email Address**
   - **First Name**

   *Note:* You can use the **Screen Name** or **Email Address** to login to the Fabric Manager. **First Name** provides the user identity. Based on your need, you can provide the appropriate information in other fields.

5. In the **User Information** group click **Save**.

   A message informing you whether the new user is created successfully or not appears.

6. In the **User Information** group click **Roles**.

   Notice that under **Regular Roles**, the **Power User** role appears as the default role for this new user. Click **Remove**.

   **Notes:**
   
   - To verify if the user is added, under **Portal**, click **Users and Organizations**. Notice that the user you have added appears under **Users** list.
   
   - Contact Administrator to change user information.

### 7.4. Setting-Up User Password

**Prerequisite:**

- You have Field Engineer or Administrator privileges.

To set up the user password

1. On the Fabric Manager user interface, click 📄.

   The **Control Panel** screen appears on the right pane.

2. On the left pane, under **Portal**, click **Users and Organizations**.

   The Users and Organizations page appears on the right pane.

3. In the **Users** list, click the newly created user.

   The newly created user information appears.

4. In the User Information group, click **Password**.

   The **Password** form appears.

5. Enter the password.
Assigning a User Role

Note: This is a temporary password. The user is prompted to change the password after first login. The new password must contain 8 to 20 characters, at least one uppercase and lower case character, one number and one special character as per the following list:

- Characters: Lowercase “a” to “z” and uppercase “A” to “Z”
- Numbers: 0 to 9
- Symbols: ! @ $ * = - ?

6. Select Password Reset Required and click Save.

The password is set to the user. Using this password the user can login to Fabric Manager user interface. The user must change the password after the first login.

7.5. Assigning a User Role

To assign a role to the user

1. On the Fabric Manager user interface, click Portal. The Control Panel screen appears on the right pane.

2. On the left pane and under Portal, click Users and Organizations. The Users and Organizations page appears on the right pane. Notice that the user you have added appears under Users list.

3. In the Users list, click the appropriate user name.

4. In the User Information group click Roles. Notice that under Regular Roles, the Power User role appears as the default role for this new user. Click Remove.

5. To add a new role or roles for the user, under Regular Roles click Select. The Roles window appears.

6. Click on the appropriate role or roles that you want to assign to the user.

7. In the User Information group, click Save. Notice that the roles assigned for the user appears under Regular Roles.

Note: You can assign multiple roles to a single user.

7.6. Assigning Permissions to a Role

To assign permissions to a role

1. On the Fabric Manager user interface, click Portal. The Control Panel screen appears on the right pane.

2. On the left pane, under Portal, click Roles.
The list of roles appears on the right pane.

3. Select the required role, click **Actions**, and then **Define Permissions**.

4. In the **Add Permissions** field, select the appropriate portlet of the Fabric Manager.
   A list of permissions associated with the portlet appears.

5. Select the appropriate permissions and then click **Save**.
   The permissions get assigned to the selected role.

### 7.7. Adding Organizations

**Organizations** in a Portal represents the hierarchy of the business. A business can contain various departments, sub-departments, and so on. In a Portal, you can create **Organizations** and **Suborganizations** at various levels. The option enables you to administer and assign the various roles to users based on the department they belong to.

**Note:** *Organization and Suborganization hierarchies can be created to unlimited levels.*

The following figure is an example of a business that has two departments and subdepartments.

![Organization and Suborganization Hierarchy](image)

**Note:** *The administrator of an organization can manage all the suborganizations under it, including the users of the suborganizations.*

To add an organization

1. On the Fabric Manager user interface, click **.**
Assigning Organizations to Users

The Control Panel screen appears on the right pane.

2. On the left pane and under Portal, click Users and Organizations.
   The Users and Organization screen appears on the right pane.

3. Click Add and select Regular Organization.
   The New User form appears.

4. Type or choose the values in the following fields:
   - Name: Type a name for the organization or business.
   - Type: Select either Regular Organization or Location.
     Note: The Location cannot have any Suborganizations.
   - Parent Organization: Select an organization from the list to be the parent (root node of the suborganizations) of the organization you create.
     Note: Click Remove to remove the currently configured parent.

5. (Optional) Click Organization Site under Organization Information, and then select the Create Site box to attach a site.

6. Click Save.
   The newly added organization is listed under Top Level Organizations.

7.8. Assigning Organizations to Users

The Portal allows you to associate a user with an organization. The user can perform various operations on the organization based on the privileges assigned.

To assign the Organization to a user

1. On the Fabric Manager user interface, click .
   The Control Panel screen appears on the right pane.

2. On the left pane under Portal, click Users and Organizations.
   The Users and Organizations screen appears on the right pane.

3. Under Top Level Organizations, select an organization to which you want to assign a user.

4. Click Actions, and then click Assign Users.
   A list of current users appears. To view all the available users, click Available.

5. Select the required user, and click Update Associations.
   The selected user is assigned to the organization.

Notes:
- You can assign the organization to multiple users.
- To view the users of the organization, click the parent organization.
### 7.9. Changing Default Email Address

When you set up a user password in a Portal, an email is sent to the user with password details. The user receives the password details from the default email address `test@liferay.com`.

You can change this default email address and the name as per your requirement.

**Prerequisite:**
- You have Field Engineer or Administrator privileges.

To change the default email address
1. On the Fabric Manager user interface, click **Control Panel**.
   The **Control Panel** screen appears on the right pane.
2. On the left pane, under **Portal**, click **Portal Settings**.
   The **Portal Settings** appears on the right pane.
3. Under **Configuration** group click **Email Notifications**.
   The **Name** and **Address** fields appear under the **Sender** tab.
4. Type the required name and email address.
5. Click **Save**.
   The senders name and email address are saved. During password reset requests, the user receives the credentials from this email address.

### 7.10. Deactivating a User

Deactivating a user means that the user can no longer access the Fabric Manager user interface.

To deactivate a user
1. On the Fabric Manager user interface, click ![Control Panel].
   The **Control Panel** screen appears on the right pane.
2. On the left pane, under **Portal**, click **Users and Organizations**.
   A list of existing users appears on the right pane.
3. Select the user that needs to be deactivated.
   **Note:** You can also select multiple users for deactivation.
4. Click **Deactivate**. Alternatively, you can also click **Actions** and choose **Deactivate**.
   A message asking you to confirm the deactivation of the selected users appears.
5. Click **OK**.
The selected user is deactivated and can no longer access the Fabric Manager user interface.

**Note:** Deactivated users will be available in the fabric and retained for audit purposes and can be activated any time.

### 7.11. Activating User

By default, except Field Engineer all the default Fabric Manager users are deactivated. Users must be activated to logon to FFM UI and perform the operations.

**Prerequisite:** You have Field Engineer privileges.

To activate the user

1. On the Fabric Manager user interface, click [ ] .
   The Control Panel screen appears on the right pane.
2. On the left pane, under Portal, click Users and Organizations.
   A list of active users appears on the right pane.
3. From the Show drop-down list, select Inactive.
   A list of inactive customers appears.
4. Select the user that needs to be activated.
   **Note:** You can select multiple users for activation.
5. Click Restore. Alternatively, click Actions choose Activate.
   A message asking you to confirm the activation of the selected user appears.
6. Click OK.
   The selected user is activated and can access the Fabric Manager user interface. Activated users are displayed under Users list.

### 7.12. Setting up User Password Lockout Preferences

The Lockout option in Portal allows you to set the number of failed login attempts that triggers the user account to lock. You can also choose whether an administrator needs to unlock the account or if it becomes unlocked after a specific duration.

1. On the Fabric Manager user interface, click [ ] .
   The Control Panel screen appears on the right pane.
2. On the left pane, under Portal, click Password Policies.
   Password Policies screen appears on the right pane.
3. Under Name, click Default Password Policy.
4. Under the **Lockout** section, select the required value for the following fields:
   - **Maximum Failure**: Allows you to set the number of failed login attempts that locks the user account. Default value is set as 5.
   - **Reset Failure Count**: Allows you to set the time before the “failed login count” is reset. Default value is 30 minutes.
   - **Lockout Duration**: Allows you to set the duration to unlock the user account automatically. Default value is 30 minutes.

5. Click **Save**.
   The modified lockout preferences are saved.

### 7.13. Unlocking User

When a user exceeds the number of allowed login attempts, the user account gets locked automatically. The account gets unlocked automatically after 30 minutes. If the user wants to unlock the account before 30 minutes, then he or she must contact the administrator.

The Administrator or Field Engineer can unlock the user account.

To unlock the user account:

1. On the Fabric Manager user interface, click **Unlock**.
   The **Control Panel** screen appears on the right pane.
2. On the left pane, under **Portal**, click **Users and Organizations**.
   A list of existing users appears on the right pane.
3. Select the user that needs to be unlocked and then click **Unlock**.
   
   **Note:** Unlock option is enabled only if the user is locked.

   The selected user account gets unlocked. The user can now login to Fabric Manager using the same credentials.

   **Note:** To unlock the forwardadmin user account contact Unisys Service Representative. The user (forwardadmin) can also wait for 30 minutes to get the account unlocked.

### 7.14. Deleting User

You can delete the user from the list of deactivated users. The deleted user can no longer access the Fabric Manager.

To delete the user:

1. On the Fabric Manager user interface, click **Unlock**.
Deleting User

The Control Panel screen appears on the right pane.

2. On the left pane, under Portal, click Users and Organizations.
   A list of existing users appears on the right pane under Users.

3. Under the Show drop-down list, select Inactive.
   A list of inactive users appears.

4. Select the user to be deleted and click Delete. Alternatively, you can also click Actions and choose Delete.
   A message asking you to confirm the user deletion appears.

5. Click OK.
   The selected user is deleted and can no longer access the Fabric Manager user interface.
Section 8
Managing the Fabric as a Whole

This section provides the information on managing the fabric in the following topics:

- 8.1 Understanding the Relationship Between System and Fabric
- 8.2 Editing the System Attributes
- 8.3 Setting the Fabric Under Maintenance Mode
- 8.4 Setting Up Call Home
- 8.5 Adding a Platform to the Fabric

8.1. Understanding the Relationship Between System and Fabric

With Forward! by Unisys™ 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 Forward! fabric, see the 2.1 Summary of the Fabric Architecture section.

8.2. Editing the System Attributes

The Forward! Fabric Manager allows you to edit the initial system attributes. Only a field engineer or an administrator can edit the initial configuration using the Fabric Manager.

Prerequisites

- The FMPs are configured as FMP 1 and FMP 2.
- The FMPs are not configured as a high availability cluster.
## Editing the System Attributes

### Notes:

- **It is recommended to take a back up of the configuration settings before editing the system attributes. See [Section 18, Backup and Restore](#), for more information on how to back up.**

- **You cannot edit the LAN Subnet IP addresses if a partition image is commissioned on a platform.**

- **You can edit the FM LAN Subnet from the FMP where the platforms are added. These platforms are added from the FMP that is designated as FMP 1 when it is shipped from Unisys. Reconfiguring the subnet from FMP 1 ensures that the required changes are done in FMP 2 that is connected in the FM LAN.**

The following table describes the various attributes of the system that you can edit

<table>
<thead>
<tr>
<th>System Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Represents the name of the system (fabric). &lt;br&gt;This name is used as the root node in the hierarchical display of platforms and partitions. &lt;br&gt;The maximum length of the system name can be up to 16 alphanumeric characters along with the character “-”. The name however cannot start with the character “-“.</td>
</tr>
<tr>
<td>Description</td>
<td>Description for the system. &lt;br&gt;It is used to provide a meaningful description of the system (fabric); for example, to which data center it belongs, to which department it is assigned, and so on. &lt;br&gt;The maximum length of the system 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.</td>
</tr>
<tr>
<td>Sys Style</td>
<td>Represents the Unisys Style number for the host system or product. &lt;br&gt;By default, this field is populated during the Fabric Manager installation. The <em>Forward!</em> system and ClearPath <em>Forward!</em> system have different Sys Style values. By default, the Fabric Manager is configured to use Sys Style codes for the <em>Forward!</em> system. These codes are present in the in the <code>/usr/local/ffm/common/jetty/FFM-PlatformType.conf</code> file. You can edit the Sys Style value based on your system configuration. &lt;br&gt;For more information about editing the Sys Style, see <a href="#">8.2.1 Editing Sys Style</a>.</td>
</tr>
<tr>
<td>System Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>FM LAN</td>
<td>An Ethernet LAN that interconnects the Forward Fabric Management Platform, enterprise partition platforms, and running partitions for management functions.</td>
</tr>
</tbody>
</table>
| IP LAN           | An Ethernet LAN that interconnects the partition images within an enterprise partition platform and across different enterprise partition platforms.  
The IP LAN uses the high-speed InfiniBand physical connection.  
The IP LAN subnet address can be changed only during the fabric installation. |
| HD LAN           | An Ethernet LAN that interconnects the Windows partition images within a given partitionable enterprise partition platform so that application modules on other partitions may communicate. |
| Platform Name    | Represents the name of the Fabric Manager Platform.  
The maximum length of the platform name can be up to 16 alphanumeric characters along with the character “-”.
The name however cannot start with the character “-”. |
| Platform Description | Description for the Fabric Manager Platform.  
The maximum length of the 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. |
| Synchronize with NTP Server | Configures the Fabric Manager to use the Network Time Protocol (NTP) server to synchronize the date and time (and time zone, if applicable) across various components of the fabric, such as the Fabric Manager, platform management card, s-Par®, partitions, and so on.  
If you do not wish to configure the Fabric Manager to use an NTP server, then you can set the date, time, and time zone attributes manually. |
| NTP Server IP(s) | IP address of the NTP server.  
You can add, delete, and set the Primary NTP Server. |

To edit the system (fabric) attributes
**Editing the System Attributes**

1. On the Fabric Manager user interface, click **Manage System** on the left pane. The **Details** screen appears on the right pane.

2. Under **Details**, in the **Summary** tab, click **Edit**. Alternatively, click the arrow next to **<Forward-System>** and click **Edit**. The **Edit System** screen appears.

3. In the **System Details** tab, you can edit the following:
   - **Name**
   - **Description**
   - **Sys Style**

4. Click **Next**.

5. In the **LAN Subnets** tab, you can edit the default **Subnet** and **Subnet Masks**. These attributes can be changed if you have different subnet IP addresses. You can change the default IP addresses of the following groups:
   - **FM-LAN IP**
   - **IP-LAN IP**
   - **HD-LAN IP**

6. Click **Next**.

7. In the **Management Platform Network** tab, you can edit the following platform details:
   - **Platform Name**
   - **Platform Description**

8. Click **Next**.

9. In the **Time Source** tab, you can choose to synchronize the Fabric Manager with an NTP server.

   In the **Synchronize with NTP Server** option, if you choose
   - **Yes** option, then you can edit the time zone. You can also add the NTP servers and delete them from the available list.
     
     **Note:** You can set the NTP server if the FMP is in clustered environment and running node is master.
   - **No** option, then you can edit the date, time, and time zone.
     
     **Note:** The default value for **Synchronize with NTP Server** is **No**.

10. Click **Submit** to save the updated information.

---

**8.2.1. Editing Sys Style**

The Fabric Manager contains the following configuration files that contain the Sys Style value:
FFM-PlatformType.conf: Used by the Forward! system

ClearPath-PlatformType.conf: Used by the Forward! system in a ClearPath environment

By default, the Fabric Manager is configured to use Sys Style codes of the Forward! system. You can edit the default Sys Style. However, you must have Field Engineer or Administrator privileges to modify the Sys Style value. The updated Sys Style value is displayed in the Event console when a Call Home event is generated for that platform. However, the System Summary tab on the Fabric Manager user interface continues to display the default Sys Style value.

If you wish to edit the default Sys Style and configure it to use the ClearPath Sys Style, do the following:

1. Using PuTTY, log on to the Fabric Management Platform as the root user.
2. Execute the following command to check the status of the FFM services:

   ```bash
   # rcffmservices status
   ```

   If the services are running, stop the FFM services by using the following command:

   ```bash
   # rcffmservices stop
   ```

3. Execute the following command to open the “FFM-PlatformType.conf” file. This file located in the directory “usr/local/ffm/common/jetty”:

   ```bash
   cd /usr/local/ffm/common/jetty
   ```

4. Edit the Sys Style value for each key present in the “FFM-PlatformType.conf” file using an appropriate editor; for example, vi editor.

5. Execute the following command to start the FFM services:

   ```bash
   # rcffmservices start
   ```

   The updated Sys Style value is displayed in the Events console when a Call Home event is generated for the system.

If your system is configured to use the ClearPath Sys Style and if you wish to configure it to use the Forward! Sys Style, do the following:

1. Using PuTTY, log on to the Fabric Management Platform as the root user.
2. Execute the following command to check the status of the FFM services:

   ```bash
   # rcffmservices status
   ```

   If the services are running, stop the FFM services by using the following command:

   ```bash
   # rcffmservices stop
   ```

3. Execute the following command to locate the “FFM-PlatformType.conf” file:

   ```bash
   cd /usr/local/ffm/common/jetty
   ```

4. Rename the “FFM-PlatformType.conf” file.

   For example, “NonClearpath-FFM-PlatformType.conf”.

5. Execute the following command to locate the “ClearPath-FFM-PlatformType.conf” file:
Setting the Fabric Under Maintenance Mode

6. Rename the “ClearPath-FFM-PlatformType.conf” file as “FFM-PlatformType.conf”.

7. Execute the following command to start the FFM services:

   ```
   # rcffmservices start
   ```

   The updated Sys Style value is displayed in the Event console when a Call Home event is generated for this system.

8.3. Setting the Fabric Under Maintenance Mode

Maintenance mode is the state of the Forward! fabric in which you can carry out scheduled maintenance activities. When you set the system to maintenance mode, you can also specify the number of hours you need to carry out the maintenance activities.

When the system is in maintenance mode, the events that are generated during the maintenance activity are not sent to Call Home. This ensures that the Unisys Customer Support Center is not flooded with the call home messages triggered by the events generated while carrying out the maintenance.

To set maintenance mode

1. On the Fabric Manager user interface, click Manage System.

   The Manage System appears on the left pane and Details appears on the right pane.

2. Under Details, in the Summary tab, click Maintenance.

   Alternatively, click the arrow next to the <Forward-System> and click Maintenance Mode.

3. To enabled the Duration field, select the Enable check box.

   The Duration field appears.

4. Type the duration in hours.

   **Notes:**
   - The default value is 2 hours and the maximum value that you can enter is 550 hours.
   - You cannot enter a floating value. For example, 2.30, 1.15, and so on.

   A warning message appears displaying the information about the time when Call Home can be resumed.

5. Click Save.

   The fabric is set to the maintenance mode.
8.4. Setting Up Call Home

This section provides information about the Call Home feature in the following topics:

- 8.4.1 Understanding Call Home
- 8.4.2 Viewing Call Home Configuration
- 8.4.3 Configuring Call Home
- 8.4.4 Verifying Call Home Configuration

8.4.1. Understanding Call Home

Unisys Call Home is a software application that automatically detects system fault events and transmits an Electronic Service Request (ESR) packet that contains the failure details to the Unisys Support Center. The Call Home application is triggered by the specific events logged in the Event Log and also at any specific request sent by the user. The Call Home application is a communication link established between the Fabric Manager and the Unisys Support Center.

The Call Home feature sends the device failure messages to the Unisys Support Center in the form of XML formatted electronic packets (ESR requests). Following are some of the scenarios during which the call home notifications are sent.

- A partition image is terminated.
- A device fails to reset during shutdown or halt of the partition image.
- A boot disk is either inaccessible, write protected, or full.
- A restore disk is either inaccessible or write protected.
- One or more virtual disks have degraded or gone offline.
• One or more physical disks have failed.
• RAID is broken due to one or more failed physical disks.
• A platform generates a Non-Maskable Interrupt (NMI).
• All the Call Home events in the call home event log are deleted.

### 8.4.2. Viewing Call Home Configuration

To view the current Call Home configuration

1. Click **Manage System**.
   
   Manage System appears on the left pane and Details appears on the right pane.

2. Under Details, click the **Customer & Call Home Info.** tab.

   The Customer & Call Home Information screen appears.

To understand the various Call Home configuration parameters, see [Appendix C, Call Home Configuration Parameters](#).

### 8.4.3. Configuring Call Home

You need to configure the Call Home feature so that the Fabric Manager can send the Call Home events to the Unisys Support Center.

**Prerequisites**

- Port number 443 (HTTPS protocol) should be opened in the firewall so that it allows communication with the IP address 129.225.192.40. This is the IP address to connect to “host callhome.unisys.com”.
- You must have field engineer or administrator privileges.
- It is recommended to back up the current configuration settings before editing.
- No partition image is commissioned on any of the platforms.

To configure the Call Home application

1. Click **Manage System**.
   
   Manage System appears on the left pane and Details appears on the right pane.

2. Under Details, click the **Customer & Call Home Info.** tab, and then click **Edit**.

   The Edit Customer & Call Home Information screen appears.

3. In the **Customer Info.** tab, type the customer details.

4. Click **Next**.

5. In the **Call Home Settings** tab, type the following values:

   - **Host Name:** callhome.unisys.com

   *Note: Do not use other values.*
• **Host Port:** 443  
  *Note:* Do not use other values.

• **Number of Retries:** 1

• **Seconds Between Retries:** 10

6. For the connection type, select one of the following:

• **LAN (with Proxy):** Specify the IP address, port, user code, and password of the proxy server.

• **LAN (without Proxy):** The default selection.

• **Modem:** Specify the modem type, location, and phone number.

7. Click **Submit** to save the updated information.

### 8.4.4. Verifying Call Home Configuration

The Fabric Manager enables you to test and verify the Call Home connectivity using the **Test Setting** option. Test Setting provides the following options:

• **Communication Test Packet:** When you use this option, the Fabric Manager establishes a connection with the Unisys Support Center and sends the ESRDIAG packet. A successful communication is acknowledged with a SACK, and an unsuccessful communication is marked as Failed. If the information within the packet cannot be fully validated, a NACK is displayed. For more information on SACK and NACK events, see **15.1 Understanding Events.**

  For information on how to test and verify the connectivity using the communication test packet, see [Testing Call Home Connectivity Using Communication Test Packet Option](#).

• **Ready for Use Test Packet:** When you use this option, the Fabric Manager user interface establishes the connection with the Unisys Support Center and sends the ESRRFU packet that validates the system style, serial number, and address information entered in the **Customer Information** tab.

  For information on how to test and verify the connectivity using the ready for use test packet, see [Testing Call Home Connectivity Using Ready for Use Test Packet Option](#).

  *Note:* The serial number is same as the service tag, and is entered in **ID** field of the **Customer Info.** tab.

## Testing Call Home Connectivity Using Communication Test Packet Option

### Prerequisites

- You must have field engineer or administrator privileges.
- The *Forward!* Fabric Management Platform (FMP) must be connected to the corporate LAN.
- Host name must be set as callhome.unisys.com.
Setting Up Call Home

Notes:
- It is recommended to backup the current configuration settings before you begin the testing. See Section 18, Backup and Restore, for more information on how to back up.

To test and verify the Call Home configuration by using the Communication Test Packet option

1. Click Manage System.
   Manage System appears on the left pane and Details appears on the right pane.
2. Under Details, click the Customer & Call Home Info. tab, and then click Edit.
   The Edit Customer & Call Home Information screen appears.
3. In the Customer Info. tab, click Next.
   The Call Home Settings tab appears.
4. In the Test Setting section, click Communication Test Packet to transmit a test Call Home packet.
   When the test packet is sent successfully, the message “ESR Sent Successfully” appears.
5. Click View acknowledgement to view the response packet details in a pop-up window. Verify that the Packet Type is SACK and the Contact Number is ESRDIAG.
6. Click Close to close the pop-up window.
7. When the configuration and tests are complete, click Submit in the lower right of the Call Home Settings tab to save the changes.

Note: Ensure that you repeat the Communication Test Packet process whenever you change the method of transmitting packets or upon a successful repair of an issue that prevented communication.

Testing Call Home Connectivity Using Ready for Use Test Packet Option

Prerequisites
- You must have field engineer or administrator privileges.
- The Forward! Fabric Management Platform (FMP) must be connected to the corporate LAN.
- Host name must be set as callhome.unisys.com.

Notes:
- It is recommended to backup the current configuration settings before you begin the testing. See Section 18, Backup and Restore, for more information on how to back up.
To test and verify the Call Home configuration using the Ready for Use Test Packet option

1. Click Manage System.
   Manage System appears on the left pane and Details appears on the right pane.

2. Under Details, click the Customer & Call Home Info. tab, and then click Edit.
   The Edit Customer & Call Home Information screen appears.

3. In the Customer Info. tab, click Next.
   The Call Home Settings tab appears.

4. In the Test Setting section, click Communication Test Packet to transmit a test Call Home packet.
   When the test packet is sent successfully, the message “ESR Sent Successfully” appears.

5. Click View acknowledgement to view the response packet details in a pop-up window. Verify that the Packet Type is SACK and the Contact Number is ESRDIAG.

6. Click Close to close the pop-up window, and then click Reset.

7. Click Ready for Use Test Packet.
   When the packet is sent successfully, the message “RFU Sent Successfully” appears.

8. Perform the following:
   - Click View acknowledgement to view the response packet details in a pop-up window.
   - Verify that the Packet Type is SACK.
   - Note down the value for Contact Number.

   Note: Unisys Support will call the phone number entered on the Customer Information tab to confirm that the packet was received, and if it was formatted correctly or to identify any issues. If the information within the packet cannot be fully validated, NACK is displayed for Packet Type, and the Problem Text field provides more information. (You may need to contact Unisys Support to resolve the issue if the cause is not readily apparent.)

9. Click Close to close the pop-up window.

10. When all configuration and tests are complete, click Submit in the lower right of the Call Home Settings tab to save changes.

   Note: Ensure that you repeat the Ready For Use (RFU) packet process whenever you change customer information details.

8.5. Adding a Platform to the Fabric

Platforms are physical computers in the fabric on which you can host one or more partition images. The Forward! Fabric Manager allows you to add additional enterprise partition platforms to the fabric. You can add up to 16 platforms to a fabric.
There are two types of platforms:

- Nonpartitionable enterprise partition platform (NEPP): A Unisys Intel 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 Intel 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 and administrators have appropriate 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. See 8.2 Editing the System Attributes for more information.

  **Note:** Only the field engineers 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, click **Manage System** on the left pane. **Details** screen appears on the right pane.
2. Under **Details**, in the **Summary** tab click **Add**. Alternatively, click the arrow next to <Forward-System> and click **Add**. A confirmatory message to verify power supply, network connection, and IP default settings appears.
3. Click **OK**. The **Add Platform** window appears.
4. 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.
      
      **Note:** The maximum length of the platform name can be up to 16 alphanumeric characters along with “-”. The name however cannot start with the character “-”.
   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.
**Adding a Platform to the Fabric**

**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.

5. Click **Add**.

A message informing you whether the platform is added successfully appears.

If the EPP is successfully added, it appears under the **Manage System** with the current state information. Also, on the **Details** pane, a summary of the newly added platform appears.

You can now commission a partition image on the newly added platform. See **5.5 Commissioning a Partition Image** for more information.
Section 9
Managing High Availability in Your Fabric

The Forward! by Unisys™ fabric offers high availability capability for the Forward! Fabric Manager.

This section provides information on the Fabric Manager high availability capability, as well as details specific to the use of the capability.

- 9.1 Redundant Fabric Management Platform for High Availability
- 9.2 Overview of Fabric Manager Clustering
- 9.3 Understanding Data Replication in Clustering
- 9.4 Understanding High Availability Fencing
- 9.5 Understanding Cluster Groups
- 9.6 Accessing the Fabric Manager Cluster
- 9.7 Managing the Fabric Manager Cluster

9.1. Redundant Fabric Management Platform for High Availability

If you purchase the Forward! Enterprise configuration, you receive two Fabric Management Platforms configured as a high availability cluster. (If you purchased the Base configuration, you may later purchase an upgrade package to add an additional redundant Fabric Management Platform.)

With the server, you receive two Fabric Management Platforms configured as a high availability cluster.

For some models of the server, you may choose to purchase or upgrade to two Fabric Management Platforms to be configured as a high availability cluster.

One Forward! Fabric Management Platform in the cluster serves as the master and the other as the standby. These roles are not fixed; at one time a given Fabric Management Platform might serve as the master and at another time as the standby. In clustering terminology, the two Fabric Management Platforms are referred to as nodes.

The high availability of the Forward! Fabric Management Platform and its Fabric Manager software is ensured in the following ways.
• Resource level failures

A resource level failure is a failure of one of the critical Forward! Fabric Manager software components. If one of these components fails, the cluster automatically restarts it on the same node, reducing down time and minimizing failovers.

• Node level failures

A node level failure is a failure that incapacitates one of the Forward! Fabric Management Platforms; for example, a failure of the operating system or internal storage drive. If the master node fails, processing automatically fails over to the standby node, ensuring continuous availability of the Forward! Fabric Management Platform and its Fabric Manager software. (When this occurs, the standby node now acts as the master node.) This configuration prevents a single point of failure for the management hardware and software.

The high availability software includes

• Elements of the SUSE® LINUX Enterprise High Availability Extension suite of open source clustering technologies

• Unisys value-add components for cluster configuration, monitoring, and management

The high availability cluster uses Distributed Replication Block Device (DRBD) technology to replicate several types of data between the master Forward! Fabric Management Platform and the standby Forward! Fabric Management Platform. DRBD copies data from the master node to the standby node, ensuring that both copies of the data remain identical. DRBD replicates data in real time without the applications being aware that the data is stored on multiple Forward! Fabric Management Platforms.

The Unisys service representative installs and configures the high availability Forward! Fabric Management Platforms at your site when your Forward! fabric is installed. Thereafter, you manage the high availability cluster using Unisys and standard Linux cluster management tools.
9.2. Overview of Fabric Manager Clustering

The Unisys high availability capability included in the Forward! Fabric Manager user interface is used to configure and manage the highly available cluster of Fabric Manager. The Unisys high availability capability is built on the SUSE® LINUX Enterprise High Availability Extension suite of open source clustering technologies.

The key components from the SUSE High Availability extension package delivered with our high availability capability are

- The HA Web Konsole (HAWK) interface and a command line interface (CLI) which enable you to manage the Fabric Manager cluster
- The Pacemaker graphical user interface (GUI) and Corosync software which enable you to manage finer details of the Fabric Manager cluster
- Distributed Block Replication Device (DRBD) software that allows for data replication of the Fabric Manager data

The key components unique to the Unisys high availability capability are

- Unisys Cluster application for configuring the Fabric Manager cluster and managing cluster services
- Enhanced Resource Agents to monitor the availability of Fabric Manager resources
- Predefined Fabric Manager high availability cluster configuration
- Push button setup for the Fabric Manager high availability cluster using the Unisys Cluster interface.

The Unisys high availability capability integrates with open source technologies and enables you to support the Fabric Manager workload in a highly available manner, eliminating single points of failure. The high availability capability automatically shares cluster configuration, replicates Forward! management data, and coordinates cluster-wide activities to ensure predictable behavior in protecting your management resources.

The Unisys highly available Fabric Manager uses several modules such as services, resources agents, network and file availability as well as a stable Linux kernel. The following figure shows the Unisys supplied resource agents in dark blue; the SLES High Availability Extension package components in medium blue; and the operating system resources, subsystems, kernel, and device drivers provided by the SLES 11 kernel in gray.
The first node of your highly available cluster is configured on site, and then a second Fabric Manager node is joined to the existing cluster. Once the base cluster is created, then the Fabric Manager resources are added.

### 9.3. Understanding Data Replication in Clustering

The *Forward!* Fabric Manager high availability cluster uses the Distributed Replication Block Device (DRBD) to replicate several types of data between the cluster nodes. This capability is a software-based, shared-nothing replicated storage solution mirroring the content of block devices (disk partitions) between hosts. That is, the DRBD copies data from the primary node to the secondary node ensuring that both copies of the data remain identical. It replicates data in real time without the applications being aware that the data is stored on multiple hosts in a synchronous manner.

The following simple diagram illustrates that each node contains local disks that are replicated between the two cluster nodes.
In the case where the master Fabric Manager node fails, the second (standby) node automatically becomes the master node. The application access point automatically moves to the second node so that clients can continue to have access, as shown in the following figure.

**Understanding the Distributed Replication Block Device**

The core functionality of the DRBD is implemented through the Linux kernel module. Because the DRBD is situated near the bottom of the I/O stack for a system and constitutes a driver for a virtual block device (disk), it provides a flexible and versatile replication solution that adds high availability to just about any application.

By definition and the Linux kernel architecture, the DRBD is separate and independent of the layers above it. It cannot add features to upper layers that they do not possess.
The DRBD uses a managed virtual block device, /dev/drbr0, in the Fabric Manager high availability cluster where the postgres data is mapped. The /dev/sda3 disk partition in the Fabric Manager high availability cluster is associated with the DRBD block device.

A file system is created on top of where the directories to be shared are stored. The Fabric Manager high availability cluster shares several directories, replicating the contents of the directories with DRBD. The replicated contents include postgres data, dumps, nagios/etc, nagios/var, and some Tomcat data. The Fabric Manager high availability mount point is /mnt/ffmha.

The DRBD resource is either primary or secondary. When it is primary, the postgres database and other Fabric Manager resources run on this cluster node. When it is secondary, it receives all updates from the peer node’s device but otherwise disallows access completely.

The Fabric Manager high availability cluster uses DRBD synchronous replication mode. That is, local write operations on the primary node are considered completed only after both the local and remote disk write have been confirmed. Thus, a single node loss does not lead to any data loss. However, if both nodes are destroyed at the same time, data loss occurs.

Data replication occurs in the Fabric Manager cluster over the Forward! Management (FM) LAN static IP address.

The DRBD provides automatic recovery from split-brain situations, which might occur if the card to the Forward! Management (FM) LAN fails. Once connectivity becomes available again and peer nodes exchange the initial DRBD protocol handshake, DRBD detects the split-brain situation. If it detects that both nodes are in the primary role, it immediately tears down the replication connection and tries to recover, resyncing the data.

**Note:** The Distributed Replication Block Device used with the Fabric Manager cluster is configured with Fabric Manager cluster definitions by default. You can find background information and other information about the DRBD in the DRBD User Guide from LinBit at http://www.drbd.org

### 9.4. Understanding High Availability Fencing

The Forward! Fabric Manager high availability cluster includes daemons to fence a misbehaving Fabric Management Platform as determined by the cluster software. These daemons use the Intelligent Platform Management Interface (IPMI) to control the integrated remote access component, which provides the remote power operations as required by the cluster. This capability enables one cluster node to reboot the other node to protect against data being written to or from both platforms simultaneously, which can cause data corruption.

The cluster operations wiring for the configuration permits automatic takeover of Fabric Manager resources in the event of a node failure, or if the card that provides access to the Forward! Management (FM) LAN fails.
9.5. Understanding Cluster Groups

The Forward! Fabric Manager high availability cluster includes cluster groups; a cluster group is a collection of resources that are dependent on one another. In the Fabric Manager clustered configuration, all resources run on one node or the other. However, the postgresql database is central to all other operations. Subgroups along Fabric Manager application lines are defined separate from the database to isolate any failures in a particular application. For example, the cluster defines an authentication group that consists of samba, winbind, wine32, and the Unisys authentication server. If any of these components fail, the log-ins from the desktop partition are temporarily not allowed until the cluster stops and restarts the related services. Thus services affected during a resource failure recovery are isolated.

The Fabric Manager high availability mount point for data replication is not part of a Fabric Manager cluster group. This mount point includes data from the postgres and Apache Fabric Manager cluster groups defined as follows:

- **DRBD Group:** This master group for the Fabric Manager high availability cluster consists of the data replication block device (DBRD) and runs on both nodes as a master slave apart from the application. One of the cluster nodes must be promoted to master before any other cluster services can start.

- **Postgres Group:** This group is the main group related to the postgres database that contains the postgresql, jetty, nagios, and nagios_feeder services. The mount point is defined as /mnt/ffmha. This file system is mounted on the system where the DRBD resource is master. It is only mounted on one system at a time. If any of these resources fail, the cluster attempts to restart the group on the same system without affecting the other groups. If the cluster cannot start the failing resource, all of the Fabric Manager resources fail over to the standby cluster node.

- **Apache Group:** This group contains cluster resources related to Apache—including Apache and Tomcat. This group depends on the DRBD resource being promoted to master. Any failure in Tomcat or Apache is isolated to this resource group only. If the cluster cannot resolve the resource failure, all resources on this cluster node fail over to the standby cluster node.

- **Authentication Group:** This cluster resource group contains the services that support partition desktop and authentication—including samba, winbind, wine32, and Unisys authentication. A resource failure in one of these services results in a possible restart of all of the related services. If the cluster cannot resolve the resource failure, a node failover occurs and all Fabric Manager resources move to the standby cluster node.

- **Other Resources:** Other resources are not connected to any one cluster resource group. The Forward! Management (FM) LAN floating IP address is connected to the DRBD resource being promoted to master on one of the cluster nodes. The Network Time Protocol (NTP) service resource runs on both nodes at all times.
9.6. Accessing the Fabric Manager Cluster

When the Forward! Fabric Manager is clustered, additional access points are available. These access points consist of “floating” IP addresses and a static IP address for each Forward! Fabric Management Platform.

The “floating” IP addresses are associated with the active Fabric Manager components. For example, if an administrator attaches to the Fabric Management Platform through the floating IP address attached to the customer corporate LAN (public LAN), the connection is to the Fabric Management Platform with the active workload.

For direct access to a particular Fabric Management Platform, the administrator uses the static IP address for that Fabric Management Platform.

The access points for your clustered Fabric Management Platforms are

- A static Forward! Management (FM) LAN address for each Fabric Management Platform enables the administrator to manage the system directly.
  
  For example, administrators with the correct credentials can complete certain tasks regarding cluster creation and the cluster service [OpenAIS] using the Unisys Cluster application and the static IP address. (Not that remote desktop is required for this use.)

- The floating IP address on the Forward! Management (FM) LAN is used for s-Par® authentication, ensuring that the syscon terminals are authenticated on the active Fabric Management Platform.

A floating IP address on the customer corporate LAN (public LAN) is available for an administrator to use to access the Fabric Manager—ensuring that the administrator is connected to the active Fabric Management Platform. The administrator can manage the day-to-day Fabric Manager cluster operations using the floating IP address as long as the cluster service is running.

9.7. Managing the Fabric Manager Cluster

You can manage the Forward! Fabric Manager high availability cluster using

- The Unisys Cluster application to manage the cluster service (OpenAIS) and to view the access points to use for access to the Fabric Manager. (Requires special privileges for the administrator and the remote desktop capability.)

- The HAWK (HA Web Konsole) interface or crm shell command line interface (CLI) to view the status of cluster resources and perform other administrative and operations tasks.

Managing the Cluster Service

Once the cluster is created and the resources are added to the cluster, the cluster service (OpenAIS) is set to not start at boot. This setting enables system administrators to recognize a hardware component failure or a severe cluster failure and analyze it before
restarting the cluster service on the node, thereby preventing a split-brain situation. In this case, the workload on the Fabric Manager continues to run on the remaining node in a degraded state such that no node failure is allowed until the cluster service is manually restarted on the failed node.

An administrator with special privileges can use the Unisys Cluster application from either cluster node to view the current status of the Fabric Manager cluster service and to perform several tasks such as starting and stopping the cluster service.

Managing the Fabric Manager Cluster

You can manage the Fabric Manager cluster using the HAWK interface or the crm shell command line interface (CLI). These tools enable you to view the status of each node and every cluster resource plus allow you to start and stop a cluster resource; to migrate cluster resources to the other node; to use cleanup resources to clear the failure count of a resource and allow the cluster to attempt to start it; and to manage or unmanage resources.

Refer to the SUSE Linux Enterprise High Availability Extension 11 SLES 11 SP3 High Availability Guide (PDF) or (web topics) for more information about using these tools to manage the Fabric Manager cluster. In the PDF version of the document, Chapter 4 of that guide provides background information; Chapter 5 provides information about managing the cluster using HAWK; and Chapter 7 provides information about managing the cluster using command line tools.

Note: Because Unisys provides Fabric Manager high availability clustering in a qualified configuration, you do not need much of the information in that guide. You should not change any configuration values without first consulting Unisys support.

The following topics describe some of the ongoing tasks that you might need to perform in the clustered environment. Unisys recommends you use the HAWK interface for day-to-day operations and the Unisys Cluster application for the few specific cluster service tasks.

- 9.7.1 Connecting to a Specific Fabric Management Platform
- 9.7.2 Identifying All Access Points for the Cluster
- 9.7.3 Managing the Cluster Service
- 9.7.4 Connecting to the Active Fabric Management Platform and Monitoring Cluster Node Status
- 9.7.5 Performing Routine Maintenance and Updates
- 9.7.6 Viewing Current Failure Status and Limits for the Fabric Manager Resources
- 9.7.7 Cleaning Up and Manually Resetting a Resource Failcount
- 9.7.8 Manually Migrating the Forward! Fabric Manager Workload
- 9.7.9 Interpreting OCF Return Codes
9.7.1. Connecting to a Specific Fabric Management Platform

Once the cluster is created, you need to use the static IP address for a specific Fabric Management Platform to connect to it. (See 9.7.2 Identifying All Access Points for the Cluster for more information about types of IP access points.)

To connect to a specific Fabric Management Platform, use a Remote Desktop Protocol (RDP) client software (for example, Remote Desktop Connection on a Windows computer) to connect to its static FMP public LAN IP address. (This IP address was recorded during fabric installation.)

9.7.2. Identifying All Access Points for the Cluster

Once the cluster is created, you can use a remote desktop session to access the Fabric Management Platform and then use the Unisys Cluster application to view the static and floating IP addresses available for completing various day-to-day and maintenance tasks.

You use the static IP address for a specific Fabric Management Platform. If you use a floating IP address, you are connected to the active Fabric Management Platform. Generally, you use the static IP address when using the Unisys Cluster application and a floating IP address when using the HAWK interface. (See 9.6 Accessing the Fabric Manager Cluster for more information about types of IP access points.)

**Note:** The administrator requires specific credentials to use the Unisys Cluster application to manage the cluster service and perform some maintenance tasks.

To identify all access points
2. Launch the Unisys Cluster application.
3. Select Other in the left column.
   The Other selections are displayed.
4. Click **Unisys Cluster**.

   The Unisys Cluster application window appears, displaying a list of IP addresses.
9.7.3. Managing the Cluster Service

Once the cluster is created, you can access and sign in to the Fabric Management Platform using Remote Desktop Protocol (RDP) client software (for example, Remote Desktop Connection on a Windows computer), and then use the Unisys Cluster application to manage the cluster service (OpenAIS). Note that you only need to occasionally manage the cluster service.

You can perform the following (limited) management actions:

- **Start Service**: Starts the cluster service when it is not running on one of the nodes.
- **Stop Service**: Stops the cluster service when the service is running.
- **Change OpenAIS on Boot**: Allows the cluster operations to come up automatically after a restart of the system (by default, this option is not enabled).
  
  **Note**: Unisys does not recommend enabling this option due to possible split-brain situations.
- **Remove Node**: Enables the Unisys service representative to remove or replace a cluster node when a Fabric Management Platform is replaced.
- **Delete Cluster**: Enables you to delete the cluster entirely. Note that OpenAIS must first be stopped all nodes.

To manage the cluster service


2. Launch the YaST Control Center.

3. Select **Other** in the left column.

   The Other selections are displayed. (See Figure 9–1.)
4. Select **Unisys Cluster** in the right column to open the Unisys Cluster application.
5. Select **Service** from the left column. (See Figure 9–2.)
   A display showing the current status of the cluster appears and offers choices for the possible management actions.

### 9.7.4. Connecting to the Active Fabric Management Platform and Monitoring Cluster Node Status

When you use the HAWK interface to view the cluster status, you can either connect to the active Fabric Management Platform with the floating IP address, or to a specific Fabric Management Platform with its static IP address.

Do the following to access the HAWK interface and monitor cluster status:

*Note: For more detailed information about using HAWK, refer to the SUSE Linux Enterprise High Availability Extension 11 SLES 11 SP3 High Availability Guide [(PDF) or web topics]. Chapter 5 Part II in the PDF file provides information specifically about using HAWK.*

1. Open a Web browser to **https:<floating FMP public LAN IP address>:7630**.
   *Note: If needed, open port 7630 on the customer corporate LAN (public LAN). For more information on configuring firewall and opening ports, refer to the SUSE Linux Enterprise Server 11 SP3 Security Guide [(PDF) or web topics] topic Configuring the Firewall with YaST (15.4.1 in the PDF file).*
2. Sign on with **hacluster** and a default password of **linux**.
3. In the left navigational bar, click **Cluster Status**.
   A screen similar to that shown in Figure 9–3 is displayed. The colors on the status display indicate the following:
   - Green means OK or running
   - Red means bad or unclean
   - Yellow means in transition
   - Gray means not running but the cluster expects it to be running
   Other self-explanatory icons might also be displayed for the state of nodes, resources, tickets, and for error messages. To display any additional actions available for a resource, click the resource, and then click on the wrench icon.
You control the cluster during maintenance tasks using the HAWK interface. For more information about using HAWK, refer to the *SUSE Linux Enterprise High Availability Extension 11 SLES 11 SP3 High Availability Guide* (PDF or web topics).

- Cluster maintenance mode maintains all processes running in the cluster; however, the monitor action is disabled for all resources. You can stop and start the processes outside the cluster without being charged a “failure” by the cluster, which would increase the resource failcounts.
- Standby a cluster node causes the entire node to be put into standby status, which moves all of the cluster resources to the node that is online. Select the cluster node using HAWK and then choose **Standby**.
Resources do not run on the standby node until it is brought back online.

**Note:** You can put a cluster node in standby and then reboot the partition if necessary. Use this method whenever the partition or platform needs to be rebooted.

- Stop (or start) a resource (or resources) if maintenance of a particular component needs to be patched. Select the resource using HAWK and choose **Stop**. Any dependent resources also stop.
- Cleanup Resources clears the failure count of a resource and allows the cluster to attempt to start it.
- Migrate/move the cluster resources to another node.

### 9.7.6. Viewing Current Failure Status and Limits for the Fabric Manager Resources

When you use the HAWK interface to view the status of the cluster, a summary is displayed showing the status of your cluster nodes and resources. You can view details about each resource by clicking the wrench icon for the resource and then choosing **View Details**.

Failures are highlighted in red (as links) at the top of the summary as shown in **Figure 9–4**. Also, an “rc” code is given for each failure. (See **9.7.9 Interpreting OCF Return Codes** for a list of frequently returned codes.) The failed resources are also grayed in the list of resources configured to signify that they are not running but are expected by the cluster to be running.

To check failure status:

1. Open a Web browser to **https:<floating FMP public LAN IP address>:7630**.
   **Note:** If needed, open port 7630 on the customer corporate LAN (public LAN).
2. Sign on with **hacluster** and a default password of **linux**.
3. In the left navigational bar, click **Cluster Status**.
   A screen similar to that shown in **Figure 9–4** is displayed.
Figure 9-4. Cluster Status with Failures Highlighted

4. Click on a failed resource in the list and click on the wrench icon to display a list of actions.

5. Choose View Details from the list.

The details show the attributes set for that resource; the failcount for the resource; the last failure timestamp (if the failcount is greater than 0); plus the operation history and timings (call id, operation, last run timestamp, execution time, queue time, return code and last rc change timestamp).

6. Click on a red link at the top of the display to get more information about the failure and to see the rc code for the failure.

9.7.7. Cleaning Up and Manually Resetting a Resource Failcount

A count of the number of failures each resource encounters is maintained. The failcounts are used to determine where resources can run. Each node has a migration threshold that determines the tolerance for failures. The migration threshold is set to 5 by default (globally), and you can change this setting using the HAWK interface or the CLI.
By default, once the threshold is reached, the node is not allowed to run the failed resource until the administrator manually resets the failcount of the resource, or the default failure-timeout (configured in 60 second increments) expires the failcount and automatically resets it. (You can change this timeout setting using the HAWK interface or the CLI.)

If a resource fails, it is automatically restarted; however, each failure increases the failcount of the resource. You might need to perform the cleanup action and reset the resource failcount. For more information about using HAWK, refer to the SUSE Linux Enterprise High Availability Extension 11 SLES 11 SP3 High Availability Guide (PDF or web topics).

**Note:** If a resource fails to stop, the cluster fences the node in order to be able to start the resource on the remaining node.

To manually clean up and rest a resource failcount:

1. Open a Web browser to `https://<floating FMP public LAN IP address>:7630`.
   **Note:** If needed, open port 7630 on the customer corporate LAN (public LAN).
2. Sign on with `hacluster` and a default password of `linux`.
3. In the left navigational bar, click `Cluster Status`.
   A screen similar to that shown in Figure 9–3 is displayed.
4. Click the wrench icon next to the failed resource and then choose `Clean Up`.
   The cleanup action resets the failcount and enables the cluster to restart the resource.
5. To continue, confirm the message that is displayed.

### 9.7.8. Manually Migrating the Forward! Fabric Manager Workload

Do the following to manually move the Fabric Manager workload to the peer cluster node:

1. Open a Web browser to `https://<floating FMP public LAN IP address>:7630`.
   **Note:** If needed, open port 7630 on the customer corporate LAN (public LAN).
2. Sign on with `hacluster` and a default password of `linux`.
3. In the left navigational bar, click `Cluster Status`.
4. Click the (green) **wrench icon** of the ffmha_fs resource.
5. On the context menu, select **Move**.
   (All Fabric Manager resources are connected together, thus moving one resource moves all connected resources.)
Figure 9–5. Moving the Workload

A dialog box appears, displaying choices of where to move the resources.

6. Choose one of the node names listed in the dialog box or choose **Away from current node** and click **OK**.

   All Fabric Manager resources complete an orderly stop, and then restart on the node selected.

7. Click the **wrench icon** of the resource again to display the choices.

8. Click **Drop Relocation Rule**.

   A dialog box displays the message: This will clear any relocation constraints set on resource `<resource name>`. Do you want to continue?

9. Click **Yes** to complete the action.

   The Drop Relocation Rule allows the resources to move back if needed.
### 9.7.9. Interpreting OCF Return Codes

The cluster starts, stops, and monitors each resource agent running in the cluster. Actions and failures return codes to provide more information. Each action has specific exit codes that it must return. The cluster software always checks the return code against the expected result. If the result does not match the expected value, then the operation is deemed to have failed and a recovery action is initiated.

Refer to the following table for a list of common return codes, their meaning, the type of failure, and the action taken by the cluster. The “rc” codes are numeric but map to an OCF Alias as shown in the table.

<table>
<thead>
<tr>
<th>RC</th>
<th>OCF Alias</th>
<th>Description</th>
<th>Return Type</th>
<th>Action Taken by Cluster</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>OCF_SUCCESS</td>
<td>Success. The command completed successfully. This is the expected result for all start, stop, promote, and demote commands.</td>
<td>Soft</td>
<td>N/A.</td>
</tr>
<tr>
<td>1</td>
<td>OCF_ERR_GENERIC</td>
<td>Generic “there was a problem” error code.</td>
<td>Soft (Transient error occurred.)</td>
<td>Restart the resource or move it to a new location.</td>
</tr>
<tr>
<td>2</td>
<td>OCF_ERR_ARGS</td>
<td>The configuration of the resource is not valid on this machine. (For example, refers to a location/tool not found on the node.)</td>
<td>Hard (Nontransient error occurred that might be specific to current node.)</td>
<td>Move the resource elsewhere; prevent retrying it on current node.</td>
</tr>
<tr>
<td>3</td>
<td>OCF_ERR_UNIMPLEMENTED</td>
<td>The requested action is not implemented.</td>
<td>Hard (Nontransient error occurred that might be specific to current node.)</td>
<td>Move the resource elsewhere; prevent retrying it on current node.</td>
</tr>
<tr>
<td>4</td>
<td>OCF_ERR_PERM</td>
<td>The resource agent does not have sufficient privileges to complete the task.</td>
<td>Hard (Nontransient error occurred that might be specific to current node.)</td>
<td>Move the resource elsewhere; prevent retrying it on current node.</td>
</tr>
<tr>
<td>5</td>
<td>OCF_ERR_INSTALLED</td>
<td>The tools required by the resource are not installed on this machine.</td>
<td>Hard (Nontransient error occurred that might be specific to current node.)</td>
<td>Move the resource elsewhere; prevent retrying it on current node.</td>
</tr>
<tr>
<td>RC</td>
<td>OCF Alias</td>
<td>Description</td>
<td>Return Type</td>
<td>Action Taken by Cluster</td>
</tr>
<tr>
<td>----</td>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>6</td>
<td>OCF_ERR_CONFIGURED</td>
<td>The configuration of the resource is invalid. (For example, required parameters are missing.)</td>
<td>Fatal (Nontransient error occurred that is common to all cluster nodes, meaning a bad configuration was specified.)</td>
<td>Stop the resource and prevent it being started on any cluster node.</td>
</tr>
<tr>
<td>7</td>
<td>OCF_NOT_RUNNING</td>
<td>The resource is safely stopped. The cluster will not attempt to stop a resource that returns this code for any action.</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>OCF_RUNNING_MASTER</td>
<td>The resource is running in Master mode.</td>
<td>Soft</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>OCF_FAILED_MASTER</td>
<td>The resource is in Master mode but has failed. The resource will be demoted, stopped, and then started (and possibly promoted again).</td>
<td>Soft (Transient error occurred.)</td>
<td>Restart the resource or move it to a new location.</td>
</tr>
</tbody>
</table>
Section 10
Controlling Power for Each Platform

This section provides information on various platform power control options provided by the Fabric Manager.

You can use the power control options on a particular platform and not on all platforms at the same time in a given system. For example, in the system if there are three platforms, platform x, platform y, and platform z, then the power control options performed on platform x are applicable only to platform x. You cannot use power control options on all three at the same time.

In general, platforms can be shutdown gracefully or forcefully.

- **Graceful Shutdown**: This is an orderly shutdown of the platform. You can use the **Soft Shutdown** and **Soft Restart** options to perform graceful shutdown of the platform. The current state of the operating system is saved during this shutdown.

- **Forceful Shutdown**: This is an unorderly shutdown where the state of the operating system is not saved. You can use the **Power Off**, **Hard Restart**, **Power Cycle**, and **Force Dump** options to perform forceful shutdown of the platform.

**Caution**

Avoid forceful shutdown unless required. This operation may result in data loss and may also cause s-Par® instances to crash.

**Note**: Platform power operations are asynchronous and Fabric Manager does not wait until the operation is complete on the platform to report the success or failure of the operation. The Fabric Manager executes the command on the platform which initiates the desired action. You should ensure manually on Fabric Manager user interface that the operation is complete on the platform and retry if required.

This section provides the following information:

- **10.1 Understanding Status of Platforms**
- **10.2 Powering-On a Platform**
- **10.3 Performing Soft Shutdown on a Platform**
10.4 Powering-Off a Platform
10.5 Performing Hard Restart on a Platform
10.6 Performing Soft Restart on a Platform
10.7 Performing Power Cycle on Platform
10.8 Performing Force Dump on a Platform

The following table provides the summary of different power operations you can perform on partitionable EPP and nonpartitionable EPP when they are powered on.

<table>
<thead>
<tr>
<th>Power Operation</th>
<th>Partitionable EPP</th>
<th>Nonpartitionable EPP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Soft Shutdown</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Hard Restart</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Soft Restart</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Power Cycle</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Force Dump</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Power Off</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

10.1. Understanding Status of Platforms

The following table lists various icons dealing with the power status of a platform:

<table>
<thead>
<tr>
<th>Icons</th>
<th>Platform Power Status</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Partitionable EPP</strong></td>
<td></td>
</tr>
<tr>
<td>🔄</td>
<td>Powered On</td>
</tr>
<tr>
<td>🔄</td>
<td>Power Inactive</td>
</tr>
<tr>
<td>🔄</td>
<td>Powered Off</td>
</tr>
<tr>
<td>🔄</td>
<td>Unreachable / Status is unknown</td>
</tr>
<tr>
<td><strong>Nonpartitionable EPP</strong></td>
<td></td>
</tr>
<tr>
<td>🔄</td>
<td>Powered On</td>
</tr>
<tr>
<td>🔄</td>
<td>Power Inactive</td>
</tr>
<tr>
<td>🔄</td>
<td>Powered Off</td>
</tr>
</tbody>
</table>
10.2. Powering-On a Platform

The powering-on platform operation is the 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, click **Manage System** on the left pane, expand `<Forward-System>`, and then select the required platform on which you want to power on.
   
   Details screen appears on the right pane.

2. In the Details pane, under **Summary** tab, click **Power On**.
   
   The selected platform is powered-on. In the **Summary** tab, the status of the platform changes to **On**.

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 **Shutdown** 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, click **Manage System** on the left pane, expand `<Forward-System>`, and then select the required platform on which you want to perform shutdown gracefully.
   
   Details screen appears on the right pane.

2. In the Details pane, under the **Summary** tab, click **Soft-Shutdown**.
   
   A message asking if you want to shut down the platform appears.

3. Click **OK**.
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-Off a Platform

Powering-off is an unorderly shutdown and power-off of the platform. This is equivalent to switching off the computer by pressing the power button. The platform is turned off without an orderly shutdown of its partition images and guest operating systems.

**Caution**

This operation may result in loss of unsaved state or data.

To power off a platform

1. On the Fabric Manager user interface, click **Manage System** on the left pane, expand `<Forward-System>`, and then select the required platform on which you want to power off.

   **Details** screen appears on the right pane.

2. In the **Details** pane, under the **Summary** tab, point to **Advanced**, and click **Power Off**.

   A message asking if you want to power off the platform appears.

3. Click **OK**.

   The selected platform is powered-off and the status of the platform changes to **Off**.

### 10.5. Performing Hard Restart on a Platform

The hard restart is an unorderly shutdown of the platform and partition images followed by a restart. After the platform restarts, the partition images are restarted based on their initial state property. This operation may result in loss of the current state of partition images and data in transaction.

To perform a hard restart
1. On the Fabric Manager user interface, click **Manage System** on the left pane, expand **<Forward-System>**, and then select the required platform on which you want to hard restart.

   On the right pane, under the **Details, Summary** tab appears.

2. In the **Details** pane, under the **Summary** tab, point to **Advanced**, and click **Hard Restart**.

   A message asking if you want to hard restart the platform appears.

3. Click **OK**.

   The selected platform shuts down followed by a restart on successful hard restart.

### 10.6. Performing Soft Restart on a Platform

Soft restart is a graceful shutdown of the platform and partition images followed by a restart. Soft restart is equivalent to clicking **Start** and then clicking the **Shutdown** and **Restart** buttons in a computer.

Following is the sequence of actions that are performed when you choose to soft restart a platform:

1. Partition images are gracefully shutdown.
2. After all the partition images are shut down, the service partitions are gracefully shutdown.
3. Platform is powered-off followed by a restart.

**Note:** You cannot perform **Soft Restart** operation on Nonpartitionable EPP.

To perform soft restart

1. On the Fabric Manager user interface, click **Manage System** on the left pane, expand **<Forward-System>**, and then select the platform on which you want to soft restart.

   On the right pane, under the **Details, Summary** tab appears.

2. In the **Details** pane, under the **Summary** tab, point to **Advanced**, and click **Soft Restart**.

   A message asking if you want to soft restart the platform appears.

3. Click **OK**.

   If the soft restart operation is successful, the selected platform shuts down gracefully and then restarts.

### 10.7. Performing Power Cycle on Platform

This is an unorderly shutdown, power-off, and then power-on of the platform.
Power cycling a platform helps in reinitializing the configuration or recovering from an unresponsive state, such as a crash or hung situation.

**Note:** The power cycle option should be performed only after all other attempts to get control of the system fail.

To power cycle the platform

1. On the Fabric Manager user interface, click **Manage System** on the left pane, expand **Forward-System**, and then select the platform on which you want to perform power cycle.
   Details screen appears on the right pane.
2. In the Details pane, under the Summary tab, point to Advanced, and click **Power Cycle**.
   A message asking if you want to power cycle the platform appears.
3. Click **OK**.
   On successful power cycle operation, the selected platform shuts down, powers off, and then powers on automatically.

### 10.8. Performing Force Dump on a Platform

This is an automatic dump, unorderly shutdown, and restart of the platform. This option is used to create the operating system dependent diagnostic dump.

When the platform restarts, the partition images are restarted based on their initial state property.

To perform force dump and run the diagnostics

1. On the Fabric Manager user interface, click **Manage System** on the left pane, expand **Forward-System**, and then select the platform on which you want to force dump.
   In **Platform Summary** on the right pane, the Summary tab appears.
2. In the Details pane, under the Summary tab, point to Advanced, and click **Force Dump**.
   A message asking if you want to reset and run the diagnostics appears.
3. Click **OK**.
   Platform shuts down and restarts on successful force dump.

**Note:** Refresh the browser to view the platform state.
Section 11
Managing Platforms

This section provides the information about managing platform in the following topics.

- **11.1 Viewing the Platform Summary**
- **11.2 Viewing Configuration Information of a Platform**
- **11.3 Editing Platform’s Name and Description**
- **11.4 Launching the Platform Management Card (PMC) Virtual Console**
- **11.5 Deleting Partitionable EPP**
- **11.6 Deleting Nonpartitionable EPP**

**Notes:**

- You cannot perform or view any options if the status of the platform is *Unknown*.
- The platform power operations are available only if the Enable Intelligent Platform Management Interface (IMPI) Over LAN option is enabled in the Network/IPMI Settings of the platform management card console. This option is enabled by default.
- Fabric Manager does not support browser context menu options. For example when you right click on any platform or partition image the options such as Open in new tab and Open in new window result in “about:blank” page.

### 11.1. Viewing the Platform Summary

The following table describes the various attributes of the platform that you can view on the platform summary:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Denotes the name assigned to a platform when it is added to the fabric.</td>
<td>BankA</td>
</tr>
</tbody>
</table>
| Description    | Provides the description of a platform when it is added to the fabric.     | This platform contains all the banking applications related to BankA. }
## Viewing the Platform Summary

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Describes the type of the platform when it is added to the fabric. The values can be NEPP or PEPP.</td>
<td>PEPP</td>
</tr>
<tr>
<td>Platform Number</td>
<td>This number is a unique numerical value that is assigned to a platform when it is added to the fabric. The value ranges from numbers 1 to 16. It represents the third octet in the FM-LAN IP of the PMC and s-Par®.</td>
<td>5</td>
</tr>
<tr>
<td>DNS RAC Name</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> 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.</td>
<td>BankA-5</td>
</tr>
<tr>
<td>Service Tag</td>
<td>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.</td>
<td>DWC4KY1</td>
</tr>
<tr>
<td>Maintenance Mode</td>
<td>Defines the status of the maintenance mode. It is enabled when maintenance activities are carried out on the fabric.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>Processor Type</td>
<td>Denotes the processor brand, product line, model number, and operating frequency.</td>
<td>Intel(R) Xeon(R) CPU E5-2667 v2 @ 3.30GHz</td>
</tr>
<tr>
<td>Processor Frequency</td>
<td>Indicates the platform processor frequency.</td>
<td>3.3 GHz (per processor)</td>
</tr>
<tr>
<td>Sockets</td>
<td>Defines the number of sockets supported by the platform processor.</td>
<td>2</td>
</tr>
<tr>
<td>Cores</td>
<td>Defines the number of cores supported by the platform processor.</td>
<td>16 (8 per socket)</td>
</tr>
<tr>
<td>Memory</td>
<td>Indicates the total memory available in the platform.</td>
<td>127 GB</td>
</tr>
</tbody>
</table>

**Platform Overview**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health</td>
<td>Denotes the status of the platform health. It can be one of the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Unknown</strong>: Indicates that the Fabric Manager is unable to understand the status of the platform.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Ok</strong>: Indicates that there are no issues found in platform.</td>
<td>Ok</td>
</tr>
<tr>
<td></td>
<td><strong>Warning</strong>: Indicates that the platform needs the attention. For example, Warning is displayed when the platform has an unsupported Software or Firmware version.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Critical</strong>: 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.</td>
<td></td>
</tr>
<tr>
<td>Power</td>
<td>Indicates the status of the platform. It can be either <strong>On</strong> or <strong>Off</strong>.</td>
<td>On</td>
</tr>
<tr>
<td>s-Par® Instance</td>
<td>Denotes the status of the s-Par® instance. It can be either Running or Stopped.</td>
<td>Running</td>
</tr>
</tbody>
</table>
### Viewing the Platform Summary

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Partition Status</strong></td>
<td>Provides the graphical representation of the partition image status.</td>
<td></td>
</tr>
</tbody>
</table>

To view the platform summary

1. On the Fabric Manager user interface, click **Manage System** on the left pane, expand `<Forward-System>`, and then select the platform that you want to view.

   **Details** appears on the right pane.

2. Click the **Summary** tab.

   The summary of the platform appears.
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, click Manage System, expand <Forward-System>, and then click the platform for which you want to view the configuration information.

The Config. Info tab comprises the following:
- 11.2.1 Partition Chassis List
- 11.2.2 Configuration Details Section
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:

![Partition Chassis List Example](image)

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.

- **Enabled Partition Image**: Displays the name of the partition image that is commissioned on the Partition Chassis.

- **Memory Limit**: Displays the maximum memory size that can be assigned to the partition image commissioned on this Partition Chassis.

- **Sizes**: Displays the size of the partition image that can be commissioned on the Partition Chassis. The available sizes are **Extra Small**, **Small**, **Medium**, **Large**, **Extra Large**, **Extra Extra Large**, and **Maximal**. The size of the partition image is displayed based on the resources available on the platform.

**Notes:**

- Only the sizes that can be assigned for that particular partition chassis are displayed. For example, for a partition image using Chassis-A, the sizes displayed can be **Small**, **Medium**, **Large**, and **Maximal**. However, for a partition image using Chassis-B, sizes can be **Small** and **Medium**.

- The size of the partition image that is already commissioned is marked with a √.

### 11.2.2. Configuration Details Section

This section displays details of the partition image configuration such as number of ports, cores, memory size, and so on.
The following is an example of the **Details** section in the **Config. Info** tab:

The **Details** section displays the configuration details of all the possible sizes that can be selected on a particular partition image in separate tabs. For example, on the partition chassis list, if you select a row that contains Chassis-A, the Small, Medium, Large, and Maximal tabs are displayed. However, if you select a row that contains Chassis-B, only the Small and Medium tabs are displayed.

The **Details** section provides you the following information:

**Cores**: Number of processor cores associated with the selected partition image. For example, if you have selected a partition image using Chassis-A, the Small size will have two cores, whereas a Medium size will have four cores.

**Memory**: Maximum and minimum memory size that can be associated with the selected partition image. For example, if you have selected Chassis-A, which is associated with a partition image, the Small size can have from 8 to 256 GB of memory. However, the Medium size can have from 16 to 256 GB of memory.

**NIC Ports**: The number and type of NIC ports that are configured for the selected partition image.
**HBA Ports**: The number and type of HBA ports that are configured for the selected partition image.

**Details**: Displays the vendor and the type of a NIC or HBA port when you click it.

**Notes:**
- To learn more about how to read the information about ports displayed in the Details section, click **Show Legends**.
- You can use the Synchronize button to refresh the data on the Details section when
  - Platforms are added or deleted.
  - Partitions 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.

### 11.3. Editing Platform’s Name and Description

If your user role gives you the required permission, you can edit the platform name and description based on your role.

It is recommended to take a back up of the configuration settings before editing the platform name and description. See Section 18, Backup and Restore, for more information on how to back up.

1. On the Fabric Manager user interface, click **Manage System** on the left pane, expand `<Forward-System>`, and then select the platform that you want to edit.
   
   Details screen appears on the right pane.
2. In the Details pane, and under **Summary** tab, click **Edit**.
   
   Edit Platform screen appears.
3. Change the platform name and description, and click **Save** to update.

**Notes:**
- Provide a unique name for the platform. The maximum length of the platform name can be up to 16 alphanumeric characters along with “-“’. The name cannot start with the character “-“.
- 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.
You can view the updated platform name under the Manage System. The changed platform name gets reflected in the event logs that are generated after renaming the platform.

### 11.4. 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.

**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, click Manage System and expand <Forward-System> to view various platforms.

   Details appears on the right pane.
3. Click the platform for which you want to launch PMC console.
4. In the Details pane, and under 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.

### 11.5. 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.

**Prerequisite:**
- 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, click **Manage System** on the left pane, expand `<Forward-System>`, and then select the partitionable EPP that you want to delete.
   Details screen appears on the right pane.
2. In the Details pane, and under **Summary** tab, click **Delete**.
   Alternatively, click the arrow next to the partitionable EPP and click **Delete**.
   A confirmatory message asking if you want to delete the partitionable EPP appears.
3. Click **Ok**.

The deleted partitionable EPP will not be visible under the **Manage System** and cannot be used any further.

*Note:* It is recommended to delete all the events related to the deleted partitionable EPP.

### 11.6. Deleting Nonpartitionable EPP

**Prerequisite:**
- 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, click **Manage System** on the left pane, expand `<Forward-System>`, and then select the nonpartitionable EPP that you want to delete.
   Details screen appears on the right pane.
2. In the Details pane, and under **Summary** tab, click **Delete**.
   Alternatively, you can also click the arrow next to the nonpartitionable EPP and select **Delete**.
3. Click **Ok**.

The deleted nonpartitionable EPP will not be visible under the **Manage System** and cannot be used any further.

*Note:* It is recommended to delete all the events related to the deleted nonpartitionable EPP.
Deleting Nonpartitionable EPP
This section provides you information about the partition. It also provides information on bringing a partition into production. This section has the following topics:

- **12.1 Understanding Partitions**
- **12.2 Managing the Blueprints**
- **12.3 Managing a Gold Image**
- **3.1.1 Overview of Commissioning a Partition**
- **5.5 Commissioning a Partition Image**
- **5.6 Starting a Partition Image**

### 12.1. Understanding Partitions

A partition is a portion of a computer system that is supported by its own hardware resources (such as processors, memory, and input/output) and runs its own operating environment. You can commission multiple partitions on a Partitionable Enterprise Partition Platform (PEPP).

To understand the factors that control the creation and running of partition images see **3.1 Partition Planning**.

**Partition Image Lifecycle**

- Commissioning the partition image
  - Discovering the available resources (blueprints and gold images)
  - Mapping the partition image to appropriate resources and attributes (blueprint, gold image, LUN size, and hyper threading)

  **Note:** Logical unit numbers (LUNs) identify a segment of storage on the enterprise partition platform that span across the internal hard drives.

- Performing starting or stopping operations (soft shutdown, force dump, force halt, soft restart, and hard restart)
- Enabling and disabling the partition image
- Adding multiple images to the partition chassis
- Decommissioning the partition image
12.2. Managing the Blueprints

A blueprint is a software template that is preinstalled on the Forward! hardware that is used to define the characteristics of a partition image. For the commissioning to occur, a blueprint must be associated with gold image. During the commissioning process (to create a partition image) you must select a blueprint and then supply required values for the partition image, such as the partition chassis, partition size, and storage size (LUNs).

This topic discusses about the following:

- 12.2.1 Blueprints, Gold Images, and Commissioning
- 12.2.2 Adding a Blueprint
- 12.2.3 Deleting Blueprints
- 12.2.4 Filtering Blueprints

12.2.1. Blueprints, Gold Images, and Commissioning

Blueprints

Forward! technology provides preconfigured software templates called partition image blueprints ("blueprints," for short). Blueprints define a partition's software resources and make creation of partitions very quick and easy.

You can use a single blueprint to create multiple partitions—for example, multiple partitions running the Windows Server 2012 R2 operating system. Other partitions can use other blueprints—for example, a partition running SUSE Linux Enterprise Server 11 SP3 would use a blueprint supplying that operating system.

The Unisys factory loads blueprints on the enterprise partition platform’s internal storage drives. In some cases
- Blueprints can be downloaded from the Unisys Product Support Site and placed on the internal storage drive.
- Blueprints are created and placed on the internal storage drive when a customer supplies his or her own operating system.

A given blueprint can be associated with only one gold image, that is, one operating system.

**Gold Images**

A blueprint is associated with a “gold image” that provides the partition with the operating system (and perhaps other software) that will run in the partition. A gold image is a static, non-bootable software image. For example, there is a gold image containing the Windows Server 2012 R2 operating system and a gold image containing the SUSE Linux Enterprise Server 11 SP3 gold image.

It is possible for a single gold image to supply the operating system for multiple blueprints. This enables creation of tailored blueprints, for example:

- A blueprint with SUSE Linux Enterprise Server 11 SP3 alone
- A blueprint with SUSE Linux Enterprise Server 11 SP3 plus Hadoop software

Like blueprints, gold images exist on the enterprise partition platform’s internal storage drives. For customer-supplied Windows operating systems, a gold image begins as a customer-supplied .iso version (Img, tar, or ISO file) which is then packaged and placed on the enterprise partition platform’s internal storage drives. For customer-supplied Linux operating systems, a gold image begins as a customer-installed and configured operating system and application environment.

**Commissioning**

The process of creating a partition is known as commissioning. Using the *Forward! Fabric Manager*, an administrator selects the desired blueprint (which has been associated with a given gold image) and then specifies values for hardware resources, such as the size of the partition. The result of commissioning is a running partition.

**12.2.2. 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
- Unisys Support Site (for a Unisys-supplied blueprint)

If you create and add your operating system image to a selected platform, you must also add the corresponding blueprint included in the toolkit for your operating system image. See 6.3 Installing a Customer-Supplied Windows or Linux OS on a Partitionable Enterprise Partition Platform for more information.

To add a blueprint

1. On the Fabric Manager user interface, click Manage System on the left pane. Details screen appears on the right pane.

    - Under Details, click the Software tab.

    The Version Info., Images, and Blueprints tabs appear.

2. Click 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. See 12.2.3 Deleting Blueprints for more information.

    Note: Each blueprint must have a unique name.

4. Click Add.

    The Add Blueprint window appears.

5. Select the desired platform for which you want to add a blueprint.

    Note: To add a blueprint to all the available platforms, select Platform Name.

6. Click Browse.

7. Navigate to the blueprint that you want to add and click Open.

8. Click Ok.

    In the Events tab the status of this activity is listed as INITIATED.

9. After the event status becomes SUCCESS, click refresh button under Blueprints tab.

    The uploaded blueprint appears in the list of available blueprints.

    The status of blueprint upload appears under the Events 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 the refresh button to view the uploaded blueprint.
12.2.3. Deleting Blueprints

Fabric Manager allows you to delete multiple blueprints associated with a platform. When the blueprint is deleted, it is removed from the EPP's SAS drive and delisted from the Fabric Manager user interface.

To delete a blueprint

1. On the Fabric Manager user interface, click **Manage System** on the left pane.

   **Details** screen appears on the right pane.

2. Under **Details**, click the **Software** tab.

   The **Version Info.**, **Images**, and **Blueprints** tabs appear.

3. Click the **Blueprints** tab.

   The available blueprints appear.

4. From the list of blueprints, select the blueprints that you want to delete.

   **Note:** You cannot delete the blueprints that are in use. The **In Use?** column displays the status of the blueprint as ‘Yes’ if it is in use.

   Click **Delete**.

   A message confirming the deletion appears.

5. Click **Ok**.

   A message informing you that the selected blueprint will be deleted appears.

6. Click **Ok**.

   A **SUCCESS** event is generated under Events console when the blueprint is deleted successfully. When the blueprint is deleted, the blueprints tab is refreshed and the deleted blueprint will not be available for commissioning a partition image on the platform.

12.2.4. Filtering Blueprints

Fabric Manager allows you to filter and display the required blueprints from the list of Blueprints.

To filter the blueprints

1. On the Fabric Manager user interface, click **Manage System** on the left pane.

   **Details** screen appears on the right pane.

2. Under **Details**, click the **Software** tab.

   The **Version Info.**, **Images**, and **Blueprints** tabs appear.

3. Click the **Blueprints** tab.

   The list of available blueprints appears.

4. In the **Filter** row, select the desired filter value from the drop-down list. For example, Blueprint1.
Managing the Blueprints

Type the value that you want to filter. For example, Blueprint1.

5. Click Go to apply the filter.

A table of blueprints appears based on your selection.

Notes:
- Click Clear to reset the filter.
- Filtering keywords are not case sensitive.
- You can use the wildcard characters to filter the multiple files with similar names. You can use them to apply the filter based on blueprint name, platform name and the version number.

The following table lists the various wildcard character supported for filtering.

<table>
<thead>
<tr>
<th>Wildcard</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>* or %</td>
<td>Use * or % that matches zero or more characters in a filtering keyword.</td>
<td>The blueprint filtering keyword BluPrin* or BluPrin% filters all the blueprints that contain the characters BluPr and further, for example Blueprint, Blueprint1, Blueprint2.</td>
</tr>
<tr>
<td>_ or ?</td>
<td>Use _ or ? that matches any single character in a filtering keyword.</td>
<td>The filtering keyword Partition_ or Partition? filters all the blueprints which contains any allowed character, for example Partition1, PartitionA.</td>
</tr>
<tr>
<td>#</td>
<td>Use # that matches any single numeric character in a filtering keyword.</td>
<td>The filtering keyword Platform# filters all the blueprints with numbers after Platform, for example Platform1. To filter the blueprints with double digit number after the keyword, insert ##. For example, filtering keyword Platform## could result in Platform11.</td>
</tr>
</tbody>
</table>
### Wildcard Description Example

<table>
<thead>
<tr>
<th>Wildcard</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>@</code></td>
<td>Use <code>@</code> that matches any single alphabet in a filtering keyword.</td>
<td>The filtering keyword <code>Blueprint@</code> filters all the blueprints with alphabets after <code>Blueprint</code>, for example <code>BlueprintA</code>, <code>BlueprintB</code>. To filter the blueprints with double digit alphabet after the keyword, insert <code>@@</code>. For example, filtering keyword <code>Blueprint@@</code> could result in <code>BlueprintAB</code>, <code>BlueprintBC</code>.</td>
</tr>
<tr>
<td><code>[ ]</code></td>
<td>Use <code>[ ]</code> that matches the characters within the brackets of the filtering keyword.</td>
<td><code>Im[ae]ge*</code> The filtering keyword <code>Blu[ae]print*</code> filters all the blueprints having the characters within the brackets, for example <code>Blueprint1</code>, <code>Blueprint2</code>.</td>
</tr>
</tbody>
</table>

### 12.3. Managing a Gold Image

A gold image is a static, non-bootable software image that exists on the hard drive of an enterprise partition platform and will, after the commissioning process, be the source of the software stack residing in a partition (or more formally, a partition image). A gold image is associated with one or more blueprints, providing the blueprints with the desired user software. (For blueprints supplied by Unisys, this association takes place in the factory). For the commissioning to occur, a gold image must be associated with a blueprint.

Based on your needs, you can add or delete the gold images. This topic discusses about the following:

- 12.3.1 Understanding a Gold Image
- 12.3.2 Adding a Gold Image
- 12.3.3 Deleting Gold Images
- 12.3.4 Filtering Images

#### 12.3.1. Understanding a Gold Image

Unisys supplies the following types of gold images:

**OS Gold Image**: A Unisys supplied software image that provides the required version of the operating system to be installed on the partition image.
**Managing a Gold Image**

**s-Par® Installation Tool (EZInstall) gold image**: Unisys supplied software image that contains the s-Par® EZInstall installation tool.

**s-Par® Driver Gold Image**: A Unisys supplied software image that provides the required drivers for the physical card ports (Network Interface Cards and Host Bus Adapters).

**Vendor Driver Gold Image**: A bootable image that provides the drivers for the physical card ports (Network Interface Card and Host Bus Adaptor) assigned to the partition image.

**Platform Diagnostic Gold Image**: A Unisys supplied software image that contains the OEM platform diagnostic tools. The platform diagnostic gold image is handled differently than the other gold images. After the completion of loading the platform diagnostic gold image on the Restore LUN, a command must be sent to s-Par® to initiate using the new platform diagnostic in the service partition. This action does not affect any partition images that are activated and enabled on the platform.

### 12.3.2. 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
- Unisys support site (for the Unisys-supplied gold image)

You can also create and add operating system images to a selected platform. See 6.3 Installing a Customer-Supplied Windows or Linux OS on a Partitionable Enterprise Partition Platform for more information.

To add a Gold Image

1. On the Fabric Manager user interface, click **Manage System** on the left pane.

   **Details** screen appears on the right pane.

2. Under **Details**, click the **Software** tab.

   The Version Info., Images, and Blueprints tabs appear.

3. Click the **Images** tab.

   The list of already available images appear.
4. Click **Add**.
   The **Add Image** window appears.
5. Select the desired platform for which you want to add an image.
   
   **Notes:**
   - To add an image to all the available platforms, select **Platform Name**.
   - Fabric Manager does not allow you to simultaneously upload the multiple gold images to a platform.
6. Click **Browse**.
7. Navigate to the image that you want to add and click **Open**.
8. Click **Ok**.
   In the **Events** tab the status of this activity is listed as **INITIATED**.
9. After the event status becomes **SUCCESS**, click refresh button under **Images** tab.
   
   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 the refresh button to view the uploaded image.

Gold image gets added to the list of images available in the Fabric Manager.

### 12.3.3. Deleting Gold Images

Fabric Manager allows you to delete multiple gold images associated with a platform. When the Gold Image is deleted, it is removed from the EPP’s SAS drive and delisted from the Fabric Manager user interface.

To delete gold images
1. On the Fabric Manager user interface, click **Manage System** on the left pane. **Details** screen appears on the right pane.
2. Under **Details**, click the **Software** tab.
   
   The **Version Info.**, **Images**, and **Blueprints** tabs appear.
3. Click the **Images** tab.
   
   The list of already available images appear.
4. From the list of images, select the images that you want to delete.
   
   **Note:** You cannot delete the Gold images that are in use. The **In Use?** column displays the status of the Gold Image as ‘Yes’ if it is in use.
5. Click **Delete**.
   
   A message confirming the deletion appears.
6. Click **Ok**.
   
   A message informing you that the selected image will be deleted appears.
Managing a Gold Image

7. Click **Ok**.

A **SUCCESS** event is generated under Events console when the image is deleted.

12.3.4. Filtering Images

Fabric Manager allows you to filter and display the required images from the list of images.

To filter the images
1. On the Fabric Manager user interface, click **Manage System** on the left pane.
   Details screen appears on the right pane.
2. Under **Details**, click the **Software** tab.
   The **Version Info.**, **Images**, and **Blueprints** tabs appear.
3. Click the **Images** tab.
   The list of available images appears.
4. In the **Filter** row, select the desired filter value from the drop-down list. For example, Image1.
   Type the value that you want to filter. For example, Image1.
5. Click **Go** to apply the filter.

A table of images appears based on your selection.

**Notes:**
- Click **Clear** to reset the filter.
- Filtering keywords are not case sensitive.
- You can use the wildcard characters to filter the multiple files with similar names. You can use them to apply the filter based on image name, platform name and the version number.

The following table lists the various wildcard character supported for filtering.

<table>
<thead>
<tr>
<th>Wildcard</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>* or %</td>
<td>Use * or % that matches zero or more characters in a filtering keyword.</td>
<td>The image filtering keyword <strong>Im</strong> or <strong>Im%</strong> filters all the images that contain the characters <strong>Im</strong> and further, for example <strong>Img</strong>, <strong>Image1</strong>, <strong>Image2</strong>.</td>
</tr>
<tr>
<td>Wildcard</td>
<td>Description</td>
<td>Examples</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
<td>----------</td>
</tr>
<tr>
<td>_ or ?</td>
<td>Use _ or ? that matches any single character in a filtering keyword.</td>
<td>The filtering keyword <code>Partition_</code> or <code>Partition?</code> filters all the images which contains any allowed character, for example <code>Partition1</code>, <code>PartitionA</code>.</td>
</tr>
<tr>
<td>#</td>
<td>Use # that matches any single numeric character in a filtering keyword.</td>
<td>The filtering keyword <code>Platform#</code> filters all the images with numbers after <code>Platform</code>, for example <code>Platform1</code>. To filter the images with double digit number after the keyword, insert <code>##</code>. For example, filtering keyword <code>Platform##</code> could result in <code>Platform11</code>.</td>
</tr>
<tr>
<td>@</td>
<td>Use @ that matches any single alphabet in a filtering keyword.</td>
<td>The filtering keyword <code>Image@</code> filters all the images with alphabets after <code>Image</code>, for example <code>ImageA</code>, <code>ImageB</code>. To filter the images with double digit alphabet after the keyword, insert <code>@@</code>. For example, filtering keyword <code>Image@@</code> could result in <code>ImageAB</code>, <code>ImageBC</code>.</td>
</tr>
<tr>
<td>[]</td>
<td>Use [] that matches the characters within the brackets of the filtering keyword.</td>
<td>The filtering keyword <code>Im[a][e][g]e*</code> filters all the images having the characters within the brackets, for example <code>Image1</code>, <code>Image2</code>.</td>
</tr>
</tbody>
</table>

### 12.4. Overview of Commissioning a Partition

Commissioning is the process of creating a partition image by using the Forward! 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; then you specify values for any additional required attributes, such as the partition image’s:

- Name
- Partition chassis
Overview of Commissioning a Partition

- Size: Extra Small, Small, Medium, Large, Extra Large, Extra Extra Large, or Maximal
- Memory size (a default value is provided which you may change)
- Boot disk storage space (LUN size)

The Fabric Manager then creates the partition image. As a result of the commissioning process, the partition image appears in the left navigation pane of the Fabric Manager, is enabled, and is in a running state. 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 commissioning screen where you select the chassis, size, and so forth.
12.5. Commissioning a Partition Image

Ensure that the required resources such as blueprint and gold image are available. See 3.1 Partition Planning for more information. Additionally, the Fabric Manager user interface provides information about the different partition images that you can commission on a particular platform. See 11.2 Viewing Configuration Information of a Platform for more information.

Notes:

• 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 B, Worksheet for Commissioning, to learn more about the worksheet.

• 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, click Manage System on the left pane, expand <Forward-System> and then select the required platform on which you want to commission the partition image. Details screen appears on the right pane.

2. On the Details pane, click Commission. Alternatively, click the arrow next to the platform and click Commission.

A message informing that the system is discovering the resources for the commissioning appears.

After the discovering the required resources to commission a partition image, the Commission window appears.

3. In the Select Blueprint tab, select the desired blueprint and click Next.

Note: The Next button is enabled only when a blueprint is selected.

4. In the Set Basic Info. tab, provide appropriate information in the following fields:

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

     Note: The maximum length of the partition image name can be up to 15 alphanumeric characters along with “-“ . The name cannot start with the character “-“.

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

     Note: The Host Computer Name should be unique across the fabric if partition images are connected within the same customer LAN subnet.

   • Description: Type a description for the partition image.
Note: Provide a meaningful description for the partition image. The maximum length of the 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.

5. Click **Next**.

6. In the **Allocate Resource** tab, select the appropriate values in the following fields:

   - **Partition Chassis**: Choose the appropriate partition chassis; for example, Chassis-B.
   - **Partition Size**: Choose the appropriate partition size; for example, Medium.

   The available options are based on the value that you have selected in the **Partition Chassis** field.

   For example, if you have selected **Chassis-A** in the **Partition Chassis** field, the available partition size could be **Small**, **Medium**, **Large**, and **Maximal**. If you have selected **Chassis-B** in the **Partition Chassis** field, the available partition size could be **Small** and **Medium**.

   - **Configuration of <name of the chassis and partition size value>**:

     Table 5–1 displays the various fields under this section. These fields are automatically populated based on the values that you have selected in the **Partition Chassis** and **Partition Size** fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cores</td>
<td>Displays the number processor cores assigned for the partition image.</td>
</tr>
<tr>
<td>Memory (&lt;x-y&gt; GB)</td>
<td>Displays the default memory allocated for the partition image.</td>
</tr>
<tr>
<td></td>
<td>This is an editable field.</td>
</tr>
<tr>
<td></td>
<td>You can also choose a different memory size. x and y denote the minimum</td>
</tr>
<tr>
<td></td>
<td>and maximum memory sizes (in GB) that you can choose.</td>
</tr>
<tr>
<td></td>
<td>Information about the remaining memory in the platform is displayed along</td>
</tr>
<tr>
<td></td>
<td>with this field. You can use the increment and decrement operator to</td>
</tr>
<tr>
<td></td>
<td>increase and decrease the memory beyond the default memory. This value</td>
</tr>
<tr>
<td></td>
<td>changes automatically based on the memory size that you have selected.</td>
</tr>
<tr>
<td>NIC Ports and HBA Ports</td>
<td>Displays information about the NIC and HBA ports. Click the Show Legends</td>
</tr>
<tr>
<td></td>
<td>tab to learn more about the displayed information.</td>
</tr>
</tbody>
</table>

**Note:** You can view the vendor and the device type details of a particular port. If you click a port, the vendor and device type information of the selected port appears under the **Details: Slot** section.
The following is an example of the **Allocate Resource** tab:

- **LUN Selection**: Choose the desired LUN size.

**Notes:**

- A LUN size of at least 60 GB if you are commissioning a Windows partition image from Unisys-supplied images.
- A LUN size of at least 20 GB if you are commissioning a Linux partition image from Unisys-supplied images.
- 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. For more information, see 6.3.5 Creating a Customer-Supplied Linux Operating System Image.

- **Enable Hyper-Threading (HT):** If you select this check box, two logical processors per core are selected. By default, the HT option is disabled for 4S platforms and enabled for 2S platforms.

7. Click **Next**.

8. In the **Set State & Credentials** tab, select the appropriate options in the following fields:

   - **Initial State (Platform Reboot):** Enables you to identify whether or not the partition image is started after a platform reboot. The available values are **Running** and **Stopped**. The default value is **Running**.
     
     **Note:** The **Initial State** value does not apply to the partition images that are currently disabled.

   - **Login Credentials:** Enables you to type the appropriate password in the **Password** field and confirm the password in the **Confirm Password** field. These fields are 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 was captured as part of the image you created. Use that information to access your Linux partition image; the input in the host computer name and password fields during commissioning is ignored.

9. Click **Next**.

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

10. Click **Submit**.

   A message informing you that the commissioning process will begin shortly appears.

11. Click **OK**.

   Commissioning of the new partition image begins. After the commissioning is complete, the newly commissioned partition image appears in the Manage System pane under the respective platform. You can also monitor the progress of the commissioning process by referring to the logs being generated under the **Events** tab.

You can set up the Windows and Linux operating environments after Commissioning a partition image. See 6.1 Completing Installation and Configuration of a Unisys-supplied Windows Partition Image and 6.2 Completing Installation and Configuration of a Unisys-
supplied Linux Partition Image for information.

### 12.6. Starting a Partition Image

**Prerequisite:** The EPP has to be powered on and the desired partition image is in a stopped state.

To start a partition image:

1. On the Fabric Manager user interface click **Manage System** on the left pane, expand `<Forward-System>` to view various platforms.
2. Expand the desired platform and then click the partition image that you want to start.
   - The **Details** pane displays the information about the selected partition image.
3. Click **Start**.
   - The status of the partition image changes to **RUNNING**.
Starting a Partition Image
Section 13
Managing Partitions

This section explains various power control operations such as starting, stopping, and restarting the partition image, and editing the partition image attributes in the following topics:

• 13.1 Understanding Status of Partition Images
• 13.2 Viewing the Partition Summary
• 13.3 Accessing a Partition Desktop
• 13.4 Changing the User/Password of the Partition Image Console
• 13.5 Deleting the User/Password of the Partition Image Console
• 13.6 Starting and Shutting down the Partition Images
• 13.7 Enabling a Partition Image
• 13.8 Disabling a Partition Image
• 13.9 Decommissioning a Partition Image
• 13.10 Adding Multiple OS Images to a Partition Chassis
• 13.11 Editing Partition Image Attributes
• 13.12 Resizing Partition Images

Note: You cannot perform or view any options if the status of the partition image is Unknown.

13.1. Understanding Status of Partition Images

The following table lists various status icons of a partition image.

<table>
<thead>
<tr>
<th>Icons</th>
<th>Partition Image Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nonpartitionable EPP image</td>
<td>Unknown</td>
<td>The Fabric Manager is unable to recognize the status of the host.</td>
</tr>
<tr>
<td>🔄</td>
<td>Running</td>
<td>The operating system on the host is up and running.</td>
</tr>
</tbody>
</table>
## Understanding Status of Partition Images

<table>
<thead>
<tr>
<th>Icons</th>
<th>Partition Image Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="icon" alt="Stopped" /></td>
<td>Stopped</td>
<td>Stopped state indicates that the operating system on the host stopped working.</td>
</tr>
<tr>
<td><img src="icon" alt="Partitionable EPP image" /></td>
<td>Unknown</td>
<td>The Fabric Manager is unable to recognize the status of the partition image.</td>
</tr>
<tr>
<td><img src="icon" alt="Running" /></td>
<td>Running</td>
<td>The partition image is defined and the s-Par® partition chassis (processor cores, memory, ports) and LUN association with partition image is available. The partition image is running.</td>
</tr>
<tr>
<td><img src="icon" alt="Stopped" /></td>
<td>Stopped</td>
<td>The partition image is defined and the s-Par® partition chassis (processor cores, memory, ports) and LUN association with partition image is available. The partition image is not running.</td>
</tr>
<tr>
<td><img src="icon" alt="Enabled" /></td>
<td>Enabled</td>
<td>The resources are allocated to the partition image.</td>
</tr>
<tr>
<td><img src="icon" alt="Disabled" /></td>
<td>Disabled</td>
<td>The resources are allocated to the partition image are freed up except LUN.</td>
</tr>
<tr>
<td><img src="icon" alt="In Progress" /></td>
<td>In Progress</td>
<td>Transition states of the partition image such as Activating, Deactivating, Starting, Stopping, and Inactive.</td>
</tr>
<tr>
<td><img src="icon" alt="Inactive" /></td>
<td>Inactive</td>
<td>The partition image is defined (LUN is allocated) and associated with a partition in the platform but does not have an s-Par® partition chassis (processor cores, memory, ports) association. The s-Par® partition chassis is available for use by another partition image.</td>
</tr>
<tr>
<td><img src="icon" alt="Starting" /></td>
<td>Starting</td>
<td>An intermediate state between the stopped and running states of a partition image.</td>
</tr>
</tbody>
</table>
13.2. Viewing the Partition Summary

The partition image summary provides you the information about different attributes of the partition image. The following table summarizes the attributes displayed, their description and examples.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Denotes the name assigned to a partition image that is commissioned on the platform.</td>
<td>Application1</td>
</tr>
<tr>
<td>Description</td>
<td>Provides the description of the partition image that is commissioned on the platform.</td>
<td>This partition image hosts Application1.</td>
</tr>
</tbody>
</table>
### Viewing the Partition Summary

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial State</td>
<td>Denotes the initial state property that is set while commissioning a partition image. This attribute enables you to identify whether or not the partition image is started after a platform reboot.</td>
<td>RUNNING</td>
</tr>
<tr>
<td>Number</td>
<td>Denotes a unique numerical value that is assigned by the user to a partition image commissioned on a platform. It represents the third octet of the FM-LAN IP address, IP-LAN IP address, and HD-LAN IP address.</td>
<td>2</td>
</tr>
<tr>
<td>Blueprint Name</td>
<td>Indicates the name of the blueprint that is used for commissioning the partition image on a platform.</td>
<td>RHEL64-Blueprint</td>
</tr>
<tr>
<td>Platform Name</td>
<td>Denotes the platform name on which the partition image is commissioned.</td>
<td>BankA</td>
</tr>
<tr>
<td>LUN Size</td>
<td>Denotes the LUN size of the partition image that is commissioned on EPP.</td>
<td>40.0 GB</td>
</tr>
<tr>
<td>Hyper-Threading</td>
<td>Denotes if Hyper Threading is enabled for the partition image. If enabled, two logical processors per core are selected.</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

### Partition Image Overview

<table>
<thead>
<tr>
<th>Health</th>
<th>Denotes the status of the partition image health. It can be Ok, Warning, or Critical.</th>
<th>Critical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current State</td>
<td>Indicates the current state of the partition image state. For more information on different states, see 13.1 Understanding Status of Partition Images.</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

### Processor
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Denotes the processor brand, product line, model number, and the operating frequency of the platform on which the partition image is commissioned.</td>
<td>Intel(R) Xeon(R) CPU E5-2680 0 @ 2.70GHz</td>
</tr>
<tr>
<td>Frequency</td>
<td>Indicates the processor frequency of the platform on which the partition image is commissioned.</td>
<td>2.7 GHz (per processor)</td>
</tr>
<tr>
<td><strong>Configuration of Chassis-X (size)</strong></td>
<td><strong>X</strong> denotes the chassis selected and <strong>size</strong> denotes the size of the partition image.</td>
<td><strong>Configuration of Chassis-B (Medium)</strong></td>
</tr>
<tr>
<td>Cores</td>
<td>Displays the number processor cores assigned for the partition image.</td>
<td>4</td>
</tr>
<tr>
<td>Memory</td>
<td>Displays the memory allocated for the partition image. You can also choose a different memory size while commissioning a partition image.</td>
<td>40 GB</td>
</tr>
<tr>
<td>NIC Ports</td>
<td>Displays the information about the number of NIC ports assigned for the partition image.</td>
<td>2</td>
</tr>
<tr>
<td>HBA Ports</td>
<td>Displays the information about the number of HBA ports assigned for the partition image.</td>
<td>1</td>
</tr>
<tr>
<td><strong>Port &amp; Config. Preview</strong></td>
<td>Provides the preview of the ports selected and the legends for the partition image when you click Port &amp; Config. Preview.</td>
<td></td>
</tr>
<tr>
<td><strong>IP Addresses</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FM-LAN</td>
<td>Displays the FM-LAN address of the partition image.</td>
<td>172.29.1.2</td>
</tr>
<tr>
<td>IP-LAN</td>
<td>Displays the IP-LAN address of the partition image.</td>
<td>172.31.1.2</td>
</tr>
<tr>
<td>HD-LAN</td>
<td>Displays the HD-LAN address of the partition image.</td>
<td>172.30.1.2</td>
</tr>
</tbody>
</table>

To view the partition summary
1. On the Fabric Manager user interface, click **Manage System** on the left pane, and expand `<Forward-System>` to view the platforms.

2. Expand the desired platform and then click the partition image that you want to view.

   The **Details** pane displays the information about the selected partition image.

   The following figure provides the summary of the selected partition image.

---

### 13.3. Accessing a 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
  - rcpwinbind 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.
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 following table lists the default user credentials.

<table>
<thead>
<tr>
<th>User</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>Administer4Me</td>
</tr>
<tr>
<td>Operator</td>
<td>Operate4Me</td>
</tr>
</tbody>
</table>

**Note:** Remember to log out and close the console when you are done with your session.
13.4. Changing the User/Password of the Partition Image Console

You can change the user/password access to the partition image console (sometimes referred to as Partition Desktop). If the user is not yet added to the Samba server (part of the Linux distribution package), you can add an existing user of the FMP to the Samba server and assign and change the password. When you run the authentication service on the FMP, it identifies the user credentials along with the passwords that are allowed to log in through the partition desktop.

To change the credentials of the user

1. Log in to the Fabric Management Platform desktop, and open a new terminal session as a root user.
   (If you are connecting remotely, use a tool like PuTTY or the remote desktop function of the Fabric Management Platform, and login as root user. The default root user login is root/Administer4Me.)

2. Use the following command to ensure that the status of the Samba server is “Running”.
   ```
   # rcsmb <status | start>
   ```
   Use “status” to check Samba server status and “start” to start the Samba server if it is not running.

3. Use the following command to ensure that the status of authentication service of Samba server “winbind” is “Running”.
   ```
   # rcwinbind <status | start | stop | restart>
   ```
   Use “status”, “start”, “stop” and “restart” commands to check the status, start the service, stop the service, and restart the service respectively.

4. Use the following command to list all the Samba users.
   ```
   # pdbedit -L
   ```
   administrator:1000:Administrator
   operator:1001:operator appears. “administrator” and “operator” are the users that are available in the Samba server.

5. If a user is not listed in step 4, add a user to the Samba server as follows:
   a. Use the following command to add a user.
      ```
      useradd user1
      ```
      Where “user1” is the user added to FMP.
   b. Use the following command to assign the password to user:
      ```
      smbpasswd -a user1
      ```
      New SMB password: appears.
   c. Type the new SMB password, and press Enter.
      Reenter New Password: appears.
   d. Type the password again, and press Enter.
Password changed. appears.
e. Check if the user is added to the Samba server by executing the following command:

```
# pdbedit -L
administrator:1000:Administrator
user1:1005:
operator:1001:operator appears with all the available users.
user1:1005: in command prompt confirms that user is added Samba server successfully.
```

6. If the user is listed in step 4, you can change the password as follows:
   a. Use the following command to change the user password.

```
smbpasswd -a user1
```

New SMB password: appears. Where “user1” is the user added to FMP.

b. Type the new SMB password, and press Enter.

Reenter New Password: appears.

c. Type the password again, and press Enter.

Password changed. appears.

### 13.5. Deleting the User/Password of the Partition Image Console

To delete the credentials of the user

1. Log in to the Fabric Management Platform desktop, and open a new terminal session as root user.
   (If you are connecting remotely, use a tool like PuTTY or the remote desktop function of the Fabric Management Platform, and login as a root user. The default root user login is root/Administer4Me).

2. Use the following command to ensure that the status of the Samba server is “Running”.

```
# rcsmb <status | start>
```

Use “status” to check Samba server status and “start” to start the Samba server if it is not running.

3. Use the following command to ensure that the status of the authentication service of Samba server “winbind” is “Running”.

```
# rcwinbind <status | start | stop | restart>
```

Use “status”, “start”, “stop” and “restart” commands to check the status, start the service, stop the service and restart the service respectively.

4. Use the following command to list all the Samba users:

```
# pdbedit -L
```
administrator:1000:Administrator
operator:1001:operator appears. "administrator" and "operator" are the users that are available in the Samba server.

5. To delete the user, use the following command:
   
   ```bash
   # userdel -r user1
   ```
   
   no crontab for user1 appears confirming the user the deletion.

### 13.6. Starting and Shutting down the Partition Images

This section has the following topics:

- **5.6 Starting a Partition Image**
- **13.6.2 Performing a Soft Restart of a Partition Image**
- **13.6.3 Performing a Hard Restart of a Partition Image**
- **13.6.4 Gracefully Shutting Down a Partition Image**
- **13.6.5 Shutting Down Multiple Partition Images**
- **13.6.6 Performing a Force Halt of a Partition Image**
- **13.6.7 Performing Force Dump on a Partition Image**

#### 13.6.1. Starting a Partition Image

**Prerequisite:** The EPP has to be powered on and the desired partition image is in a stopped state.

To start a partition image

1. On the Fabric Manager user interface click Manage System on the left pane, expand `<Forward-System>` to view various platforms.
2. Expand the desired platform and then click the partition image that you want to start. The Details pane displays the information about the selected partition image.
3. Click Start. The status of the partition image changes to RUNNING.

#### 13.6.2. Performing a Soft Restart of a Partition Image

Soft restart is an orderly shutdown and restart of the partition image.

To perform a soft restart

1. On the Fabric Manager user interface, click Manage System on the left pane, expand `<Forward-System>` to view various platforms.
2. Expand the desired platform and then click the partition image you want to soft restart.
The **Details** pane displays the information about the selected partition image.

3. Point to **Advanced** and click **Soft Restart**.
The partition image shuts down followed by a restart.

**Notes:**
- Advanced tab is only present if the partition is running.
- When the partition image restarts, the initial state is not retained.

### 13.6.3. Performing a Hard Restart of a Partition Image

Hard restart is an unorderly shutdown and restart of the partition image.

To perform a hard restart
1. On the Fabric Manager user interface, click **Manage System** on the left pane, expand `<Forward-System>` to view various platforms.
2. Expand the desired platform and then click the partition image you want to hard restart.
   The **Details** pane displays the information about the selected partition image.
3. Point to **Advanced** and click **Hard Restart**.
   
   **Notes:**
   - Advanced tab is only present if the partition is running.
   - When the partition image restarts, it returns to the initial state.

### 13.6.4. 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, click **Manage System** on the left pane, expand `<Forward-System>` to view various platforms.
2. Expand the desired platform and then click the partition image you want to shut down gracefully.
   The **Details** pane displays the information about the selected partition image.
3. Click **Soft Shutdown**.
   The status of the partition image changes to Stopped and Disabled.

### 13.6.5. Shutting Down Multiple Partition Images

You can shut down multiple partition images using one of the following options:

**Option 1:** Shutting down partition images that are running on the same platform
If you want to shut down all the partition images that are running on a single platform, perform a Soft Shutdown operation on that platform. See 10.3 Performing Soft Shutdown on a Platform.

If you want to shut down a few selected partition images that are running on a single platform, you should shut them down one by one. Fabric Manager does not allow you to shut down these partition images at the same time. It is strongly recommended to gracefully shutdown the partition images as this operation prevents data loss.

**Option 2**: Shutting down partition images that are running on multiple platforms

If you want to shutdown partition images that are distributed across various platforms, you should shut them down one by one across different platform at the same time. It is strongly recommended to gracefully shutdown the partition images as this operation prevents data loss.

### 13.6.6. Performing a Force Halt of a Partition Image

Force Halt is an unorderly shutdown of the partition image.

**Caution**

Avoid performing Force halt unless required. This operation may result in data loss.

To perform a Force Halt

1. On the Fabric Manager user interface, click Manage System on the left pane, expand `<Forward-System>` to view various platforms.
2. Expand the desired platform and then click the partition image you want to Force Halt.
   The Details pane displays the information about the selected partition image.
3. Point to Advanced and click Force Halt.
   The partition image shuts down and the status of the partition image changes to STOPPED.

   **Note**: Advanced tab is only present if the partition is running.

### 13.6.7. Performing Force Dump on a Partition Image

Force dump is an automatic dump of the operating system, unorderly shutdown, and reset of the partition image. Use the force dump option to get operating system dependent diagnostic dump.

To perform a force dump
1. On the Fabric Manager user interface, click **Manage System** on the left pane, expand `<Forward-System>` to view various platforms.

2. Expand the desired platform and then click the partition image you want to force dump.
   
The Details pane displays the information about the selected partition image.

3. Point to **Advanced** and click **Force Dump**.
   
The status of the partition image returns to the initial state.

   *Note:* Advanced tab is only present if the partition is running.

### 13.7. Enabling a Partition Image

Enabling a partition image is a process by which you select the partition image that should be currently active on a chassis. It also assigns the hardware resources (processor cores, memory, and I/O ports) required by the partition image to the chassis. Once the partition image is enabled, the assigned hardware resources are unavailable for other chassis.

**Notes:**

- Fabric Manager does not allow you to enable a partition if the required resources are not available.
- Partition image is enabled by default. You can enable the partition image if it in disabled state.

To enable a partition image

1. On the Fabric Manager user interface, click **Manage System** on the left pane, expand `<Forward-System>` to view various platforms.

2. Expand the desired platform and then click the partition image that you want to enable.

3. On the **Details** pane, click **Enable**.
   
The status of the partition image changes to **Running**.

### 13.8. Disabling a Partition Image

Disabling a partition image is the process by which the s-Par® association of the partition image (LUN) along with the partition chassis (processor cores, memory and I/O ports) is released and the partition chassis is available for use by another partition image. Disable a partition image when you want to make its resources available to other partition images but do not want to permanently delete the partition image.

To disable a partition image

1. On the Fabric Manager user interface, click **Manage System** on the left pane, expand `<Forward-System>` to view various platforms.

2. Expand the desired platform and then click the partition image that you want to disable.
3. On the **Details** pane, click **Disable**.

The status of the partition image changes to Stopped. The partition image no longer appears in the display.

### 13.9. Decommissioning a Partition Image

Decommissioning a partition image deletes the partition image. This process releases the resources back to the resources pool.

**Prerequisite:**

Partition desktop of the partition image that is being decommissioned must have been closed.

This action destroys the selected partition image and you can no longer access it.

**Note:** *Prior to decommissioning a partition image, you should use a disk scrubber tool of choice to scrub (remove or render unreadable) the contents of the boot disk to prevent undesirable recovery of data.*

To decommission a running partition image

1. On the Fabric Manager user interface, click **Manage System** on the left pane, expand `<Forward-System>` to view various platforms.

2. Expand the desired platform and then click the partition image that you want to decommission.

   The **Details** pane displays the information about the selected partition image.

3. Click **Decommission**.

   A message asking if you want to stop the partition image before you begin the decommissioning process appears.

4. Click **OK**.

   The status of the partition image changes to **STOPPED**. Events for initiation and completion are logged and displayed in the event console.
13.10. Adding Multiple OS Images to a Partition Chassis

Fabric Manager allows you to add multiple OS images to a partition chassis. This means that, in a platform, single partition chassis is shared among multiple partition images as long as only one of the partition images is enabled at a time.

Using the Fabric Manager, you can disable the partition images that are already enabled. Disabling all the partition images that share the same chassis enables you to commission multiple partition images that use the same chassis. (Disabling a partition image frees-up its hardware resource blocks; however the partition image content is persisted on mass storage for possible future use. That means you can enable the partition image later.)

You can assign multiple partition images to a partition chassis.

**Prerequisite:** Additional resources required to add multiple OS images to a partition chassis are available.

To add multiple images to a partition chassis

1. On the Fabric Manager user interface, click **Manage System** on the left pane, expand `<Forward-System>` to view various platforms.
2. Expand the desired platform and then click the partition image that you want to add multiple OS images to.
3. On the Details pane, click **Disable**.
   The status of the partition image changes to **Disabled**.
4. Commission a new partition image, using the same partition chassis as the partition image that you disabled. For information, see 5.5 Commissioning a Partition Image.

   **Note:** When you commission a partition image, ensure that you select the partition image chassis that belonged to the partition image that you disabled. For example, if the chassis of the partition image that you disabled was A, then choose A as partition image chassis during commissioning.

13.11. Editing Partition Image Attributes

Depending on your role, you can edit the name, description, and initial state of a partition image. It is recommended to back up the configuration settings before editing the partition image attributes. See Section 18, Backup and Restore, for more information on how to back up.

**Note:** You cannot edit the attributes if the status of the partition image is Unknown.

To edit partition image attribute

1. On the Fabric Manager user interface, click **Manage System** on the left pane, and expand `<Forward-System>` to view various platforms.
2. Expand the desired platform and then click the partition image to edit its attributes.
3. In the **Details** pane, click **Edit**. Alternatively, click the arrow next to the partition image, and click **Edit**. The Edit Partition Image window appears.

4. Edit one or more of the following fields as needed:
   - **Partition Name**: Modify the partition image name. This should be unique across the fabric since it is required to monitor the state and health of the partition images within the FM LAN subnet. This field is mandatory.
     
     **Note:** The maximum length of the partition image name can be up to 15 alphanumeric characters. The name cannot start with the character “-” (hyphen).
   - **Partition Description**: Modify the description.
     
     **Note:** The maximum length of the description can be up to 256 alphanumeric characters, which may include, “–” (hyphen), space, and “.” (dot). The length of any word in the description should not exceed 20 characters.
   - **Initial State**: Select the initial state (this field enables you to identify whether or not the partition image is started after a platform reboot) from the list.
     
     **Note:** If the partition image is in a Stopped state, the Hyper-Threading (HT) check box is also displayed. If you select this check box, two logical processors per core are selected. Do not select this option for a 4-socket EPP.

5. Click **Save**.

   A message asking if you want to save changed attributes appears.

6. Click **OK**.

   The modified attributes are saved and displayed in the partition image **Summary** tab.

### 13.12. Resizing Partition Images

Using the Fabric Manager, you can resize partition images in the following situations:

- The allocated resources (memory size and cores) for a partition image are not sufficient.
- The resources of a partition image are under-utilized.

**Recommendations**

- Back up your data before resizing a partition image. It prevents loss of data from any catastrophic failures during the resizing process. See **Section 18, Backup and Restore**, to know more about the backup procedures.
- Resize the partition image unless the existing setup currently causes problems or may cause problems soon. For example, the partition image has utilized the memory space completely or is expected to add enough data to overfill.
- See **3.1 Partition Planning** and the other subsections to know more about the partition image sizes and planning the partition sizes.
**Prerequisites**

- Required additional resources are available on the platform.
- The partition image should be in Stopped state.

To resize a partition image

1. On the Fabric Manager user interface, click **Manage System** on the left pane, and expand `<Forward-System>` to view various platforms.

2. Expand the desired platform, and then click the partition image to resize and edit the attributes.

3. In the **Details** pane, click **Edit**.
   Alternatively, click the arrow next to the partition image and click **Edit**.
   The **Edit Partition Image** window appears.

4. (Optional) Edit the partition name and partition description values.

5. In the **Partition Size** field, select the required size for resizing.
   **Note:** Only the available sizes are displayed for selection.

6. (Optional) Select an initial state (this field enables you to identify whether or not the partition image is started after a platform reboot) value from the list.

7. Under the **Configuration of <name of the chassis and partition size value>** section, enter the memory value using the increment and decrement operator beyond the default memory. You can also use the edit box to enter the memory value manually. This value changes automatically based on the partition size that you have selected.

8. Based on the configuration, select the Hyper-Threading (HT) option. If you select HT, two logical processors per core are selected.

9. Click **SAVE**.
   The selected partition image is now resized.
Section 14
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.

- **14.1 Hardening Your Operating System**
- **14.2 Forward! Hardening Tools for Windows and Linux**
- **14.3 Using the Forward! Hardening Tool for Windows**
- **14.4 Using the Forward! Hardening Tool for Linux**

14.1. Hardening Your Operating System

To ensure that your 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 Forward! 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

Leveraging its extensive experience in the industry and understanding of the needs of the Forward! fabric, Unisys integrates its knowledge with best practices 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
  – Windows Server 2012
• Red Hat documentation for Red Hat Enterprise Linux (RHEL), for example
  – https://access.redhat.com/site/documentation/Red_Hat_Enterprise_Linux/
• SUSE documentation for SUSE LINUX Enterprise Server (SLES), for example
• 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

  Note: This website may not be accessible from all global locations.

14.2. *Forward!* Hardening Tools for Windows and Linux

Using recommendations by various security organizations, Unisys implements over 200 security settings that can be configured to provide various levels of security for supported operating systems.

For the predefined security levels recommended for *Forward!* environments, Unisys developed a series of configuration files describing three levels of hardening:

• 0 – Minimally hardened, recommended by or provided by the operating system vendor.
• 1 – Medium hardened, defined by Unisys as the recommended hardened state for operating systems commissioned with Unisys-supplied blueprints.
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.

These configuration files can be applied on a target operating system using the Forward! Hardening Tools.

**Note:** 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.

You can also use the Hardening Tools to audit your current operating system security settings, generate a report, or applying a different configuration file to remove or restore hardening parameter settings.

The 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 14.1 Hardening Your Operating System).

### 14.3. Using the Forward! Hardening Tool for Windows

The 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.
- **<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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>–reportOnly</td>
<td>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.</td>
</tr>
<tr>
<td>–noRollback</td>
<td>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&lt;timestamp&gt;.xml). Include this option to omit the creation of a rollback file.</td>
</tr>
<tr>
<td>–file &lt;file name&gt;</td>
<td>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&lt;OS version&gt;.xml) is used. This option is ignored if the –level parameter is set to 0.</td>
</tr>
<tr>
<td>–verbose</td>
<td>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.</td>
</tr>
</tbody>
</table>

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

14.4. Using the Forward! Hardening Tool for Linux

The 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`
Using the *Forward! Hardening Tool for Linux*

- 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/confgs/Harden-SLES11SP3-Level1-default.cfg`
Section 15
Managing Events

Events provide an overview of the activities of the fabric.

Using the Fabric Manager user interface you can view, acknowledge, close, and re-open the events.

This section has the following topics:

- 15.1 Understanding Events
- 15.2 Event Lifecycle
- 15.3 Call Home Service
- 15.4 Viewing Events
- 15.5 Filtering Events
- 15.6 Accepting Events
- 15.7 Closing Events
- 15.8 Re-Opening Events
- 15.9 Re-Sending Failed Call Home Events
- 15.10 Editing Event Log Retention Period

15.1. Understanding 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. The Fabric Manager maintains a single consolidated event log for all events occurring in all platforms and partitions in the fabric.

Events generated in the Fabric Manager are broadly classified into general events and Call Home events.

**General Events**: General events are audit and system generated events. These are user actions, such as user login, user logout, powering on a platform, commissioning a partition image, and so on. These events are generated by the Fabric Manager console.

**Call Home Events**: Call Home events are Fabric Management Platform (FMP) events, s-Par® events and platform management console events, which are critical in nature. For example, events generated during FRU replacements.
Note: Periodically, Fabric Manager sends a test packet to the Call Home service to check that the system is capable of sending a Call Home packet to Unisys when required. The frequency is once every seven days.

Event Status

Each event is assigned to one of the following operation statuses which indicate what action has been performed on the event:

• OPEN: This status is assigned to an event immediately after it is generated. This is the default status.

• ACCEPTED: User assigns this status to an OPEN event indicating that corrective action is being taken. It is recommended to accept events when they occur.

• CLOSED: User assigns this status to an OPEN or ACCEPTED event after taking corrective actions.

• Successful Acknowledgement (SACK): The Unisys Service Center assigns this status to a Call Home event and processes the request after validating the information sent. A SACK on a periodic test packet or Communication Test packet implies that the Unisys front-end servers acknowledge receiving the packet, but no validation of the content of the packet has taken place.

• Non-Successful Acknowledgement (NACK): The Unisys Service Center assigns this status to a Call Home event if the Unisys Service Center recognizes the information sent as invalid.

• SEND: FAILED: The fabric assigns this status to a Call Home event if the fabric is unable to send the information to the Unisys Service Center.

• SEND: IN-PROGRESS: The fabric assigns this status to a Call Home event when the fabric begins sending the event to the Unisys Service Center.
15.2. Event Lifecycle

General Events

![Event Lifecycle Diagram]

**Figure 15–1. General Event Lifecycle**
15.3. Call Home Service

Unisys Call Home is a software application that automatically detects system fault events and transmits an Electronic Service Request (ESR) packet that contains the failure details to the Unisys Support Center. Call Home is triggered by the specific events logged in the Event Log and also at the specific request set by the user. The Call Home settings can be changed by editing the platform attributes.

You can view and edit Call Home configurations. You can specify when a service request should be sent to Unisys and also the method used to send the service request (LAN with proxy, LAN without proxy or modem) to the Unisys Support Center. You also have the option of disabling the Call Home facility while carrying out maintenance activities. However, Call Home will not be disabled if it is already scheduled to be sent after a certain time.
15.4. Viewing Events

Fabric Manager allows you to store the events for a maximum period of 180 days. For more information about setting the event log retention period, see 15.10 Editing Event Log Retention Period.

To view the events, click Events.

A table of events with the following information appears.

- **Status**: Status of the events. For example, success or failure and so on.
- **Device**: Source from where the event or events are generated.
- **Application Type**: Type of the application (Audit, s-Par®, IPMI_SEL, and so on) reporting the event.
- **Severity**: The severity value denotes the impact of the event on the fabric. For example, Critical, Warning, and so on.
- **Message**: Detailed description of the event that occurred.
- **Report Date/Time**: Time stamp of when that event occurred.
- **Operation Status**: Operation Status of the Events. For Example, Open/Close/Accepted/NACK/SACK/Send In-Progress/Send Failed.

**Notes:**

- You can customize the number of columns you want to view. Click the drop-down arrow next to each column heading to select or clear the required column.
- To view more information about an event, click the desired event.

The following is an example of a table of events:
15.5. Filtering Events

Fabric Manager allows you to filter and display only the required events in the Events console.

The following table lists the various events types and categories which you can use to filter the events in the event console.

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Categories</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Ok, Running, Stopped, Critical, Unknown, Warning, Success, Failed, Initiated, Informational</td>
<td>Displays the status of the events. If the event is associated with a Device (Platform or Partition) it shows the status of Platform or Partition when the event occurs.</td>
</tr>
</tbody>
</table>
### Event Type Categories Description

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Categories</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message</td>
<td>Event message</td>
<td>Provides detailed description of the event that occurred in Fabric Manager.</td>
</tr>
<tr>
<td>Device</td>
<td>Device name</td>
<td>Displays the source from where the event or events are generated.</td>
</tr>
</tbody>
</table>
| Application Type | Audit, IPMI_SEL, Nagios, SPAR, CHCS | Displays the type of the application which reports the event. The event types are:  
- Audit events: User interactions with the Forward! Fabric Manager user interface.  
- IPMI_SEL (IPMI_System Event Log): Important hardware related events identified by the platform management card; for example, hardware faults.  
- NAGIOS: This event type is captured in a log file and it is part of the Diagnostic dumps.  
- SPAR events: Important hardware and software events, identified by the s-Par® firmware.  
- CHCS: Events related to the ESR Test Packets sent through the FFM call home central service component. (That is, ESRTEST heart beat check packets which are sent to Unisys Support Center. It also includes the ESRDIAG and ESRRFU packets sent while testing connections from the Call Home settings tab under Edit System.) |
| Severity   | Ok, Critical, Warning, Low, High, Informational, Fatal, Performance, Statistic, Serious, Unknown, Normal, Major, Minor, Unreachable | The severity value denotes the impact of the event on the fabric. For example, Critical, Warning, and so on. |
| Report Date/Time |                              | Day on which the event occurred. |
| Operation Status | Open, Closed, Accepted, Sack, Nack, Send failed, Send in progress | Operation Status of the Event. |

IPMI_SEL and SPAR events in any operation state other than CLOSED state reflect the health status of the platform. Based on the severity, health status of the platform (Critical, Error, Major, and so on) is shown under the Manage System and Summary page.

For example, if there is a Critical event generated for a platform, the status of the platform is shown as Critical. If there are no Critical events for that platform, and there are only warning events available, then, the status of the platform is shown as Warning.
Filtering Events

For a partitionable EPP, both IPMI_SEL and SPAR events are consolidated to reflect the health status. For example, if there is an open Critical IPMI_SEL event and an open Warning SPAR event, then health status is shown as Critical.

For a non-partitionable EPP, only the IPMI_SEL event severity is considered for indicating the health status.

The following table provides the combination of various events and the corresponding Health Status.

<table>
<thead>
<tr>
<th>Event Severity</th>
<th>Health Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical/Error/Major</td>
<td>Critical</td>
</tr>
<tr>
<td>Warning/Minor</td>
<td>Warning</td>
</tr>
<tr>
<td>Anything else</td>
<td>OK</td>
</tr>
</tbody>
</table>

To filter the events
1. In the Filter row, select the desired filter values from the drop-down lists.
2. Click Go to apply the filter.

A table of events appears based on your selection.

**Note:** Click Clear to clear the filter and display all the events.

**Further Information**

For example, in Figure 15–3, a filter is applied to view the events related to platform PEPP1. When the filter is applied, event console displays:

- All the 10 events related to PEPP1.
- Events related only to the platform PEPP1.

Based on the requirements you can also do the following:

- Hide the columns to be viewed. Device, Application Type, and Report Date/Time columns are hidden in Figure 15–3.
- Widen the Message field, to be able to read each message.
15.6. Accepting Events

Accepting an event indicates that you are aware of the event and plan to take action.

To accept an event
1. Click **Events**.
2. Select the desired event with status as **UNKNOWN** or **RUNNING**.
3. Click **Accept**.
4. Click **Yes**.
   The operating status of the event changes to **Accepted**.

**Notes:**
- Accepted events are displayed in the event console.
- Only the Close operation can be performed on the accepted events.

15.7. Closing Events

Closing an event indicates that your response to the event is complete.

To close an event
1. Click **Events**.
2. Select the desired event with either **Open** or **Accepted** operation status.
3. Click **Close**.
   The operating status of the event changes to **Closed**.

**Note:** By default, closed events are not displayed in the event console.
15.8. Re-Opening Events

You can re-open an event that you had previously closed in case the event requires further action.

To re-open an event
1. Click Events.
2. In the filter row drop-down lists, select the values All, OperationStatus, and Close.
   A table of all the closed events appears in the events console.
3. Select the desired event with operation status CLOSED.
4. Click Re-Open.
   The operation status of the event changes to Open and appears in the events console.

15.9. Re-Sending Failed Call Home Events

Call Home events are automatically sent to the Unisys Support Center. If the support center fails to acknowledge a particular event, then the event’s operation status is set to NACK in the event console.

Fabric Manager allows you to re-send the failed Call Home events that are listed as NACK in the event console. To re-send a failed Call Home event
1. Click Events.
2. In the filter row drop-down lists, select the values All, OperationStatus, and NACK.
   A table of all the NACK events appears in the events console.
3. Select the desired NACK event.
   Details of the ESR packet that is sent and the acknowledgement details received from the Call Home are displayed in the Details section.
4. Click Re-Send.
   The operating status of the event changes to SEND: IN-PROGRESS and appears in the events console.

15.10. Editing Event Log Retention Period

You can specify the period for which the event logs should be retained in the event log database by the Fabric Manager. The event logs are stored in the Fabric Management Platform at the location: usr/local/ffm-db-events-backup.

To edit the event log retention period
1. On the Fabric Manager user interface, click Manage System on the left pane. Details screen appears on the right pane.


3. Click the Settings tab.

4. Click Edit. The Edit Settings dialog box appears.

5. In the Event log retention period field, select the required event log retention value. Note: The minimum value is 30 days and the maximum value 180 days.

6. Click Save, and then click OK. The new event log retention value appears in the Event log retention period field.
Section 16

Configuring a Hadoop Cluster

This section describes the procedure to configure a Hadoop cluster on the Forward! by Unisys fabric.

**Audience**

This topic is intended for the Hadoop administrator; that is, the person responsible for setting up and maintaining the Hadoop cluster on the Forward! fabric. The Hadoop administrator should be assigned to the administrator user role in the Forward! Fabric Manager.

**Prerequisites**

This topic assumes that the Hadoop administrator is familiar with the following concepts:

- Hadoop release 2.2, Hadoop clusters and nodes, Hadoop distributed file system (HDFS), and Hadoop YARN. This section does not describe how a Hadoop system works or the commands that run and control a Hadoop cluster. See the Apache Hadoop website for information about Hadoop:
  
  http://hadoop.apache.org/

- Various roles a partition plays in a Hadoop cluster.


- SUSE Linux Enterprise Server (SLES) or Red Hat Enterprise Linux (RHEL) operating environments.

**Terminology**

The following terms are used in this chapter. In addition, see the *Forward! by Unisys Glossary* for the definition of terms related to the *Forward! fabric* or the Apache Hadoop website (http://hadoop.apache.org/) for terms related to Hadoop.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>A partition in the <em>Forward!</em> fabric used in a Hadoop cluster.</td>
</tr>
</tbody>
</table>
### Preliminary Tasks

To configure a Hadoop cluster on the Forward! fabric, the administrator updates the systemDetails.txt file with the details of the cluster. Before updating the systemDetails.txt file, make sure the tasks in the following subsections are complete.

#### 16.1.1. Determine the Number of Nodes in the Hadoop Cluster

Determine how many nodes you initially need in your Hadoop cluster. If needed, you can use the procedure in 16.6 Adding Additional DataNodes to a Hadoop Cluster to add additional DataNodes to an existing Hadoop cluster.

#### 16.1.2. Commission the Partitions for all Nodes in the Hadoop Cluster

Unisys supplies two blueprints for a Hadoop implementation on the Forward! fabric:

- Hadoop blueprint for SUSE Linux Enterprise Server (SLES)
- Hadoop blueprint for Red Hat Enterprise Linux (RHEL)

For each node in the Hadoop cluster, commission a partition using one of the Hadoop blueprints. To commission the partition, use the Forward! Fabric Manager to select either the SUSE or RHEL Hadoop blueprint for that partition. Repeat the commissioning process for each node in the Hadoop cluster. The examples in 16.2 Creating the Configuration File configure a Hadoop cluster of eight nodes. For those examples, the administrator needs to commission eight partitions, each with the appropriate Hadoop blueprint.

See the Installation, Administration, and Operations Guide or the Information Center for the procedure to select a blueprint and commission a partition.

At the time of commissioning, each partition is assigned the following addresses:

- Inter-partition LAN (IP LAN) address
- Fabric Management LAN (FM LAN) address

The FM LAN is used to access the SSH shell on the NameNode.

---

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name or machine name</td>
<td>The name by which a given Linux OS instance identifies itself. This name is associated with the IP address on the customer corporate (the public or enterprise) LAN.</td>
</tr>
<tr>
<td>Internal name</td>
<td>The name associated with a specific partition’s IP address on the Inter-partition LAN (IP LAN).</td>
</tr>
<tr>
<td>External disk</td>
<td>A folder associated with a segment of disk space from the disk system provided by the Forward! fabric. This is not the primary disk system of the partition’s operating system.</td>
</tr>
</tbody>
</table>
16.1.3. Select a Partition for the Nodes

Select a partition for the NameNode and each DataNode in the cluster.

Suggested Node Assignments

Unisys recommends that the NameNode and Resource Manager not be DataNodes. In fact, the Node Manager will not run on the same node as the Resource Manager. The Secondary NameNode can be a DataNode as well. Unisys does not support configuring the Secondary NameNode on the same partition as the NameNode.

16.1.4. Gather Node Information

For each node in the cluster, gather the following information:
- Inter-partition LAN IP address
- External IP address (if the dynamic IP address is not used)
- External disk folder or disk folders

The administrator must give an internal name to each Inter-partition LAN IP address and must know the host name for each partition. These are specified when the partition is commissioned. They appear in the window containing information about the partition on the Forward! Fabric Manager. The IP LAN address is toward the bottom of the window.

16.1.5. Identify a Local Folder

The local folder acts as a Hadoop temporary file location. The configuration scripts create the file so the user does not need to.

The user must also specify a folder for local use on each Hadoop node. This local folder can be in the home folder of ‘hdadmin’, for example, /home/hdadmin/hadTemp.

However, for jobs which traverse large amounts of data, a folder on a local drive is insufficient. Therefore, for most installations, Unisys recommends specifying a local folder on an external disk.
16.1.6. Mount External Disk LUNs

Before creating the configuration file, log onto each partition and mount the external disk LUNs. See the Installation, Administration, and Operations Guide or the Information Center for more information about LUNs.

16.1.7. Establish Root Password

The password that was specified for the partition when it was commissioned must be changed. You must establish the actual runtime root password before you can run the configuration script.

Use the following procedure to establish the runtime root password:

1. From the Forward! Fabric Manager, open an SSH session to the partition.
   When the first connection is made to the partition, the Linux operating system asks for the password that was specified when the partition was commissioned.
2. Enter the password you want to use at runtime. The Linux operating system will also ask you to verify the password.
3. Exit the SSH session.
4. Repeat this procedure for the other partitions in the cluster.

Note: Do not use the Terminal application from a Remote Desktop connection to the Fabric Manager or the Partition Desktop to establish the first connection to a partition. This can have unpredictable results including creating unknowable passwords and file corruption. Use a SSH client such as PuTTY to connect to the Fabric Manager and from there connect to a given partition using its FM-LAN address (172.29.x.x). The first connection establishes the new password. You must establish the initial connection to each partition in this manner before running the configuration script.

16.2. Creating the Configuration File

Once all the preliminary tasks are complete, update the systemDetails.txt file.

1. Use PuTTY or another SSH client to establish an SSH connection to the Forward! Fabric Manager.
   For example, if the Fabric Manager is at the following web address:
   http://182.43.221.114
   Specify an address of 182.43.221.114 in PuTTY.
   The credentials are root/adpass, where adpass is the password used to log into the Fabric Manager remote desktop.
2. Once logged into the Forward! Fabric Manager shell, establish an SSH connection to the FM LAN of the NameNode.
   To establish the SSH connection, you need the IP address of the FM LAN. The IP address of the FM LAN is listed toward the bottom of the partition information
Creating the Configuration File

window on the Forward! Fabric Manager. The IP address of the FM LAN is of the form 172.29.L.p where L is the platform number and p is the partition number on the platform. The FM LAN of the first partition created is 172.29.1.1. If the first commissioned partition has the FM LAN IP address of 172.29.1.1, from the bash shell of the Forward! Fabric Manager, enter `ssh 172.29.1.1` to establish an SSH connection to that partition.

From the Forward! Fabric Manager shell, use the FM LAN IP address of the partition chosen to be the NameNode to enter the bash shell of that partition. You will be running as `root`.

3. In the `/usr/bashScript` folder, locate the `systemDetails.txt` file. This file is a template of the required information. Make sure that `systemDetails.txt` has fully open permissions (777).

The template looks like this:

```plaintext
NameNode= ; ; ; ; ; ;
ResourceManager= ; ; ; ; ; ;
SecondaryNameNode= ; ; ; ; ; ;
DataNodes: ; ; ; ; ; ;
EndDataNodes:
```

4. For each principal node (NameNode, ResourceManager, Secondary NameNode), enter information in the following order:
   - `NodeType=host name`
   - `External IP address or “DHCP”`
   - `Inter-partition LAN name`
   - `Inter-partition LAN IP address`
   - `Temp folder location (Separate multiple paths with a comma.)`
   - `External disk location for DataNode data`
   - `External disk location for NameNode data`

5. In the lines between the “DataNodes:” and “EndDataNodes:” headings, enter the information for each DataNode in the following order:
   - `NodeType=host name`
   - `External IP address or “DHCP”`
   - `Inter-partition LAN name`
   - `Inter-partition LAN IP address`
   - `Temp folder location (Separate multiple paths with a comma.)`
   - `External disk location for DataNode data`
   - `External disk location for NameNode data`

The default setting of all newly commissioned Hadoop partitions have the external IP address set by the corporate DHCP server.
Creating the Configuration File

Example 1

In the following configuration, all external IP addresses are statically assigned. In addition, the first DataNode also serves as the Secondary NameNode. There are no external disks, so all data storage is on the local partition. This configuration is useful for small experiments but not for large amounts of data.

NameNode=NN;192.63.237.188;hadoop1;172.31.1.1;/home/hdadmin/tpm1;/home/hdadmin/data1;/home/hdadmin/name1
SecondaryNode=SN;192.63.237.189;hadoop2;172.31.1.2;/home/hdadmin/tpm1;/home/hdadmin/data1;/home/hdadmin/name1
ResourceManager=JT;192.63.237.187;hadoop3;172.31.1.3;/home/hdadmin/tpm1;/home/hdadmin/data1;/home/hdadmin/name1

DataNodes:
SN;192.63.237.189;hadoop2;172.31.1.2;/home/hdadmin/tpm1;/home/hdadmin/data1;/home/hdadmin/name1
DN1;192.63.237.127;hadoop4;172.31.1.4;/home/hdadmin/tpm1;/home/hdadmin/data1;/home/hdadmin/name1
DN2;192.63.237.126;hadoop5;172.31.1.5;/home/hdadmin/tpm1;/home/hdadmin/data1;/home/hdadmin/name1
DN3;192.63.237.125;hadoop6;172.31.1.6;/home/hdadmin/tpm1;/home/hdadmin/data1;/home/hdadmin/name1
DN4;192.63.237.124;hadoop7;172.31.1.7;/home/hdadmin/tpm1;/home/hdadmin/data1;/home/hdadmin/name1
DN5;192.63.237.123;hadoop8;172.31.1.8;/home/hdadmin/tpm1;/home/hdadmin/data1;/home/hdadmin/name1

Example 2

In the following example, the external IP addresses are obtained by DHCP. Each partition has been assigned a set of external disks that have been mounted as /mnt/ext1. The NameNode is duplexed, that is, its data is duplicated automatically by Hadoop on two separate disks. This is to enable cluster recovery in the case of a NameNode failure. The second disk is /mnt/ext2. Note that the temporary folder on each node is also assigned to the external disk.

NameNode=NN;DHCP;hadoop1;172.31.1.1;/mnt/ext/tmp1;/mnt/ext1/data1;/mnt/ext1/name1
SecondaryNode=SN;DHCP;hadoop2;172.31.1.2;/mnt/ext/tmp1;/mnt/ext1/data1;/mnt/ext1/name1
ResourceManager=JT;DHCP;hadoop3;172.31.1.3;/mnt/ext/tmp1;/mnt/ext1/data1;/mnt/ext1/name1

DataNodes:
SN;DHCP;hadoop2;172.31.1.2;/mnt/ext/tmp1;/mnt/ext1/data1;/mnt/ext1/name1
DN1;DHCP;hadoop4;172.31.1.4;/mnt/ext/tmp1;/mnt/ext1/data1;/mnt/ext1/name1
DN2;DHCP;hadoop5;172.31.1.5;/mnt/ext/tmp1;/mnt/ext1/data1;/mnt/ext1/name1
DN3;DHCP;hadoop6;172.31.1.6;/mnt/ext/tmp1;/mnt/ext1/data1;/mnt/ext1/name1
DN4;DHCP;hadoop7;172.31.1.7;/mnt/ext/tmp1;/mnt/ext1/data1;/mnt/ext1/name1
DN5;DHCP;hadoop8;172.31.1.8;/mnt/ext/tmp1;/mnt/ext1/data1;/mnt/ext1/name1

EndDataNodes:
16.3. Running the Configuration

Once you have updated the systemDetails.txt file, run the configuration script by entering the following command:

/usr/bashScripts/HadoopConfigurationBash.sh /usr/bashScripts/systemDetails.txt

If any errors are detected in the configuration settings, they are reported and the configuration stopped. Fix the error and then rerun the configuration script.

At the end of a successful execution of the configuration script, you receive a prompt to format the NameNode. Answer Y to continue.

After the execution of the configuration script, you are running as the “hdadmin” user.

16.4. Starting Hadoop

This topic contains only basic information about running Hadoop. For more detailed information, see the Apache Hadoop website:

http://hadoop.apache.org/

The configuration script creates the Hadoop users. To access Hadoop, the user must log in using the following credentials:

User-id: hdadmin
Password: hdadpass

If the NameNode was not previously formatted, before starting Hadoop, format the NameNode using the following command:

hdfs namenode -format

To start Hadoop, the user runs the following script:

start-dfs.sh

start-yarn.sh

16.5. Component Locations

In the Forward! fabric, commissioning the Hadoop blueprint places the Hadoop components in the folders shown in the following table.

<table>
<thead>
<tr>
<th>Component</th>
<th>Folder</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hadoop</td>
<td>/usr/hadoop</td>
</tr>
</tbody>
</table>
16.6. Adding Additional DataNodes to a Hadoop Cluster

Use the following procedure to add a one or more DataNodes to an existing Hadoop cluster:

1. In the /usr/bashScripts folder, locate the additionalDataNodesDetails.txt file.
2. In this file, enter the details for the DataNodes to be added to the existing Hadoop cluster. Use the same format as the systemDetails.txt file (see 16.2 Creating the Configuration File).

```
DNpart1;129.52.34.25;hadoop3;172.31.1.3;/home/hdadmin/tpm1;/home/hdadmin/data1;/home/hdadmin/name1;/home/hdadmin/che1
DNpart2;129.52.34.26;hadoop4;172.31.1.4;/home/hdadmin/tpm1;/home/hdadmin/data1;/home/hdadmin/name1;/home/hdadmin/che1
DNpart3;129.52.34.27;hadoop5;172.31.1.5;/home/hdadmin/tpm1;/home/hdadmin/data1;/home/hdadmin/name1;/home/hdadmin/che1
DNpart4;129.52.34.28;hadoop6;172.31.1.6;/home/hdadmin/tpm1;/home/hdadmin/data1;/home/hdadmin/name1;/home/hdadmin/che1
DNpart5;129.52.34.29;hadoop7;172.31.1.7;/home/hdadmin/tpm1;/home/hdadmin/data1;/home/hdadmin/name1;/home/hdadmin/che1
```

**Note:** Do not change the input file format. For example, do not include a space between the parameters or the semicolon.

3. Execute or run the addDataNodesToCluster.sh script under /usr/bashScripts in the NameNode partition.

```
bashScripts]# ./addDataNodesToCluster.sh
/usr/bashScripts/additionalDataNodesDetails.txt
```

Running this script configures the DataNodes and starts the required daemons on the DataNode partition.
16.7. Configuring Oozie

Oozie is a workflow scheduler system to manage Hadoop jobs. It is included in the Hadoop blueprint but it is not configured as part of the original configuration. Use the following procedure to configure Oozie:

1. During the process of configuring Oozie, the scripts download the open source package “extjs”. To download this package, the NameNode must be configured to use name servers.

2. By default, all newly commissioned partitions have their name servers configured by the corporate DHCP servers. If these have been removed or if the site wants to use different name servers, you must edit the following file:

   `/etc/resolv.conf`

3. Once the name servers have been set and activated, run the following script:

   `/usr/bashScripts/prepooz.sh`

To start the Oozie server, enter:

   `/usr/oozie/bin/oozied.sh start`

16.8. Specifying the Location of Secondary NameNode Data

You can add an additional location parameter; for example, `/home/hdadmin/checkpoint`, at the end of each configuration statement to specify where on the local file system the Secondary NameNode stores the temporary images to merge. This is useful if you want to check the Secondary NameNode data.

**Example**

```
NameNode=NN;192.63.237.188;hadoop1;172.31.1.1;/home/hdadmin/tpm1;/home/hdadmin/data1;/home/hdadmin/name1
SecondaryNode=SN;192.63.237.189;hadoop2;172.31.1.2;/home/hdadmin/tpm1;/home/hdadmin/data1;/home/hdadmin/name1;/home/hdadmin/checkpoint
ResourceManager=JT;192.63.237.187;hadoop3;172.31.1.3;/home/hdadmin/tpm1;/home/hdadmin/data1
DataNodes:
   SN;192.63.237.189;hadoop2;172.31.1.2;/home/hdadmin/tpm1;/home/hdadmin/data1;/home/hdadmin/name1
   DN1;192.63.237.127;hadoop4;172.31.1.4;/home/hdadmin/tpm1;/home/hdadmin/data1;/home/hdadmin/name1
   DN2;192.63.237.126;hadoop5;172.31.1.5;/home/hdadmin/tpm1;/home/hdadmin/data1;/home/hdadmin/name1
   DN3;192.63.237.125;hadoop6;172.31.1.6;/home/hdadmin/tpm1;/home/hdadmin/data1;/home/hdadmin/name1
   DN4;192.63.237.124;hadoop7;172.31.1.7;/home/hdadmin/tpm1;/home/hdadmin/data1;/home/hdadmin/name1
   DN5;192.63.237.123;hadoop8;172.31.1.8;/home/hdadmin/tpm1;/home/hdadmin/data1;/home/hdadmin/name1
EndDataNodes:
```
Section 17
Shutting Down and Starting Up the Entire Fabric

This section provides information on

- 17.1 Shutting Down the Entire Fabric
- 17.2 Restarting the Fabric

17.1. Shutting Down the Entire Fabric

There may be occasions when you want to shut down the entire fabric, not just particular partitions or platforms. The following procedure describes how to do this. You must shut down the fabric platform by platform.

If you want to shut down just parts of the fabric, not the entire fabric, you can perform just a subset of the procedure.

1. Typically you first stop your applications in whatever manner is correct for them. For example, this could consist of stopping web services, followed by stopping application logic, followed by stopping database services.

2. It is recommended that you take a back up of an enterprise partition platform’s configuration settings before powering down the platform. See Section 18, Backup and Restore, for more information on how to back up.

3. Power down the first enterprise partition platform, using the Soft Shutdown command from the Fabric Manager. Doing this accomplishes the following:

   - Performs an implicit graceful shutdown of all of the partitions on the platform (and the partition operating systems)
   - Implicitly stops s-Par

   See 10.3 Performing Soft Shutdown on a Platform for the procedure.

   This removes DC power to the EPP. Note that this does not remove AC power from the EPP’s platform management card, which is powered by keep-alive power from the system’s uninterruptible power supply (if one exists).

   **Approximate duration of step:** Typically three to four minutes. It is recommended that you wait ten minutes before taking remedial action.
If step does not complete successfully: If a given operating system does not respond, do as follows.

a. Individually stop the offending operating system, for example, using Remote Desktop.
   
   If this does not work, do a **Force Halt** (unorderly stop) of the partition, using the Fabric Manager.

b. Do a **Soft Shutdown** of the whole platform again, using the Fabric Manager.

c. If the preceding step does not work, then use the Fabric Manager **Power Off** command to do an unorderly power off of the platform.

4. Remove AC power from the EPP’s platform management card by removing the two EPP AC power cords from the power strips inside the cabinet. (The two cords lead to two different power supplies.)

5. Power down all of the other enterprise partition platforms, as described in steps 3 and 4.

6. Perform an orderly shutdown of the Linux operating system on the Fabric Management Platform, using one of the following methods:
   
   • From a putty terminal session, specify `shutdown –h now`.
   
   • After logging in as the root user, perform a `poweroff` command.

   Doing this stops the Fabric Manager software, stops the Fabric Management Platform’s Linux operating system, and powers down the Fabric Management Platform.

   **If step does not complete successfully:** Physically press the power button on the Fabric Management Platform.

### 17.2. Restarting the Fabric

The following procedure describes how you restart the fabric after shutting it down.

You can skip any steps that you did not perform when shutting the fabric down.

1. Power up the Fabric Management Platform by pressing the power button. This will boot the Linux operation system.

2. Launch and access Fabric Manager.
   
   See **4.1 Forward!** Fabric Manager User Interface.

3. Ensure that AC power is available to the first EPP’s platform management card. If you removed the EPP’s two AC power cords from the power strips inside the cabinet, plug the cords back in.

4. Power up the first enterprise partition platform, using the Fabric Manager **Power On** command.
   
   See **10.2 Powering-On a Platform** for the procedure.
Doing this accomplishes the following:

- Applies DC power to the EPP.
- Starts s-Par on the EPP.
- May or may not put the EPP’s partition images in a running state, depending on the value of each partition’s Initial State attribute (see 5.6 Starting a Partition Image). Initial State is set to Running by default.

  If Initial State is set to Stopped, you must explicitly start the partition image using the Fabric Manager Start command (see 5.6 Starting a Partition Image).

- Once the partition is in a Running state, the operating system is automatically booted.

Approximate duration of step: Dependent on the number of partitions and other factors, but ten to twenty minutes is a rough approximation.

5. Power up all the other enterprise partition platforms as described in steps 3 and 4.
6. Start your applications in whatever manner is correct for them.
Restarting the Fabric
Section 18
Backup and Restore

This section provides information on backup and restore procedures in the following topics:

- 18.1 Backing Up Fabric Manager
- 18.2 Restoring Fabric Manager Database and Configuration Files
- 18.3 Backing Up Application Operating Environments on Enterprise Partition Platforms
- 18.4 Restoring Application Operating Environments on Enterprise Partition Platforms
- 18.5 Examples of Tools for Backing Up and Restoring Application Operating Environments

18.1. Backing Up Fabric Manager

The Forward! 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 the backup script be run at suitable intervals to capture any possible changes.

To ensure that no ongoing updates cause integrity issues during the backup process, the backup script 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, you manually run the backup script 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 run the backup script on the Fabric Management Platform running the Fabric Manager services (that is, the active or master Fabric Management Platform).

Depending on the configuration, backing up the Fabric Manager database and configuration files can take up to 10 minutes.

18.1.1. Preparing to Back Up Fabric Manager

The backup script reads the file `/usr/local/ffm/scripts/smsbackup.lst` to identify Forward! Fabric Manager files and directories that need backing up. You can specify extra files or directories by adding the absolute path (full path) as a new line in `smsbackup.lst`.

8222 4544-003 18–1
For example, if you want to add the file `myconfig.txt` in the directory `/home/user` to the backup, add the following line at the end of `smsbackup.lst`:

```
/home/user/myconfig.txt
```

When the backup script is next run, the file `myconfig.txt` will also be backed up.

**Example of smsbackup.lst**

```
/usr/local/ffm/nagios/etc
/usr/local/ffm/nagios/etc/sms
/usr/local/ffm/nagios/etc/objects
/usr/local/ffm/scripts/ntp.conf

/home/user/myconfig.txt
```

**18.1.2. Backing up Fabric Manager Database and Configuration Files**

Do the following to back up the *Forward!* Fabric Manager database and configuration files to the `/usr/local/ffm-backup` folder:

1. Log in to the *Forward!* Fabric Management Platform desktop, and open a new terminal session as root user.
   (If you are connecting remotely, use a tool like PuTTY or the remote desktop function of the Fabric Management Platform, and login as root user. The root user login is root/Administer4Me.)
2. In the terminal session, change the working directory to the following directory where the backup script is located:
   ```
   cd /usr/local/ffm/scripts
   ```
3. Use the following command to run the backup script:
   ```
   sh backupsms.sh
   ```
   The script prompts for confirmation.
4. Enter `y` to proceed.
   The script stops all Fabric Manager services, and backs up the Fabric Manager database and configuration files. When the backup is complete, the script restarts the Fabric Manager services, as well as displays the backup file name
   ```
   FFM_BACKUP_servername_DDMMYYHMMSS.tar
   ```
   (where `servername` is the name of the particular Fabric Management Platform, and `DDMMYYHMMSS` is the date and time stamp).
5. Copy the backup file to a safe location so that it is available in case of reinstallation or a catastrophic failure.
18.2. Restoring Fabric Manager Database and Configuration Files

Restoring Forward! Fabric Manager database and configuration files should only be performed by Unisys support personnel. Contact Unisys Support if you need to restore. If you are a qualified service representative, refer to the Fault Isolation and Servicing Guide for more information.

18.3. Backing Up Application Operating Environments on 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 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 18.5 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 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 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.
18.4. Restoring Application Operating Environments on Enterprise Partition Platforms

The 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 18.5 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.

18.5. 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
  Only backup or restore the system state, and files and folders for the entire boot drive.

- 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.
Examples of Tools for Backing Up and Restoring Application Operating Environments
Section 19

Time Management

This section provides information about time management in the following topics:

- 19.1 Understanding Time Management
- 19.2 Setting Time for Your Platform

19.1. Understanding Time Management

 Forward! Fabric Manager uses Network Time Protocol (NTP) to synchronize the date and time (and time zone, if applicable) across various components of the fabric such as Fabric Manager, platform management card, Secure Partitioning (s-Par®), partitions, and so on. NTP uses a port to pass time and timing values that are used to lock a client system’s clock in step with its time server.

For all the components within the fabric, Forward! Fabric Management Platform (FMP) acts as the time source for all the fabric components.

Alternately, you connect the Fabric Management Platform to an external NTP time source, which can then serve as the time source for the Fabric Management Platform itself, and thus the other fabric components. For the partitions, the user has the option to configure the partition to use the Fabric Management Platform or an alternate time source as the time source for the partition.

If you have two Fabric Management Platforms and they are configured as a high availability cluster, the second Fabric Management Platform uses the first Fabric Management Platform as its time source. And partitions can be configured to access both Fabric Management Platforms through each Fabric Management Platform’s static IP address, and use the Fabric Management Platforms as time sources.

19.2. Setting Time for Your Platform

You use the Fabric Manager user interface to accomplish both of the following:

- Setting the date, time, and time zone for the Fabric Management Platform, so that it can serve as the time source for the fabric
- Configuring an external NTP server as the time source for the fabric

For both of these tasks, changing the time source, see 8.2 Editing the System Attributes.
Forward! Fabric is equipped to provide common and consistent security management and policies. This section provides information on the following topics:

- 20.1 Understanding Security Management
- 20.2 Using the Unisys Stealth Solution

### 20.1. Understanding Security Management

Forward! Fabric is equipped to provide common and consistent security management and policies.

Forward! Fabric provides the following security features:

- **Identity Management** – Role-based access control is implemented using the Fabric Manager. This limits the user’s ability to make configuration changes and limits their ability to control the behavior of the fabric which is defined by their designated role. This is achieved through
  - Identification – Uniquely identifying each user as a member of a role.
  - Authentication – Ensuring the validity of the user’s identity.
  - Authorization – Limiting the scope of the user’s permitted activities, such as access to various system resources, actions that the user can perform on various system resources, and so on.
  - Validation – Validation of the user identity and authorizations.

- **Audit** – Information systems are audited for compliance, regulations, and so on. Information such as timestamp, user identity, and severity of the event are critical for auditing. Fabric Manager tracks and logs all the actions and events such as adding and deleting configuration settings, communication failures, and login attempts that are carried out within the fabric.

- **Network Security** – The entire fabric, including platforms and partitions, is protected from both internal and external threats. Network security policies, configurations, and processes are managed centrally and applied consistently across the fabric. This includes
  - Confidentiality – Ensuring that only the intended recipient can read the data.
  - Integrity – Ensuring that the data is not modified in-motion.
  - Non-repudiability – Ensuring that the sender of the data cannot claim not sending it.
20.2. Using the Unisys Stealth Solution

Unisys Stealth™ is an optional component that is designed to secure communications on both physical and virtual networks, permitting only authorized users to access systems and data.

The Stealth solution includes one or more hardware appliances as well as software to configure the solution, to create an Authorization Server for centralized authorization, and to protect the endpoint workstations, servers, and partition images in your environment.

You use the standard Stealth documentation to install, configure, and administer Stealth in the Forward! fabric. This topic provides an additional overview that is specific to this environment, as well as guidelines and some best practices for installing Stealth in this environment.

20.2.1. Understanding Stealth Security

Stealth protects the communication between different components in your environment through the use of Communities of Interest (COIs). Communities of Interest enable you to configure which groups of physical servers, virtual machines, and Forward! partitions can communicate with one another, with other components in your environment, and with components outside of the secured environment. The network traffic for each COI is cryptographically separated using defense-grade cryptographic algorithms.

In this way, Stealth enables multiple user communities to securely share the same IT infrastructure. Stealth isolates applications so that only the authorized users can see and access the data unique to that application.

In addition to adding Stealth security to the corporate LAN, use of Communities of Interest can be extended through a Forward! secure partition to the Inter-Partition LAN. The result is that even if data packets are delivered to the wrong place (either maliciously or accidentally because of a configuration error), they are unreadable. Additionally, the connection between a system administrator and the Fabric Manager user interface can be protected using Stealth security.

Stealth requires no application or infrastructure changes. It also supports many application scenarios, such as multicast traffic and video.

20.2.2. Stealth Architecture

The following figure shows a simple example of a data center that includes a two-platform Forward! fabric and also includes Stealth.
In this configuration, the two blue boxes form a Forward! fabric. There are three Stealth Appliances in this example, as follows:

- Two appliances make up the Stealth Appliance Team (Licensing), and they are teamed together to provide high availability. They provide licensing for workstations and servers running supported Windows and Linux operating systems and the Stealth endpoint software, which are known as Stealth endpoints. (The Stealth endpoints include the workstation and network servers running Stealth software in the Enterprise Network, the data center server running Stealth software, and the two Forward! partitions running Stealth software.)

- One appliance is the Stealth Appliance (Gateway), which acts as a gateway to traffic in the network, protecting servers that cannot run the Stealth endpoint software (because they do not run a supported Windows or Linux operating system).

In this example, the Stealth Appliance (Gateway) manages the COIs on behalf of the server running an operating system not supported by Stealth. Note that for resiliency, the Stealth Appliance (Gateway) can also be deployed as a Stealth Appliance Team.
Endpoints that include the Stealth workgroup COI (shown in yellow) can communicate with one another. Endpoints receive their licenses through the License COI (shown in purple) from the Stealth Appliance Team designated for that function. The Stealth configuration machine is used to set up the environment and communicate the COI information to the appliances through use of the Admin COI (shown in pink).

This simple example shows only one workgroup COI, but the number of workgroup COIs can be expanded to as many as are needed to separate and protect the network traffic in the environment.

As required, you can purchase additional Stealth Appliances and additional licenses to enable simultaneous Stealth-secured communications for as many Stealth-enabled physical servers, virtual machines, and Forward! partitions as you want to configure in the environment.

### 20.2.3. Required Knowledge and Documentation

To install the Stealth Solution, you should be familiar with the following:

- The existing and planned network configuration, including IP addresses and routing
- Stealth release 2.5, 2.7, 2.8 or higher 2.x release

Before you begin, obtain the following documents:

- *Unisys Stealth Solution Planning, Installation, and Administration Guide* (3843 4569), which is available from the Stealth Release page of the Unisys Product Support website ([http://www.support.unisys.com](http://www.support.unisys.com)).
- Documentation Updates Problem List Entry (PLE) for the *Unisys Stealth Solution Planning, Installation, and Administration Guide*, which includes the latest updates and corrections to the Stealth document. This PLE is referenced in the “Documentation Updates” section of the *Planning, Installation, and Administration Guide*.

### 20.2.4. General Networking Guidelines

Stealth provides both unparalleled security and incredible flexibility. This topic provides overall guidelines on using Stealth in a Forward! fabric.

#### General Stealth Security Considerations

Stealth COIs can be defined as needed to provide the required security for the environment. You can create multiple COIs to enable various levels of security and install Stealth endpoint software on all components in the environment, or you can Stealth-enable a limited number of components and allow all other systems to use clear text communication. You can use Stealth filters to further refine the traffic that can be communicated between Stealth-enabled and non-Stealth enabled components.
It is important to define the scope of the Stealth enclave, which servers and workstations it includes, and which other systems need to be communicated with using clear text communication (including Infrastructure services, the Fabric Management Platform, Active Directory (AD) server, DHCP servers, and so on). However, the scope of the Stealth enclave is completely variable, depending on the needs of the particular environment.


**Stealth Configuration Machine and Authorization Server Setup and Network Locations**

The Stealth configuration machine and Authorization Server can be installed in Forward! partitions that meet the operating system and software requirements for each of these components. Alternatively, these Stealth components can be installed outside of the Forward! system and connected to the Forward! fabric using the customer LAN.

As is recommended in all Stealth installations, the configuration machine should be isolated, and it should use local Stealth authentication (it should not use the Authorization Server).

The Authorization Server can be inside or outside of the Stealth network (although locating it inside the Stealth network is more secure). The Authorization Server must be able to access the AD server, and that AD server must include the user names that the Stealth software will use for each Stealth-enabled Forward! partition.

The most important factor in installing these components is to be sure that they can communicate with the Stealth Appliances using the customer’s regular data network. (The Stealth Appliance does not use the InfiniBand for communication.)

**Note:** Although an Authorization Server is not required, it is recommended in this environment.

**Stealth Appliance Teaming**

If the order includes multiple Stealth Appliances, they can be organized in the same team for load balancing and redundancy. Alternatively, you can configure multiple appliances as stand-alone or each as a team of one, depending on the needs of the environment.

For more information, see “Understanding Appliance Teaming” in the Planning, Installation, and Administration Guide.
Stealth Endpoint Installation

Stealth endpoint software can be installed on any physical or virtual system in the environment that runs a supported operating system, as follows:

- Supported Linux operating systems include Red Hat Enterprise Linux (RHEL) 5.x, Red Hat Enterprise Linux (RHEL) 6.x, SUSE Linux Enterprise Server (SLES) 11.x, and Ubuntu 12.04 LTS.

As described in 20.2.2 Stealth Architecture, if the environment includes servers that cannot run the Stealth endpoint software (because they do not run supported Windows or Linux operating systems), the Stealth Appliance can act as a gateway to traffic in the network.

You install the Stealth endpoint software on a Forward! partition as you would any other configured system running Windows or Linux.

Stealth Licensing Information

You can install the Stealth endpoint software on as many Forward! partitions or other systems as allowed by the licensing agreement with Unisys.

Your order includes Value licenses, which means that components in your environment use a different category of Stealth license depending on the operating system. For the Forward! fabric, your order includes Server licenses for servers running Windows Server 2003, Windows Server 2008, Windows Server 2012, Red Hat Enterprise Linux (RHEL) 5.x or 6.x, SUSE Enterprise Linux Server (SLES) 11.x, or 64-bit Ubuntu 12.04 LTS.

Depending on your environment needs, your order might also include Client licenses for workstations running Windows XP, Windows 7, Windows 8, or 32-bit Ubuntu 12.04 LTS.

**Note:** Be sure to install Stealth only on the appropriate number and type of endpoints allowed by the licensing agreement with Unisys.

Your order also uses Enterprise licensing, which means that you insert one license fob into any appliance in a team, and the licenses are shared between the appliances in the team. Although the control appliance (the first appliance to boot) actually manages the license distribution and maintenance, the license fob can be inserted into any appliance in the team.

See “Understanding Licensing,” in the Planning, Installation, and Administration Guide for more information.
Applicable Stealth Features

All of the standard features of Stealth are available in a Forward! environment, but some features do not apply to Forward! partitions in a typical configuration. Note the following:

- If you are installing the Stealth endpoint software only on Forward! partitions or on servers in the datacenter, the Stealth On Demand and Stealth VPN (also known as Stealth for Secure Remote Access) features do not apply. (This is because Stealth server endpoints should be configured to run Stealth Always On (rather than On Demand) and should not need to use VPN to connect to the Stealth enclave.)
- In a typical environment, access is controlled using user names and passwords (rather than smart cards or one-time passwords); therefore, any information regarding smart cards and one-time passwords does not apply.

20.2.5. General Installation and Configuration Guidelines

The following are specific Forward! guidelines when using the Unisys Stealth Solution Planning, Installation, and Administration Guide to configure your environment:

Configuring the Authorization Server

- You should typically use IntegratedWindowsAuthentication for the Authentication Scheme.
- You should typically use only one authentication scheme to authenticate users.

Using the Provisioning Utility

In general, you should set up filters for the Infrastructure services and for the Fabric Management Platform to ensure that Stealth-enabled Forward! partitions can communicate with these components.

Using the Configuration Utility

- You should generally use the default values for SecureParser M, SecureParser N, and Max Queue Depth.
- Enter the IP address of the Fabric Management Platform for the Network Time Protocol (NTP) server.

Optional Endpoint Software Configuration (Before Endpoint Installation)

The Planning, Installation, and Administration Guide includes optional procedures for endpoint software configuration. In a typical Forward! fabric, you can skip all of these procedures, because this extra configuration is not required. However, you can perform these procedures if you choose to do so or if your environment requires them.
The following are the optional procedures:

- Configuring clear text filters or licensing behavior in endpoint registry for non-silent installs

  This procedure describes how to configure a clear text filter in the registry of a Stealth endpoint; for example, if the domain controllers are not running Stealth endpoint software, but the workstation requires domain authentication, you could create a clear text filter that allows access to the domain controller prior to user log on using this procedure.

  This procedure also describes how to disable the default endpoint licensing behavior and prevent an authenticated endpoint from receiving a license from another appliance team (if multiple appliance teams exist in the environment).

  If the environment does not include either of these circumstances, you can skip this procedure.

- Configuring silent installation for Windows endpoints

  This procedure describes how to create a silent installation package for Windows endpoints. If there are a very large number of Windows workstations and servers to which you want to silently deploy the Stealth software, you might want to perform this procedure. However, if you are deploying the software only to a limited number of Forward! partitions running Windows, you can skip this extra configuration and follow the procedure to install the Stealth endpoint software if silent installation is not configured (and follow the simple prompts when installing the software).

- Using the Consolidation Utility

  This procedure describes how to use the Stealth Consolidation Utility to collate configuration information from multiple Stealth enclaves and create a single installation package that you can install on Stealth endpoints that need access to these various Stealth enclaves (for example, a laptop running Stealth endpoint software that switches enclaves when connecting from different locations like the office or home).

  If you are deploying the software only on Forward! partitions, or if you have only one Stealth enclave, you can skip this procedure.

### Endpoint Software Installation

When you install the Stealth software on Windows endpoints, you must respond to the following questions (assuming you did not configure a silent installation package):

- Should Stealth always be enabled on this computer?

  For Forward! partitions, select **Yes** so that Stealth is configured as Always On.

  However, if you are installing the Stealth endpoint software on other systems that users use both inside and outside the Stealth network, then you can select No and install Stealth On Demand on those systems.

- If you selected the option for Stealth to be Always On, should Stealth VPN be enabled? (If you installed Stealth as On Demand, Stealth VPN can be enabled or disabled using the Stealth applet any time after installation is complete.)

  For Forward! partitions, do **not** enable Stealth VPN.
However, if you are installing the Stealth endpoint software on other Windows systems that users use both inside and outside the Stealth network, and if the configuration must meet all of the requirements for Stealth VPN, then you can enable this feature if needed.

- Should the endpoint use COIs from an Authorization Server or use local authentication?

  It is recommended that an Authorization Server be configured in the environment and that all Forward! partitions use the Authorization Server for authentication.

For Windows Forward! partitions, be sure to perform the procedure to configure server mode after you install the Stealth endpoint software.

For Linux Forward! partitions, perform the appropriate procedures in “Configuring Linux Endpoints.”

**Using Stealth Troubleshooting Information**

For troubleshooting information, refer to the *Planning, Installation, and Administration Guide*.

If you need to report an issue to Unisys using a User Communication Form (UCF), be sure to describe the configuration of the Forward! fabric, how Stealth components (such as the configuration machine and Authorization Server) are integrated in the environment, and what type of endpoints are included in the environment.

**Note:** Information on using Stealth to secure communications between a Stealth enclave and virtual machines located in a public cloud does not apply to the Forward! fabric.
Section 21
Diagnostic Management

The Fabric Manager enables you to collect diagnostic data in the form of dumps for Fabric Management Platform and s-Par® on EPP. A dump file is an archive consisting of log files, command operations, configuration files and so on. You can use the dump file for debugging, troubleshooting, and auditing.

After the dump is collected, you can send it to the Unisys Support Center to help Unisys personnel to analyze the cause of a reported issue.

If you have two Fabric Management Platforms and they are configured as a high availability cluster, be sure to also collect dumps from the second Fabric Management Platform.

This section has the following topics:

- 21.1 Managing Fabric Management Platform Dumps
- 21.2 Managing Platform Dumps


You can generate, download and delete the dump file that is generated for the Fabric Management Platform (FMP).

This section has the following topics:

- 21.1.1 Generating FMP Dumps
- 21.1.2 Downloading FMP Dump File
- 21.1.3 Deleting FMP Dump File

21.1.1. Generating FMP Dumps

You can generate dumps to collect data instantly from all the software components on the FMP for analysis.

**Prerequisite:** FMP is powered on.
Managing Fabric Management Platform Dumps

Caution

If there are already five dump files listed in the System Dumps tab, the files older than the latest five are automatically deleted when you generate a new dump.

To generate dumps
1. On the Fabric Manager user interface, click Manage System on the left pane. Details screen appears on the right pane.
3. Click the System Dumps tab.
4. Click Generate Dump.
   A confirmation message appears.
5. Click Ok.
   The dump file is generated and listed under the System Dumps tab.

21.1.2. Downloading FMP Dump File

You can download a dump file to your local system for analysis.

Prerequisite: Dump file is available under System Dumps tab.

To download a dump file
1. On the Fabric Manager user interface, click Manage System on the left pane. Details screen appears on the right pane.
3. Click the System Dumps tab.
   Note: You can customize the number of columns you want to view. Click the drop-down arrow next to the column to select or clear the required column.
4. Select the dump that you want to download.
5. Click Download.
   The dump file is downloaded to your local system.
21.1.3. Deleting FMP Dump File

You can delete a dump file to remove it from the list.

Prerequisite:
- Dump file is available under System Dumps tab.
- You must have a field engineer or an administrator role.

You can delete a dump to remove it from the list of dumps that are displayed.

To delete a dump
1. On the Fabric Manager user interface, click Manage System on the left pane. Details screen appears on the right pane.
2. Under Details, click the Diagnostics tab.
System Dumps and Settings tabs appear.
3. Click the System Dumps tab.
   Note: You can customize the number of columns you want to view. Click the drop-down arrow next to each of the column heading to select or clear the required column.
4. Select the dump that you want to delete.
5. Click Delete.
   A confirmation message appears.
6. Click Ok.
   The selected dump file is deleted and no longer listed in the System Dumps tab.

Note: By default, the dumps older than the latest five dumps are automatically deleted.

21.2. Managing Platform Dumps

You can generate, download, and delete dump files for the partitionable EPP.

This section has the following topics:
- 21.2.1 Generating Platform Dump
- 21.2.2 Downloading Platform Dump
- 21.2.3 Deleting Platform Dump

21.2.1. Generating Platform Dump

You can generate a platform dump to collect the data instantly for analysis.

Prerequisite: Platform is powered on and s-Par® is running.
To generate a dump
1. On the Fabric Manager user interface, click Manage System on the left pane, expand <Forward-System>, and then select the required platform.
   Details screen appears on the right pane.
2. Under Details, click Diagnostics, and then click the Platform Dumps tab.
   A list of available dumps appears.
3. Click Generate Dump.
   A confirmation message appears.
   **Note:** By default, the Generate Dump button is activated.
4. Click Ok.
   The dump file is generated and listed under the Platform Dumps tab.
   The status of Generate Dump appears under the Events tab as an event INITIATED. Once the status of the event becomes SUCCESS, click the refresh button to view the latest dump file. The event FAILED indicates that the dump file is not generated.

**Notes:**
- The Fabric Manager might take several minutes to generate a dump file depending on how long the platform is up and running.
- You can generate a maximum of 10 dump files for a platform after which the Fabric Manager displays an error message. You need to delete a dump file that is already generated and then generate a new dump file.
- You cannot generate multiple dump files for a platform at the same time. If you try to generate multiple dump files, then the Fabric Manager displays an error message informing you that the dump file generation is already in progress.
- When you perform a Force dump operation on a platform, it generates a fDump. This dump file is displayed in the list of available dumps.

### 21.2.2. Downloading Platform Dump

You can download the platform dump for error analysis.

**Prerequisite:**
- The platform is powered on and s-Par® is running.
- A dump file is available under Platform Dumps tab.

To download a dump
1. On the Fabric Manager user interface, click Manage System on the left pane, expand <Forward-System>, and then select the required platform.
   Details screen appears on the right pane.
2. Under Details, click Diagnostics, and then click Platform Dumps tab.
A list of available dumps appears.

3. Select a dump file from the list of available dump files and then, click **Download**.

   A confirmation message appears.

   **Note:** The **Download** button is enabled only when you select a dump file.

4. Click **Ok**.

   The dump file is downloaded to your local system.

### 21.2.3. Deleting Platform Dump

You can delete a dump file if it is no longer required.

**Prerequisite:**
- The platform is powered on and s-Par® is running.
- A dump file is available under **Platform Dumps** tab.
- You have the field engineer or administrator role.

To delete a dump

1. On the Fabric Manager user interface, click **Manage System** on the left pane, expand `<Forward-System>`, and then select the required platform.

   **Details** screen appears on the right pane.

2. Under **Details**, click **Diagnostics**, and then click the **Platform Dumps** tab.

   A list of available dumps appears.

   **Note:** You can customize the number of columns that you want to view. Click the drop-down arrow next to each of the column headings to select or clear the required column.

3. Select a dump file from the list of available dumps, and click **Delete**.

   A confirmation message appears.

   **Note:** The **Delete** button is enabled only when you select a dump file.

4. Click **Ok**.

   The selected dump file is deleted and no longer listed in the **Platform Dumps** tab.
Section 22
Troubleshooting

This section provides information on various problems that you might come across, and the possible causes and solutions. If you are unable to resolve the problem using the solutions provided in this section contact Unisys service representative.

- 22.1 Troubleshooting Fabric Management Platform Problems
- 22.2 Troubleshooting FFM User Problems
- 22.3 Troubleshooting Image Problems
- 22.4 Troubleshooting Commissioning Failure
- 22.5 Troubleshooting Dump Problems
- 22.6 Troubleshooting Platform Problems
- 22.7 Troubleshooting Hardware Failures
- 22.8 Troubleshooting Info Pane Problems
- 22.9 Troubleshooting Fabric Manager Services Problems
- 22.10 Reporting Problems to Unisys

22.1. Troubleshooting Fabric Management Platform Problems

This section lists the various Fabric Management Platform and Partition Desktop problems, common causes, and their solutions.

- 22.1.1 Troubleshooting Fabric Management Platform Problems
- 22.1.2 Unable to Generate Call Home Events for Fabric Management Platform
- 22.1.3 Unable to Launch Partition Image Console: Browser Settings Problem
- 22.1.4 Unable to Launch Partition Desktop: Installation Problem
## 22.1.1. Troubleshooting Fabric Management Platform Problems

### Health Status of the Fabric Management Platform changes to “Warning” or “Critical”

<table>
<thead>
<tr>
<th>Symptoms</th>
<th>Causes</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>FFM Server Health</strong> status changes to “Critical” or “Warning” state.</td>
<td>Fabric Manager services are not responding.</td>
<td><strong>Recommendations</strong></td>
</tr>
<tr>
<td>• Fabric Manager user interface stops functioning.</td>
<td></td>
<td>• Allow some time for the services to settle down. This might cause health status of the Fabric Management Platform to change to <strong>Ok</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ensure that minimum number of applications are running on the Fabric Management Platform.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If this does not work, then:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Logon to the Fabric Management Platform server as a root user using PuTTY (or use the RDP client session of the Fabric Management Platform). The root user login is root/Administer4Me.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Using the following command restart the Fabric Manager services:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>#rcffmservices stop</td>
</tr>
<tr>
<td></td>
<td></td>
<td>#rcffmservices start</td>
</tr>
</tbody>
</table>
# Troubleshooting Fabric Management Platform Problems

<table>
<thead>
<tr>
<th>Symptoms</th>
<th>Causes</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Memory</strong> status under FFM Server Health changes to “Critical”.</td>
<td>Excessive utilization of the Fabric Management Platform memory.</td>
<td><strong>Recommendation</strong>&lt;br&gt;Ensure that minimum number of applications are running on the Fabric Management Platform.&lt;br&gt;If this does not work, then:&lt;br&gt;1. Logon to the Fabric Management Platform server as a root user using PuTTY (or use the RDP client session of the Fabric Management Platform). The root user login is root/Administer4Me.&lt;br&gt;2. Using the following command to free up the memory in the Fabric Management Platform:&lt;br&gt;   <code>bash&lt;br&gt;   sync; echo 3&gt;/proc/sys/vm/drop_caches&lt;br   </code>&lt;br&gt;&lt;br&gt;<em>Note:</em> Ensure that no other operations are performed in the Fabric Management Platform while executing this command.</td>
</tr>
</tbody>
</table>
| **Swap** status under FFM Server Health changes to “Critical”. | Excessive utilization of the swap memory. | **Recommendation**<br>Ensure that minimum number of applications are running in the Fabric Management Platform.<br>If this does not work, then:<br>1. Logon to the Fabric Management Platform server as a root user using PuTTY (or use the RDP client session of the Fabric Management Platform). The root user login is root/Administer4Me.<br>2. Using the following command free up the memory in the Fabric Management Platform:<br>   ```bash<br>   sync; echo 3>/proc/sys/vm/drop_caches<br   ```
### Troubleshooting Fabric Management Platform Problems

<table>
<thead>
<tr>
<th>Symptoms</th>
<th>Causes</th>
<th>Solutions</th>
</tr>
</thead>
</table>
| Disk status under FFM Server Health changes to “Critical”. | Excessive utilization of the disk memory. | 1. Log on to the Fabric Management Platform server as a root user using PuTTY (or use the RDP client session of the Fabric Management Platform). The root user login is root/Administer4Me.  
2. Browse to the following location: `/usr/local/ffm-db-events-backup`  
3. Save (download) the dump file using the Fabric Manager user interface.  
4. Delete the dump from the Fabric Management Platform. |

#### 22.1.2. Unable to Generate Call Home Events for Fabric Management Platform

**Symptoms**
Call Home events for the Fabric Management Platform (FMP) are not listed in the Events console.

**Cause**
- Post-install script was not run during the factory installation.
- Software services to manage the FMP are corrupted.

**Solution**
1. Log in to the Fabric Management Platform desktop, and open a new terminal session as the root user. The login ID for the root user is root/Administer4Me.

   **Note:** If you are connecting remotely, then use a tool — such as PuTTY or the remote desktop function — of the Fabric Management Platform, and then log in as the root user.

2. Execute the following command to run the post-installation script:

   `# /usr/local/ffm/scripts/post_install.sh`

   Various options to install the Fabric Manager services are displayed in the command prompt.

3. Type 8 in the command prompt to choose the option “Get service tags of FMPs”.

   The message “Successfully updated the DB” appears on the command prompt window.
22.1.3. Unable to Launch Partition Image Console: Browser Settings Problem

Symptoms
Unable to launch the partition image console on Fabric Management Platform.

Cause
Firefox browser preferences are not set by the user to access the Fabric Manager on Fabric Management Platform.

Solution
Note: The partition image console can only be accessed from a Firefox browser session on the Fabric Management Platform since the access to the partition image console is restricted on FM-LAN.

To set the preferences in Firefox browser on the Fabric Management Platform

1. Open the Firefox browser on the Fabric Management Platform with a RDP client (login as administrator/Administer4Me).
2. Type about:config into address bar and press Enter.
   A warning message appears.
3. Click I will be careful, I promise.
   A list of preferences appears.

   Note: This step applies to Firefox version 29. It may vary depending upon the version you use.

4. On preferences window, right-click and select New and Boolean to create a Boolean variable to support the usyscon protocol.

   New Boolean value dialog appears.
5. Type the variable name network.protocol-handler.expose.usyscon and click OK.

   Enter Boolean value dialog appears.
6. Select false and click OK.
   usyscon protocol is set.
7. Next time you click the Launch Console button from Fabric Manager for a selected partition image, you are asked which application to open it with. Navigate to the usyscon.sh script provided under the path /usr/lib/usyscon_partitiondesktop/. You can also check Remember my choice for usyscon links if you do not want the dialog box to come up every time you click Launch Console from the Fabric Manager.
22.1.4. Unable to Launch Partition Desktop: Installation Problem

**Symptoms**  Administrator or Operator is unable to access the Partition Desktop to do the following:

- View the status of the partition image OS installation during the commissioning process.
- Perform the initial configuration of the partition image after successful commissioning.
- Troubleshoot the boot issues of the partition image.

**Cause**

- User did not run the post install script after the ISO is installed.
- The installation software for the Partition Desktop is corrupted or the initial installation did not go through as required.
Solution

Prerequisite

- You are in the FM LAN environment and logged on to the Fabric Management Platform.

- Platform is accessible through FM LAN from Fabric Manager and s-Par is running on the platform.

1. Log in to the Fabric Management Platform desktop, and open a new terminal session as root user.

   (If you are connecting remotely, use a tool like PuTTY or the remote desktop function of the Fabric Management Platform, and login as root user. The root user login is root/Administer4Me.)

2. Execute the following commands to verify that the software packages `unisysauthservice`, `usyscon_partitiondesktop`, and `wine` are installed.

   ```sh
   # rpm -qa | grep unisyscon
   # rpm -qa | grep usyscon_partitiondesktop-4.1.17.23728-1.sles
   # rpm -qa | grep unisysauthservice
   # rpm -qa | grep wine
   ```

3. Execute the following command to verify the services `samba service`, `winbind service`, and `unisysauthservice` are running.

   ```sh
   # rcsmb status
   # rcwinbind status
   # rcunisysauthservice status
   ```

4. If one of the services is not running, execute the following commands to restart the services.

   ```sh
   # rcsmb restart
   # rcwinbind restart
   # rcunisysauthservice restart
   ```

5. Execute the following command to verify that the user (administrator or operator) is added to authentication database.

   ```sh
   # pdbedit -L
   ```

   A list of all the available users appears.

6. On the FMP, access the Fabric Manager and launch the Partition Desktop. See 13.3 Accessing a Partition Desktop for instructions.

7. If the Partition Desktop is still not accessible, execute the following command to reinstall the software packages.

   ```sh
   # /usr/local/ffm/scripts/post_install.sh
   ```

8. Use the Steps 2, 3 and 4 to reinstall and configure the Partition Desktop.
22.2. Troubleshooting FFM User Problems

This section provides various FFM user problems, causes and solutions in following topics:

- 22.2.1 Unable to Search Users
- 22.2.2 Fabric Manager User Forgot Password
- 22.2.3 Resetting Password
- 22.2.4 Unable to Edit Customer Identifier Information

22.2.1. Unable to Search Users

**Symptoms**
Unable to search the Fabric Manager default users using the *Users and Organizations* option in the Portal.

**Cause**
Search reindexing did not happen.

**Solution**
Prerequisite: You have Field Engineer or Administrator privileges.

1. On the Fabric Manager user interface, click *Control Panel*. The Control Panel screen appears on the right pane.
2. On the left pane, under *Server*, click *Server Administration*. The Server Administration appears on the right pane.
3. In the Actions group and next to the *Reindex all search indexes* option, click Execute.

    You will now be able to search the default Fabric Manager users in the *Users and Organizations*.

22.2.2. Fabric Manager User Forgot Password

**Symptoms**
Unable to login to the Fabric Manager.

**Cause**
The Fabric Manager user has forgotten the password.

**Solution**
Contact the Filed Engineer or Administrator to reset the password.

*Note*: If forwardadmin user forgets the password then contact Unisys service representative.

22.2.3. Resetting Password

**Symptoms**
Unable to login to the Fabric Manager.

**Cause**
The Fabric Manager user has forgotten the password.
**Troubleshooting Image Problems**

**22.2.4. Unable to Edit Customer Identifier Information**

**Symptoms**: Unable to edit the field ID* (customer identifier) information in Customer Info. tab under Customer and Call Home Information tab of Fabric Manager.

**Cause**: Fabric Manager does not allow you to edit the ID* field.

**Solution** **Prerequisite**: Atleast one EPP is added to the fabric.

1. Logon to Forward! Fabric Management Platform desktop, and open a new terminal session as a root user.
   
   (If you are connecting remotely, use a tool like PuTTY or the remote desktop function of the Fabric Management Platform, and login as root user. The root user login is root/Administer4Me).

2. Run the command `cd /usr/local/ffm/scripts`.

3. Run the command `./setCustomerId.sh`.
   
   This assigns the Service tag of the EPP as customer identifier.

**22.3. Troubleshooting Image Problems**

This section describes various Image problems, causes and solutions.

- [22.3.1 Unable to view the recently added image in Fabric Manager](#)
- [22.3.2 Unable to Add a Blueprint or an Image](#)
- [22.3.3 Unable to Shut Down the Partition Image](#)
### 22.3.1. Unable to view the recently added image in Fabric Manager

**Symptoms**  
The recently added image is not listed under the **Software** tab.

**Cause**  
Browser does not automatically refresh when a new image is added.

**Solution**  
In the **Software** tab, click **Refresh**.

### 22.3.2. Unable to Add a Blueprint or an Image

**Symptoms**  
Unable to add a blueprint or an image to the Fabric Management Platform.

**Cause**  
The physical memory of the Fabric Management platform is used by the applications as cache or buffer.

**Solution**  
Free up the in Fabric Management Platform by executing the command

```
sync; echo 3>/proc/sys/vm/drop_caches
```

*Note: No other operations should be performed on the Fabric Manager while executing this command.*

### 22.3.3. Unable to Shut Down the Partition Image

**Symptoms**  
Unable to shut down the partition image.

**Cause**  
When a screensaver is active and locked using a password on Windows 2008 R2, Windows 2012 or Windows 2012 R2, you cannot perform any operation on that partition image. To perform any operation, you must unlock the screen using the password of the partition image.

**Solution**  
**Prerequisite:** Ensure a screensaver is not active prior to issuing a partition image shutdown request or clear the screensaver option so that it does not require a password on resume.

To shut down the partition image

1. Using a RDP client software (for example, Remote Desktop Connection on a Windows Computer), access the partition image that is hung shutting down.
2. From the Windows desktop, perform **Shutdown** operation.

   An error message appears instructing you to synchronize the I/O data.

*Note: Process of shutting down the Windows 2008 R2 differs for later versions.*
22.4. Troubleshooting Commissioning Failure

This section provides information on roll back failure when the commission fails and possible solutions.

**Symptoms**  
If the commissioning of a partition image is unsuccessful, the Roll Back function of the Fabric Manager user interface and s-Par® may also fail. The Roll Back function can:

- Fail in both s-Par® and Forward! Fabric Manager
- Fail in s-Par® but succeed in Forward! Fabric Manager
- Fail in Forward! Fabric Manager but succeed in s-Par®

This is indicated in the event console of the Fabric Manager user interface. The state of the partition image is displayed as **Unknown** or **Inactive**.

**Impact**  
All the s-Par® resources such as LUNs, chassis, and LAN subnets that are used by the failed partition image are blocked and cannot be used for commissioning another partition image. Also, the images and blueprints associated with the failed partition image cannot be deleted.

**Solution**  
1. Identify the s-Par® IP address. For more information, see 22.4.1 Identifying the s-Par® IP Address.
2. Determine the UUID. For more information, see 22.4.2 Determining the Universal Unique Identifier (UUID) of a Partition Image.
3. Perform one of the following:
   - If the roll back failed in both s-Par® and Forward! Fabric Manager
     a. Delete the partition image. For more information, see 22.4.3 Deleting a Partition Image.
     b. Clean FFM environment using the FMP desktop. For more information, see 22.4.4 Cleaning the FFM Environment.
   - If the roll back failed in s-Par® but succeed in Forward! Fabric Manager, clean up the s-Par® environment. For more information see 22.4.3 Deleting a Partition Image.
   - If the roll back failed in Forward! Fabric Manager but succeed in s-Par®, clean up FFM using the FMP desktop. For more information see 22.4.4 Cleaning the FFM Environment.

- 22.4.1 Identifying the s-Par® IP Address
- 22.4.2 Determining the Universal Unique Identifier (UUID) of a Partition Image
- 22.4.3 Deleting a Partition Image
- 22.4.4 Cleaning the FFM Environment
22.4.1. Identifying the s-Par® IP Address

To identify the s-Par® IP address perform the following steps on the Fabric Manager user interface:

1. On the Fabric Manager user interface, click Manage System.
   
   The Manage System appears on the left pane and Details appears on the right pane.

2. Under Details, in the Summary tab, click Edit.
   
   The Edit System screen appears.

3. Select the LAN Subnets tab and view the FM-LAN IP Subnet value.
   
   The four octet s-Par® IP address is formulated based on the FM-LAN network ID, platform number and the assigned default value. The first two octets of s-Par® IP address is the default FM-LAN network ID (FM-LAN IP Subnet value). The third octet would be the platform number. The fourth octet would be the assigned default value.

   For example, if the four octet value displayed under Subnet field is 172.29.1.253, then the first two octets 172.29 are the default FM-LAN IP value, the third octet 1 is the platform number, and the fourth octet 253 is the assigned default value.

22.4.2. Determining the Universal Unique Identifier (UUID) of a Partition Image

To determine the UUID of the partition image

1. Using RDP client software, for example, Remote Desktop Connection on a Windows computer, log on to the Fabric Management Platform.

2. In the Firefox browser, type the s-Par® IP address. For example, 172.29.1.253.

   The partition console appears.

3. Log on to the partition console using the following credentials:
   
   Username:
   Administrator
   
   Password:
   Administer4Me

4. In the Summary page, click on the partition image you want to delete.

   The Partition Summary page now displays the UUID.

22.4.3. Deleting a Partition Image

Prerequisites

- s-Par® IP address is available
- UUID of the partition is available
To clean up the s-Par®, execute the following commands on a FMP terminal session:

1. Run the following command:

```
wsman invoke -a RequestStateChange -optimize http://schema.unisys.com/wbem/wscim/
1/cim-schema/2/spar/
SPAR_SoftPartitionComputerSystem?__cimnamespace=root/
virt,Name=<partition_image_uuid>,
CreationClassName=SPAR_SoftPartitionComputerSystem" --transport-timeout=15 --
hostname=<s_par_ip_address> --port=443 --auth=basic
--username=Administrator --password=Administer4Me --noverifypeer --noverifyhost --
cacert=/dev/null -k RequestedState=60011
```

where

- `<partition_image_uuid>` is the UUID name of the partition image
- `<s_par_ip_address>` is s-Par® IP address of the Platform

Partition image is disabled.

2. Run the following command:

```
SPAR_SoftPartitionComputerSystem?__cimnamespace=root/
virt,UUID=<partition_image_uuid>,CreationClassName=SPAR_SoftPartitionComputerSystem"
--transport-timeout=15 --hostname=<s_par_ip_address> --port=443 --auth=basic --
username=Administrator --password=Administer4Me --noverifypeer --noverifyhost --
cacert=/dev/null
```

where

- `<partition_image_uuid>` is the UUID name of the partition image
- `<s_par_ip_address>` is s-Par® IP address of the partition image

The partition image is deleted.

### 22.4.4. Cleaning the FFM Environment

To clean up the FFM environment, execute the following commands on a FMP terminal session:

1. Run the command `cd /usr/local/ffm/scripts`.
2. Run the command `./deleteDeviceByName.sh`
   A prompt appears to type the device (platform or partition) name.
3. Type the name of the device that you want to delete.
   This removes the device from the database, with nagios configuration file and then, restarts the nagios.

### 22.5. Troubleshooting Dump Problems

This section provides various dump problems, causes and solutions.

- **22.5.1 Unable to Generate the Dump**
22.5.1. Unable to Generate the Dump

**Symptoms**
Unable to generate the dump using the Fabric Manager.

**Cause**
Fabric Manager user interface is down and not allowing you to generate the dumps.

**Solution**
1. Log on to the Fabric Management Platform as root user using PuTTY.
2. Execute the command
   
   ```bash
   /usr/local/ffm/scripts/generate_dumps_chk.pl /root
   ```
   By default, the dumps are collected under root folder. You can change the destination to a different folder based on your requirement.

22.5.2. Unable to download the dump

**Symptoms**
Unable to download the dump from the Fabric Manager user interface.

**Cause**
Fabric Manager user interface is down and not allowing you to download the dumps.

**Solution**
1. Log on to the Fabric Management Platform as root user using PuTTY.
2. Use the following command to go to the dump files folder:
   
   ```bash
   cd /usr/local/ffm/liferay-portal/tomcat-7.0.40/webapps/ROOT/attachments/
   ```
3. Use the command `ls` to list the dump files.
   
   The list of dump files appears.
4. Use one of the following methods to copy the dump files to your system:
   - Use the command
     
     ```bash
     scp <SOURCE DIR/FILE> <DESTINATION DIR/FILE>
     ```
   - Use utilities such as “winscp” to copy the files between Fabric Management Platform and your system.

22.5.3. Unable to view the downloaded dump

**Symptoms**
Unable to view the downloaded dump in the Fabric Manager user interface.
Troubleshooting Dump Problems

### 22.5.4. Unable to Delete the Dump

**Symptoms**
Using the Fabric Manager you are unable to delete the dump.

Unable to delete the dump using the Fabric Manager user interface.

**Cause**
Fabric manager is not functional and you are unable to delete the dumps.

Fabric Manager is down and not allowing you to delete the dumps.

**Solution**

1. Log on to the Fabric Management Platform as root user using PuTTY.
2. Use the following command to go to the dump files folder:
   \`cd /usr/local/ffm/liferay-portal/tomcat-7.0.40/webapps/ROOT/attachments/\`
3. Use the command `ls` to list the dump files.
   The list of dump files appears.
4. Use one of the following methods to copy the dump files to your system:
   - Use the command
     \`scp <SOURCE_DIR/FILE> <DESTINATION_DIR/FILE>\`
   - Use utilities such as “winscp” to copy the files between Fabric Management Platform and your system.

   The deleted dump is removed from the list of available dumps.

### 22.5.5. Unable to Display the Dumps

**Symptoms**
Unable to view the dumps from Fabric Manager user interface.

**Cause**
Fabric Manager user interface is down and not allowing you to view the dumps.
**Troubleshooting Platform Problems**

**Solution**

1. Log on to the Fabric Management Platform as root user using PuTTY.
2. Use the following command to go to the dump files folder:
   `cd /usr/local/ffm/liferay-portal/tomcat-7.0.40/webapps/ROOT/attachments/`
3. Use the command `ls` to list the dump files.
   The list of dump files appears.

22.6. **Troubleshooting Platform Problems**

This section provides information on various problems that you might come across and possible causes and solutions.

- 22.6.1 Unable to add the platform
- 22.6.2 Unable to view recently added platform
- 22.6.3 Platform Health is shown as Unknown, Critical or Warning
- 22.6.4 Unable to delete the partitionable EPP
- 22.6.5 Unable to get the Chassis Details of partitionable EPP
# 22.6.1. Unable to add the platform

## Symptom

When you attempt to add a platform using the **Add Platform** option on the **Platform Summary** page, the Fabric Manager user interface does not add the platform to the fabric. The error message “Unable to add the platform” appears.

## Causes

- Power cord is not connected to the platform.
- FM LAN switch is not connected to the platform.
- Default IP address of the platform is not properly configured.

## Solutions

- Manually verify if the platform is connected to the AC power.
- Manually verify if the platform is connected to the FM LAN switch.
- Verify if the platform’s default IP address is correctly configured. If you do not have the IP address details, contact the Unisys service representative.
- Platform settings and configurations such as BIOS settings should be verified. Contact the Unisys service representative for modifying the settings.

### Network settings are not configured in the platform management console.

In the platform management console
1. Verify if the IPMI connections are enabled.
2. Verify if the **forwardfm** user is created.
3. Verify if the processor frequency, core count, and memory are supported by Fabric Management Platform.

**Note:** Only field engineer has the privilege to log in to the platform management console.

### s-Par® IP is not properly configured.

If the platform is a PEPP then power on the platform using the Platform Management Console. After few minutes, ping the default s-Par® IP address. If the ping is successful, you can add the platform.

If the ping is not successful, contact the Unisys service representative and report the problem.

### Platform management card NTP settings are not disabled and cleared before adding platform

Disable the NTP setting and clear the NTP server settings on platform management card using the platform management console.

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Causes</th>
<th>Solutions</th>
</tr>
</thead>
</table>
| When you attempt to add a platform using the **Add Platform** option on the **Platform Summary** page, the Fabric Manager user interface does not add the platform to the fabric. The error message “Unable to add the platform” appears. | - Power cord is not connected to the platform.  
- FM LAN switch is not connected to the platform.  
- Default IP address of the platform is not properly configured. | - Manually verify if the platform is connected to the AC power.  
- Manually verify if the platform is connected to the FM LAN switch.  
- Verify if the platform’s default IP address is correctly configured. If you do not have the IP address details, contact the Unisys service representative.  
- Platform settings and configurations such as BIOS settings should be verified. Contact the Unisys service representative for modifying the settings. |
| Network settings are not configured in the platform management console. | | In the platform management console  
1. Verify if the IPMI connections are enabled.  
2. Verify if the **forwardfm** user is created.  
3. Verify if the processor frequency, core count, and memory are supported by Fabric Management Platform.  
**Note:** Only field engineer has the privilege to log in to the platform management console. |
| s-Par® IP is not properly configured. | | If the platform is a PEPP then power on the platform using the Platform Management Console. After few minutes, ping the default s-Par® IP address. If the ping is successful, you can add the platform.  
If the ping is not successful, contact the Unisys service representative and report the problem. |
| Platform management card NTP settings are not disabled and cleared before adding platform | | Disable the NTP setting and clear the NTP server settings on platform management card using the platform management console. |
### Troubleshooting Platform Problems

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Causes</th>
<th>Solutions</th>
</tr>
</thead>
</table>
| When you attempt to add a platform using the **Add Platform** option on the **Platform Summary** page, the Fabric Manager user interface does not add the platform to the fabric. The error message “Unable to configure the Platform Management Card FM-LAN IP Address” appears. | Network connectivity issues or IPMI setting issues. | 1. Reset the platform to its default IP addresses.  
2. Make sure BIOS, platform management card, s-Par® instance (applicable to PEPP) settings are set back to the default values. |
| Fabric Manager fails to roll back to the platform management card’s previous default IP address. |  | **Note:** It is recommended to perform this step with the assistance from Unisys Service Representative. |
| An attempt to re-add the platform fails. | | |

#### 22.6.2. Unable to view recently added platform

**Symptoms**

When you click and expand `<Forward-System>` in the Fabric Manager user interface and try to view the underlying platforms, the newly added platform is not visible.

**Cause**

Browser does not refresh automatically when a new platform is added.

**Solution**

Refresh the browser to view the newly added platform.

#### 22.6.3. Platform Health is shown as Unknown, Critical or Warning

**Symptoms**

Platform Health status indicates Unknown, Critical, or Warning
**Cause**  
Excessive usage of the platform resources

**Solution**  
From the list of events, identify the events related to the platform health status. With the help of the events, analyze the reasons for platform’s health status is changed to Unknown, Critical or Warning. After taking a corrective action to address the issues, do the following:

- Refresh the browser from which you are accessing the Fabric Manager user interface.
- In the Fabric Manager user interface, click **Events** and then close the relevant event.

The health status of the platform gets updated.

---

### 22.6.4. Unable to delete the partitionable EPP

**Symptoms**  
Unable to delete the platform using the Fabric Manager user interface.

**Cause**  
Network settings are not configured in the platform management console.

**Solution**  
**Prerequisite:** If the platform type is PEPP then it should be in ON state.

Log on to the platform management console and verify if

- the IPMI connections are enabled.
- forwardfm user has been created.
- processor frequency, core count, and memory are supported by Fabric Management Platform.

**Note:** Only a field engineer has the privilege to log into the platform management console.

---

### 22.6.5. Unable to get the Chassis Details of partitionable EPP

**Symptoms**  
An error message stating “Unable to get the details for Chassis on platform error” appears at the end of adding the platform operation.

**Cause**  
- The I/O information did not get saved on database for the platform on which the commissioning is initiated.
- The I/O information is not up to date for the platform.
Solution | Prerequisite:
--- | ---
• After adding the partitionable EPP, a **Success** event is generated and it is available in the events list.
• A message stating that the I/O information update failed for the platform is generated. This message is updated in the audit messages itself.

To update the I/O information

1. On the Fabric Manager user interface, click **Manage System** on the left pane, expand `<Forward-System>`, and then select the platform that you added.

   **Details** screen appears on the right pane.

2. Under **Details**, click **Config. Info** tab.

   An error message appears instructing you to synchronize the I/O data.

3. Click **Ok** and then click **Synchronize**.

   The I/O information is saved on the database. This enables you to commission a partition image on partitionable EPP.

   **Note:** If this error appears when you initiate a Commissioning process on the platform, you can still ignore the message to continue the operation. This error message does not impact the commissioning process.

---

22.7. Troubleshooting Hardware Failures

This section provides information on various problems that you might come across and possible causes and solutions.

- 22.7.1 Fabric Management Platform Suffers a Repairable Failure
- 22.7.2 Fabric Management Platform Suffers a Catastrophic Failure

### 22.7.1. Fabric Management Platform Suffers a Repairable Failure

**Symptoms**

Fabric Management Platform suffers failure and is repairable. However, the disks are not corrupt.

**Solution**

Contact Unisys service representative for further assistance.

### 22.7.2. Fabric Management Platform Suffers a Catastrophic Failure

**Symptoms**

Fabric Management Platform has suffered a catastrophic failure and the disks are corrupt.
Solution If you have planned for a cold spare, then you can swap over to the cold spare Forward Management Platform. Contact Unisys service representative for further assistance.

22.8. Troubleshooting Info Pane Problems

This section provides information on various Info Pane problems that you might come across and possible causes and solutions.

- 22.8.1 Info Pane Content does not Get Refreshed

22.8.1. Info Pane Content does not Get Refreshed

Symptoms When you switch between the tabs in Fabric Manager user interface, Info Pane content does not get refreshed. It shows the same content as in previous content pane.

Cause The maximum allowed cache memory is utilized by the application.

Solution Clear the browser cache. See browser help for information on clearing the cache.

22.9. Troubleshooting Fabric Manager Services Problems

This section provides information on various problems that you might come across and possible causes and solutions. It also talks about the best practices that you should to follow so that the Fabric Manager keeps up and running.

Best Practices

- Do not leave any of the RDP client sessions unattended.
- Limit the number of RDP client sessions to Fabric Management Platform.
- Limit the number of browser sessions opened on Fabric Management Platform.
- Always logout from the ssh or RDP client session rather than closing the window.
- Do not leave any browser session opened on the Fabric Management Platform.
- Before you logout from Fabric Management Platform, ensure that all the applications are closed.

This section has the following topics:

- 22.9.1 Fabric Manager Services are not functional
22.9.1. Fabric Manager Services are not functional

**Symptoms**

- Uploaded blueprints/images do not appear in the list of images in Fabric Manager User Interface.
- Various buttons in the user interface are not functional.
- Fabric Manager User Interface does not get loaded or not accessible or access to user interface is very slow.
- Database operations are getting affected. Due to this,
  - events may not appear
  - some part of the user interface is unaccessible
  - unable to access the user interface
- FFM Server health status remain in Warning or Critical for long time.
- Data in user interface becomes inaccurate which was accurate earlier.
- Status of the platform and partition images under Manage System does not refresh.
- Events are not updated.
- Some of the operations are inconsistent.
- Any other issues where troubleshooting steps without an attempt to restart the Fabric Manager services did not work.

**Cause**

Fabric Manager services are not working
Solution

1. Ensure that there are no active operations such as partition or platform operations, commissioning or decommissioning operations are in progress. If the operations are in progress, wait until they are complete and success or failure event is generated.

2. Logout from Fabric Manager.

3. Close all the RDP client sessions to Fabric Management Platform.

4. Close all the applications and browser sessions that are running on the Fabric Management Platform.

5. Close all remote browser sessions accessing Fabric Manager User Interface.

6. Logon to the Fabric Management Platform as root user using ssh client like PuTTY.

7. Close all the RDP client sessions using the command:
   
   #rcxrdp restart

8. Use the following commands to Start, Stop, or check the status of Fabric Manager services:

   - To check the status of Fabric Manager services, use:
     
     #rcffmservices status

   - To stop the Fabric Manager services, use:
     
     #rcffmservices stop

   - To start the Fabric Manager services, use:
     
     #rcffmservices start

   **Note:** After the services are started, it takes at least 2 to 3 minutes before the Fabric Manager becomes accessible from a browser session.

If the above procedure does not resolve the issue, reboot the Fabric Management Platform and then, restart Fabric Manager services.

**Note:** Reboot the Fabric Management Platform in consultation with Unisys service representative.

To reboot the Fabric Management Platform:

1. Logon to the Fabric Management Platform as root user using an ssh client like PuTTY.

2. Stop the Fabric Manager services using the command:

   #rcffmservices stop

3. Reboot the Fabric Management Platform using the command:

   #reboot
Further Information

Figure 22–1, provides the information on codes for verifying the status of Fabric Manager services and their output.

Figure 22–1. Fabric Manager Service commands and their output

22.10. Reporting Problems to Unisys

The Unisys Support Center provides support for your Forward! fabric. For access to product support and documentation, visit the Unisys Support website:

http://www.unisys.com/unisys/support/index.jsp?id=3400003

To request support, do one of the following:
• Submit a request on the Unisys eService Portal (http://www.serviceonline.unisys.com).

If you are a first-time user, register using the New User Registration link and then request access to the products for which you are entitled to support.

To submit a Service Request, log on to the Unisys eService Portal, click Create Service Incident, and follow the on-screen instructions.

The following video demonstrates the registration process and other capabilities of the Unisys eService Portal:

http://webcast.unisys.com/flvplay/player_flv_webinar.asp?id=2751eservice_demo

• Call the Unisys Call Reception Center (CRC).

In the United States, the toll-free phone number is 800-328-0440.

Outside the United States, use the Telephone Support link on the Unisys Support website to locate your toll-free phone number:

http://www.unisys.com/unisys/support/index.jsp?id=3400003

When calling the Call Reception Center, please be ready to provide the following information:

– Customer number (also called Installed at Number or IA Number)
– Serial number
– Description of problem

After you enter a Service Request, an analyst from your regional Customer Support Center (CSC) contacts you. The analyst works with you to ensure the issue is fully understood and, if necessary, contacts Unisys engineering on your behalf. During this process, the analyst may request additional diagnostic information.

When analysis is complete, the analyst updates the Service Request with the findings, a resolution, or the details of a workaround.
# Appendix A
## User Roles and Privileges

### Table A–1. User Roles and Privileges

<table>
<thead>
<tr>
<th>No.</th>
<th>Task</th>
<th>Field Engineer</th>
<th>Administrator</th>
<th>Operator</th>
<th>Observer</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Platform Management</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Add and edit initial configuration of the Platform</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>2</td>
<td>Power on Platform</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>3</td>
<td>Power off Platform</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>4</td>
<td>Graceful Shutdown</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>5</td>
<td>Reset Platform (Warm boot)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6</td>
<td>Power Cycle Platform (Cold boot)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>7</td>
<td>Halt System Operation</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>8</td>
<td>Configure PMC</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>9</td>
<td>Configure Platform Time</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>10</td>
<td>View Overall Platform Health Status</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>11</td>
<td>View Platform Status</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>12</td>
<td>Launch PMC</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>13</td>
<td>Launch platform management card console</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>14</td>
<td>View s-Par® Instance Status</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>15</td>
<td>Launch s-Par® Instance KVM Console</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td><strong>Partition Management</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Commission a Partition</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>2</td>
<td>Decommission a Partition</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>User Roles and Privileges (cont.)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>----------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>View Partition Status</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>4</td>
<td>View Partition Settings</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>5</td>
<td>Modify Partition Settings</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6</td>
<td>Perform Partition Action</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>7</td>
<td>Manage Unisys Gold Image</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Fabric Manager Monitoring**

|   | Monitor Common Infrastructure | Yes | Yes | Yes | No |
| 2 | Monitor Platform | Yes | Yes | Yes | No |
| 3 | Monitor Partition | Yes | Yes | Yes | Yes |
| 4 | Monitor Alerts | Yes | Yes | Yes | No |

**Portal Administration**

|   | Create / Modify / Delete a User group | Yes | Yes | No | No |
| 2 | Create / Modify / Delete a User | Yes | Yes | No | No |
| 3 | Add / Delete user to User group | Yes | Yes | No | No |
| 4 | Create / Modify / Delete a Role | Yes | Yes | No | No |
| 5 | Add/Delete permission to a Role | Yes | Yes | No | No |
| 6 | Map Role to a User/User group | Yes | Yes | No | No |
| 7 | Add / Modify operations to a custom portlet | Yes | Yes | No | No |
Appendix B
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 Table B–1, 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 B–1. Worksheet for commissioning

<table>
<thead>
<tr>
<th>Tab</th>
<th>Write the selected parameter details</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Select Blueprint</strong></td>
<td></td>
<td>SLES11-SP3-STANDARD</td>
</tr>
<tr>
<td>Blueprint</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Set Basic Info.</strong></td>
<td></td>
<td>Partition1</td>
</tr>
<tr>
<td>Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host Name</td>
<td></td>
<td>Partition1</td>
</tr>
<tr>
<td>Description</td>
<td></td>
<td>new partition</td>
</tr>
<tr>
<td><strong>Allocate Resource</strong></td>
<td></td>
<td>Chassis -B</td>
</tr>
<tr>
<td>Partition Chassis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Partition Size</td>
<td></td>
<td>Small</td>
</tr>
<tr>
<td>LUN Size</td>
<td></td>
<td>23.0GB</td>
</tr>
<tr>
<td>Enable Hyper-Threading (HT)</td>
<td></td>
<td>Checked</td>
</tr>
<tr>
<td><strong>Set State &amp; Credentials</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
<td>abc123!</td>
</tr>
</tbody>
</table>
Appendix C  
Call Home Configuration Parameters

The following table describes the various Call Home configuration parameters that are listed in the Customer & Call Home Information screen of the Forward! Fabric Manager.

* Denotes required information.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Customer Information</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name*</td>
<td>Configures the customer name that is recognized by the Service Request Management System (SRMS). It is used to identify the customer if the CustomerID is missing or invalid. The customer name can be up to 30 alphanumeric values and can include spaces.</td>
<td>XYZ Company Limited</td>
</tr>
<tr>
<td>Street*</td>
<td>Configures the customer’s street address. It is used to identify the customer’s location if the CustomerID is not recognized or if the address is other than the one contained in the customer record. This information can contain up to 24 alphanumeric values including spaces.</td>
<td>678 Street</td>
</tr>
<tr>
<td>Address</td>
<td>Configures the customer’s suite, floor, and other address information. This information can contain up to 60 alphanumeric values including spaces.</td>
<td>Suite 8B, 3rd Floor</td>
</tr>
<tr>
<td>City*</td>
<td>Configures the customer’s city. This information can contain up to 30 alphanumeric values including spaces.</td>
<td>Philadelphia</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>State*</td>
<td>Configures the customer’s state. This information can contain up to 15 alphanumeric values.</td>
<td>Middlesex PA</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> For the United States, this value is restricted to two-digit abbreviations. This restriction does not apply for other countries.</td>
<td></td>
</tr>
<tr>
<td>Country*</td>
<td>Configures the customer’s country. This information can contain up to 15 alphanumeric values.</td>
<td>India</td>
</tr>
<tr>
<td>Post Code*</td>
<td>Configures the customer’s postal code or ZIP code. This information can contain up to 10 alphanumeric values.</td>
<td>90210 A23-1011</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> For the United States, this value is restricted to five digits. This restriction does not apply for other countries.</td>
<td></td>
</tr>
<tr>
<td>ID*</td>
<td>Configures the unique customer identifier. The customer number can be up to 30 alphanumeric values in free format.</td>
<td>113658047</td>
</tr>
<tr>
<td>Contact Name*</td>
<td>Configures the customer contact name for Unisys call back (if required). This information can contain up to 20 alphanumeric values.</td>
<td>Anderson</td>
</tr>
<tr>
<td>Contact Phone</td>
<td>Configures the phone number for the Contact Name. This information can contain up to 22 alphanumeric values.</td>
<td>01-203-555-1212-5555 For US, where 01 is the country code, 203 is the area code, 555 is the exchange code, 1212 is the number, and 5555 is the extension number (optional).</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Console Phone</td>
<td>Configures the phone number of the operator’s console.</td>
<td>01-203-555-1212-5555</td>
</tr>
<tr>
<td></td>
<td>This information can contain up to 22 alphanumeric values.</td>
<td>For US, where 01 is the country code, 203 is the area code, 555 is the exchange code, 1212 is the number, and 5555 is the extension number (optional).</td>
</tr>
<tr>
<td></td>
<td><strong>Notes:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Do not use space.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• For the United States, the format must be as shown in the example.</td>
<td></td>
</tr>
<tr>
<td>Remote Phone</td>
<td>Configures the phone number of the remote support interface (modem).</td>
<td>01-203-555-1212-5555</td>
</tr>
<tr>
<td></td>
<td>This information can contain up to 22 alphanumeric values.</td>
<td>For the United States, where 01 is the country code, 203 is the area code, 555 is the exchange code, 1212 is the number, and 5555 is the extension number (optional).</td>
</tr>
<tr>
<td></td>
<td><strong>Notes:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Do not use space.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• For the United States, the format must be as shown in the example.</td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td>Configures the email address of the Contact Name.</td>
<td><a href="mailto:john.smith@customer.com">john.smith@customer.com</a></td>
</tr>
<tr>
<td></td>
<td>This information can contain up to 80 alphanumeric values without spaces.</td>
<td></td>
</tr>
<tr>
<td>Department</td>
<td>Configures the location of the reporting product within the customer’s facility.</td>
<td>Accounts</td>
</tr>
<tr>
<td></td>
<td>This information can contain up to 15 alphabetic characters.</td>
<td></td>
</tr>
<tr>
<td>CUIC</td>
<td>Configures the country code in which the calling system is located.</td>
<td>CA</td>
</tr>
<tr>
<td></td>
<td>It is a X.400 standard specific two-lettered, upper case alphabetic country code.</td>
<td></td>
</tr>
<tr>
<td>Special Handling</td>
<td>Configures the escalation comments on the contact information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This information can contain up to 512 alphanumeric values.</td>
<td></td>
</tr>
</tbody>
</table>
### Call Home Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sys Style</td>
<td>This is Unisys Style number for the host system or product. This field is populated by default during the Fabric Manager installation.</td>
<td>2200/500</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A16</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DP500</td>
</tr>
<tr>
<td>Host Name*</td>
<td>Configures the name of the host on the Unisys Customer Support Center, which receives the call packets.</td>
<td>callhome.unisys.com</td>
</tr>
<tr>
<td></td>
<td>This information can contain up to 64 alphanumeric values accepted with standard product nomenclature.</td>
<td></td>
</tr>
<tr>
<td>Host Port*</td>
<td>Configures the port number of the host on the Unisys Customer Support Center.</td>
<td>443</td>
</tr>
<tr>
<td>Number of Retries</td>
<td>Configures the number of times the modem should retry if it fails to connect to the Internet.</td>
<td>1</td>
</tr>
<tr>
<td>Seconds Between Retries</td>
<td>Configures the time in seconds for which the modem should wait before retrying for connection.</td>
<td>10</td>
</tr>
<tr>
<td>Connection Type</td>
<td>Configures the type of LAN.</td>
<td>lanwithoutproxy</td>
</tr>
<tr>
<td>Communicate Test Packet</td>
<td>Configures the test packet for testing the Call Home feature.</td>
<td></td>
</tr>
</tbody>
</table>