IBM Flex System and IBM PureFlex Firmware Updates Best Practices

Flex Version 1.3.3
(June, 2015)

IBM Flex System and IBM PureFlex Firmware Updates Best Practices

Flex Version 1.3.3
(June, 2015)

First Edition (June 2015)

Contents

Chapter 1. Introduction

This document describes the best practices for updating the firmware and management software for IBM Flex System and IBM PureFlex components. It provides instructions for updating the firmware and management software to version 1.3.3.

Important Considerations

- Security is one of the highest priorities for IBM and our customers. The IBM Product Security Incident Response Team (PSIRT) is a global team that manages the receipt, investigation and internal coordination of security vulnerability information related to IBM offerings. Before you update firmware for the IBM Flex System products, you can go to the following site to determine if there are any security issues that have been identified for the Flex System products:

  https://www.ibm.com/connections/blogs/PSIRT/?lang=en_us
- Make sure that you verify the part number of the fan logic modules in your chassis and replace them if necessary.

  ECA083 (Engineering Change Announcement) provides for proactive replacement of the fan logic module in a limited number of IBM PureFlex systems.
- Use this document to upgrade firmware if the IBM FSM that you have installed is currently at version 1.3.0 or higher. If the IBM FSM version is earlier than 1.3.0, make sure that you review 1.1, "Upgrading from an earlier version of Flex System firmware," on page 3.
- Before beginning to update the IBM Flex System and IBM PureFlex components, you should check for any Service Bulletins related to updates. Service Bulletins related to updates are available at this website:

  http://www.ibm.com/Search/?q=%22retain+tip%22++AND+update+AND+problem+AND+flex+OR+pureflex&co=us&lo=any&ibm-submit.x=0&ibm-submit.y=0&sn=&lang=en&cc=US&en=utf&hpp=

Note: To filter or expand the results, add or remove terms from the search query.

Special Considerations for Intelligent Cluster Systems

For Flex Systems that are shipped as Intelligent Clusters, these systems follow a designed Best Recipe for both Software and Firmware levels. Intelligent Cluster systems are shipped as a solution and have been tested for interoperability. Each cluster is shipped with specific code levels for each of the components included in the Bill of Materials and these levels should be strictly adhered to. Due to the interdependencies of the components within a cluster, any deviation from approved Best Recipe code levels must first be evaluated and approved by Product Engineering and Cluster development prior to updating code.

In the rare event the need exists to update code levels in a cluster outside of the approved Best Recipe, the code update procedures and order of updates contained in this guide can be followed directly for updating the individual components. Note that this should only occur after the evaluation and approvals have been obtained from engineering and development.

Contact your local IBM Service Representative for additional information regarding your specific Customer Support Plan (CSP) for your installation.

Firmware updates for IBM Flex System and IBM PureFlex components are tested and released together. Therefore, you must update all components in a chassis to the same software level, as defined at the IBM PureSystems Centre website.

Tips:

- Firmware updates require that components be restarted for the updates to take effect. Therefore, updates will be disruptive unless you have virtualization (such as KVM, VIOS, or ESX) and mobility configured with resources available to evacuate compute nodes and update them individually.

  For more information about virtualization, see the quick start guides, which are available at this location:

  http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.commontasks.doc/commontasks_virtualization.html

  For more information about ESX, see the VMware website at this location:

  http://www.vmware.com/
- To minimize service disruptions when updating I/O modules (switches and pass-thru modules), make sure that you update I/O modules sequentially.

When updating the firmware for IBM Flex System and IBM PureFlex components, you need to perform the updates in the following order:

1. Update the components in the chassis.
   - If you are updating chassis components through an IBM Flex System Manager management node (IBM FSM) that is connected to the Internet, follow the procedures listed in Chapter 2, "Updating firmware from an IBM FSM that is connected to the Internet," on page 13.
   - If you are updating chassis components through an IBM FSM that is not connected to the Internet, follow the procedures listed in Chapter 3, "Updating firmware from an FSM that is not connected to the Internet," on page 63.
   - If you are updating chassis components but you do not have an IBM FSM installed in your environment, follow the procedures listed in Chapter 4, "Updating all components in a chassis when an IBM FSM is not present," on page 121.
2. Update the IBM Storwize V7000 if it is installed in your environment. See Chapter 5, "Updating the IBM Storwize V7000," on page 133.
3. Update top-of-rack (TOR) switches if they are installed in your environment. See Chapter 6, "Updating Top-of-Rack (TOR) switches," on page 135.

If you have issues during the update process, see Chapter 7, "Troubleshooting update issues," on page 137 to resolve those issues.

Note: To hide an FSM status entry that is showing as active for a condition reported by the CMM, use the "Ignore" action on the IBM FSM from the Problems/Active Status view. If the status entry is deleted (i.e., rather than ignored) on the IBM FSM and the condition remains active on the CMM, the next resynchronization with the CMM will cause the status entry to be reasserted on the IBM FSM.

1.1 Upgrading from an earlier version of Flex System firmware

Depending on the release of Flex System firmware that is currently installed, you might need to perform multiple firmware upgrades to get to the latest version of firmware if you are upgrading firmware through the IBM FSM.

The following table shows the upgrade path that you must follow if you are upgrading firmware for a system through the IBM FSM, depending on the version of Flex System firmware and IBM FSM that is currently installed in your environment.

Table 1. Upgrade path depending on the level of IBM FSM that is currently installed

If you are using:	Interim upgrade steps (must follow the steps in)	Final upgrade step
IBM FSM 1.0.0	1. IBM FSM 1.2.1. Follow the steps listed in "Upgrade all components to Flex version 1.2.1." 2. IBM FSM 1.3.0. Follow the steps listed in "Upgrade all components to Flex version 1.3.0."	IBM FSM 1.3.2
IBM FSM 1.1.0	1. IBM FSM 1.2.1. Follow the steps listed in "Upgrade all components to Flex version 1.2.1." 2. IBM FSM 1.3.0. Follow the steps listed in "Upgrade all components to Flex version 1.3.0."	IBM FSM 1.3.2
IBM FSM 1.2.0	IBM FSM 1.3.0. Follow the steps listed in "Upgrade all components to Flex version 1.3.0."	IBM FSM 1.3.2
IBM FSM 1.2.1	1. IBM FSM 1.3.0. Follow the steps listed in "Upgrade all components to Flex version 1.3.0." 2. IBM FSM 1.3.2. Follow the steps listed in “Upgrade all components to Flex version 1.3.2.”	IBM FSM 1.3.3
IBM FSM 1.3.0	IBM FSM 1.3.2. Follow the steps listed in “Upgrade all components to Flex version 1.3.2.”	IBM FSM 1.3.3
IBM FSM 1.3.1	IBM FSM 1.3.2	IBM FSM 1.3.3
IBM FSM 1.3.2		IBM FSM 1.3.3

For example, if you are upgrading from Flex version 1.2.0 to Flex version 1.3.3 and you are using an IBM FSM, you **must** follow a three-step process:

1. Upgrade all components to Flex version 1.3.0.
2. Upgrade all components to Flex version 1.3.2.
3. Upgrade all components to Flex version 1.3.3.

Upgrade all components to Flex version 1.2.1

To upgrade to Flex version 1.2.1, you will need to upgrade using the following document:

IBM Flex System Updating Best Practice, version 1.2.1 and earlier

This document is available at the following website:

http://download.boulder.ibm.com/ibmdl/pub/systems/support/system_x_pdf/ibm_updating_flex_best_practice_v1.2.1.pdf

Important Consideration:

Specifically, you must follow the procedures described in Section 2.5, "Updating when the IBM FSM is not connected to the Internet" of that document, **even if** the IBM FSM that you are using is connected to the Internet.

If you attempt to download updates as described in Section 2.5.1, "Obtaining all updates," of that document, you will be directed to download the latest updates (version 1.3.1). Therefore, complete the following steps to obtain all updates:

1. Point your browser to the following website:
   http://www.ibm.com/software/brandcatalog/puresystems/centre/
2. Click the **System Updates** tab.
3. Click the **Flex System 1.2.1** tab.
4. Download the updates using the instructions that begin in section 2.5.1.1, "Downloading the IBM FSM updates" of *IBM Flex System Updating Best Practice, version 1.2.1 and earlier*.
5. Use the instructions beginning in section 2.5.2, "Updating the IBM FSM" of *IBM Flex System Updating Best Practice, version 1.2.1 and earlier* to install and activate updates.

Upgrade all components to Flex version 1.3.0

To upgrade to Flex version 1.3.0, you will need to upgrade using the following document:

IBM Flex System Updating Best Practice, version 1.3.0 and earlier

This document is available at the following website:

http://download.boulder.ibm.com/ibmdl/pub/systems/support/system_x_pdf/
ibm_updating_flex_best_practice_v1.3.0.pdf

Important Consideration:

Specifically, you must follow the procedures described in Section 3.5, "Updating when the IBM FSM is not connected to the Internet" of that document, **even if** the IBM FSM that you are using is connected to the Internet.

If you attempt to download updates as described in Section 3.5.1, "Obtaining all updates," of that document, you will be directed to download the latest updates (version 1.3.1). Therefore, complete the following steps to obtain all updates:

1. Point your browser to the following website:
   http://www.ibm.com/software/brandcatalog/puresystems/centre/
2. Click the **System Updates** tab.
3. Click the **Flex System 1.3.0** tab.
4. Download the updates using the instructions that begin in section 3.5.1.1, "Downloading the IBM FSM updates" of *IBM Flex System Updating Best Practice, version 1.3.0 and earlier*.
5. Use the instructions beginning in section 3.5.2, "Updating the IBM FSM" of *IBM Flex System Updating Best Practice, version 1.3.0 and earlier* to install and activate updates.

Upgrade all components to Flex version 1.3.2

To upgrade to Flex version 1.3.2, you need to upgrade by using the following document:

IBM Flex System Updating Best Practice, version 1.3.2 and earlier

This document is available at the following website:

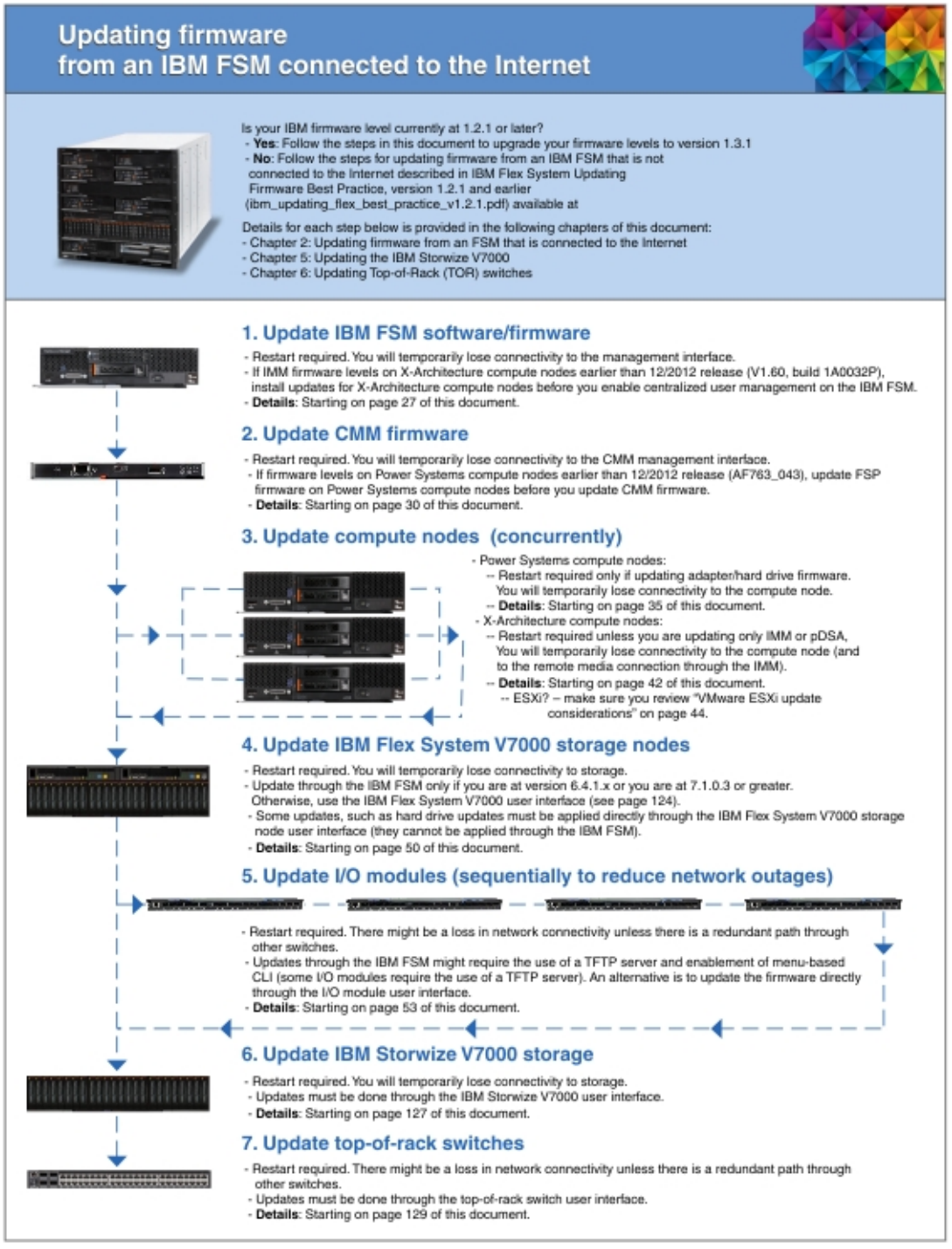
http://download.boulder.ibm.com/ibmdl/pub/systems/support/system_x_pdf/ibm_updating_flex_best_practice_v1.3.2.pdf

Upgrade all components to Flex version 1.3.3

After you have successfully upgraded to Flex version 1.3.2, you can use procedures in this document to upgrade to Flex version 1.3.3.

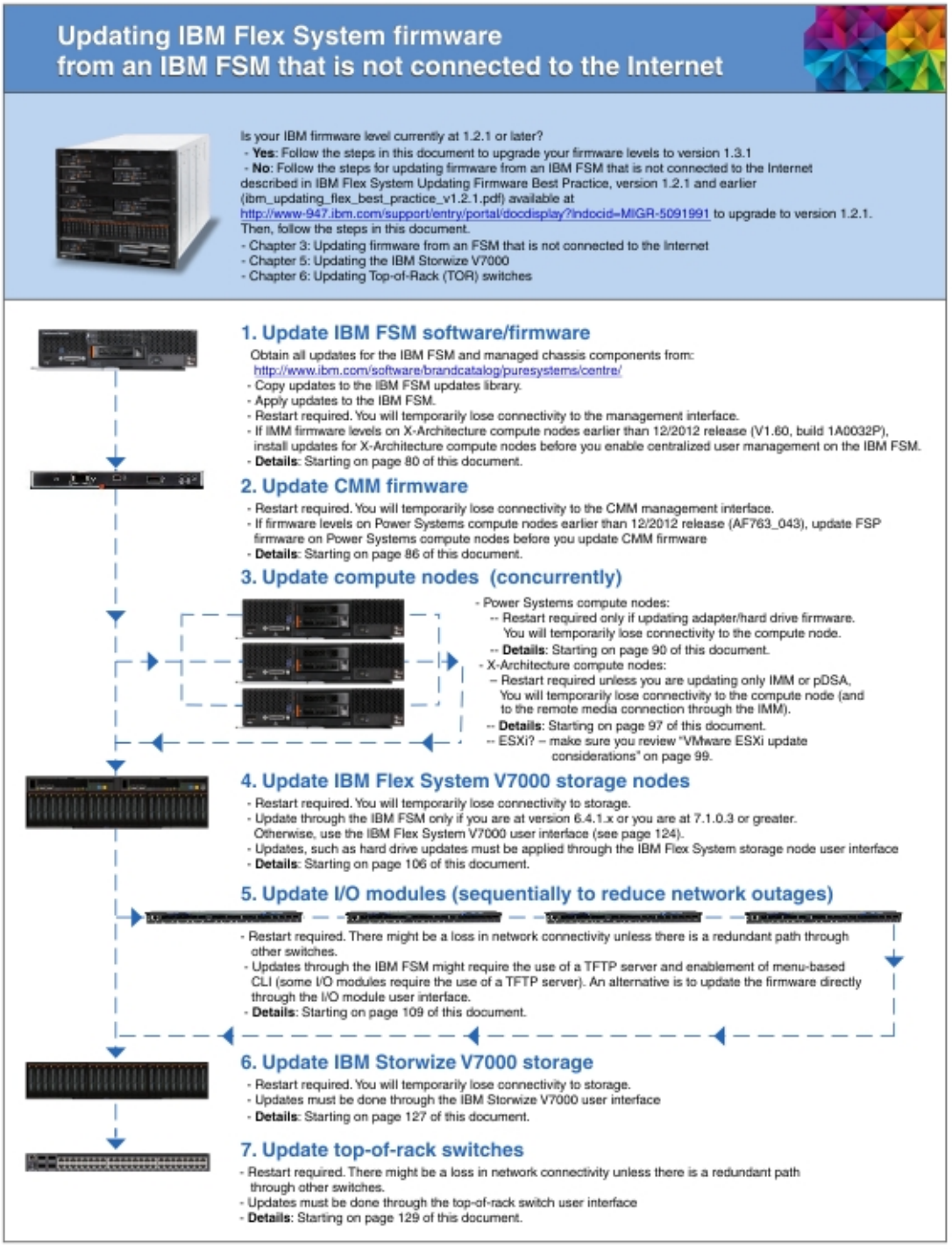
1.2 Upgrading firmware through an IBM FSM connected to the Internet

This flow diagram explains the steps that are required to update firmware through an IBM FSM that is connected to the Internet.



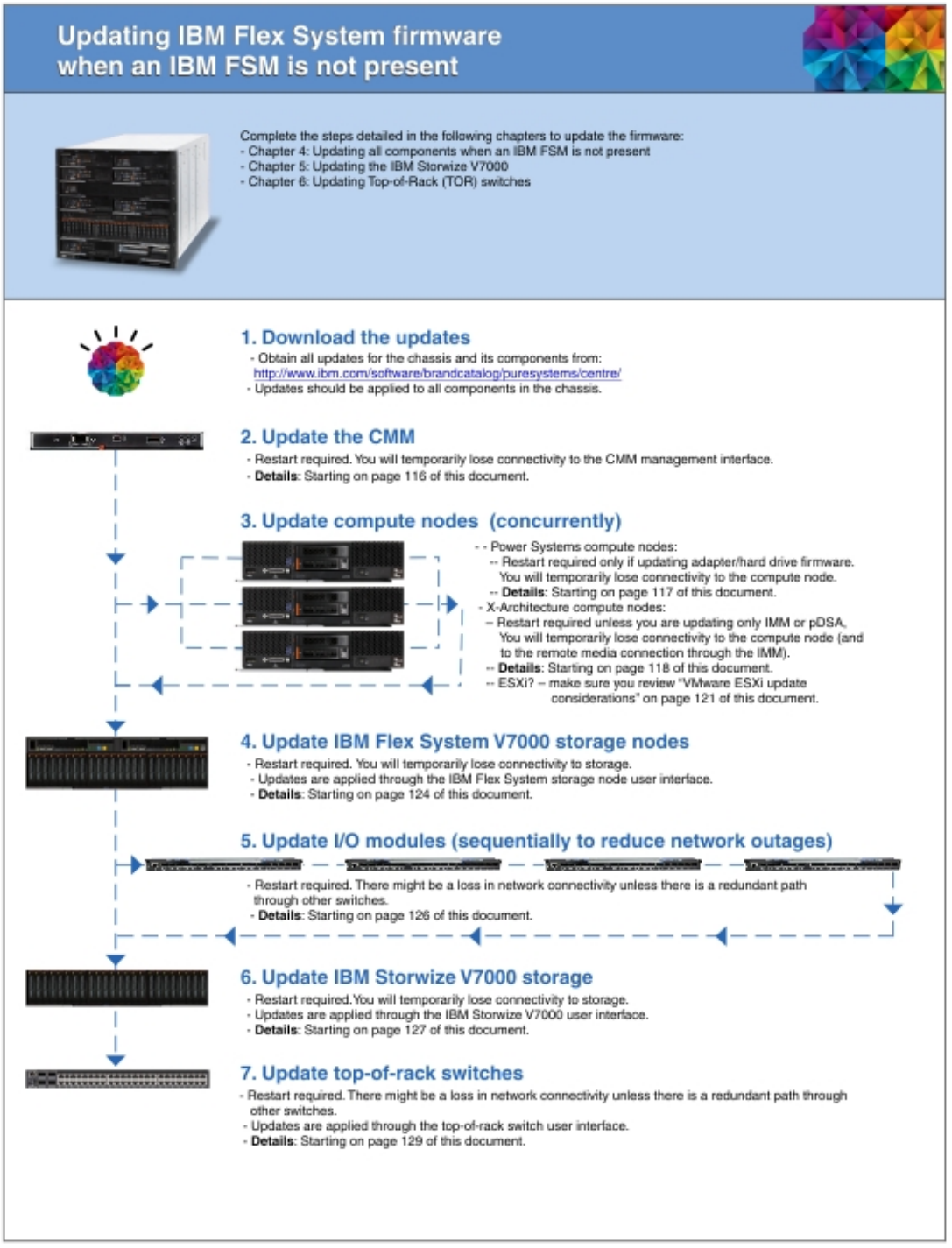
1.3 Upgrading firmware through an IBM FSM that is not connected to the Internet

This flow diagram explains the steps that are required to update firmware through an IBM FSM that is not connected to the Internet.



1.4 Upgrading firmware when an IBM FSM is not present

This flow diagram explains the steps that are required to update firmware for devices in an IBM Flex System chassis when an IBM FSM is not present.



1.5 How much time does an update take?

Use this table to determine approximately how much time it will take to update your system to version 1.3.3.

The total amount of time required to perform an update to your system will depend on the number of devices to be updated (a single chassis takes less time than multiple chassis) and the configuration of the system (in virtualized environments, you must move workloads around before performing updates).

The following table provides an estimated time to perform an update, which includes:

- Acquiring the update for a device.
- Applying the update to the device.
- Restarting the device to activate the update.

Table 2. Estimate amount of time required to update devices in the IBM Flex and IBM PureFlex systems

Device	Estimated Time for Update	Restart required?
IBM Flex System Manager (IBM FSM)	2 hours	Yes
Chassis Management Module (CMM)	30 minutes	Yes
X-Architecture compute node **Note:** The amount of time required for an update depends on the operating system that is installed. For example, if you have VMware installed, you will need to take into consideration the amount of time required to move VMs off the compute node before the update and back on to the compute node after the update.	1.5 - 3.0 hours	Yes
Power Systems compute node **Note:** The amount of time required for an update depends on the amount of time required to move VMs off the compute node before the update and back on to the compute node after the update.	1 hour	Yes
IBM Flex System V7000 storage node	1 hour	Yes
I/O modules	1 hour	Yes
IBM Storwize V7000	1 hour	Yes
Top-of-rack switches	1 hour	Yes

1.6 Minimizing downtime during firmware updates

You can minimize the disruptions caused by restarting devices to activate firmware updates. In some cases, you can apply the updates, but wait until later to actually activate them.

Important consideration:

Firmware updates for IBM Flex System and IBM PureFlex components are tested and released together. Therefore, you must update all components in a chassis to the same software level, as defined at the IBM PureSystems Centre website. In particular the management software components might have some interdependencies. Therefore, it is important to make sure that all management software components (IBM FSM, CMM, IMM on X-Architecture compute nodes, FSP on Power Systems compute nodes, and the IBM Flex System V7000 storage node) are updated to the same software level.

Follow these steps to update the firmware while minimizing disruptions to running workloads and applications:

1. Update the firmware and software for the IBM FSM and restart the IBM FSM server to activate the changes. Make sure that you restart the server itself, not just the IBM FSM software.

   Restarting the IBM FSM does not affect running workloads or applications on the compute nodes.
2. Update the firmware for the Chassis Management Module (CMM) and restart the CMM to activate the changes.

   Note: When you update the CMM through the IBM FSM, the default is to **Automatically restart as needed during installation**. Use the default.

   Restarting the CMM to activate firmware updates will temporarily interrupt the management network. However, it does not affect running workloads or applications on the compute nodes.
3. Update the firmware for the X-Architecture compute nodes, but make sure that you do not select **Automatically restart as needed during installation**. The firmware update will be applied but it will not be activated.

   Tip: If the compute nodes are set up in a virtualized environment, consider moving workloads while updating firmware. Before updating firmware for a compute node that is running ESXi, make sure that you enable maintenance mode. For information about enabling maintenance mode, see the documentation that is provided with ESXi.

   Note: Remember that if you do not select **Automatically restart as needed during installation** when updating the firmware through the IBM FSM, you will receive an error in the job log reminding you that you need to restart the compute node for the changes to take affect.

   When you apply the firmware update, the IMM is automatically reset which causes the IMM update to be activated. However, the other updates will not be activated until the compute node is actually restarted. Therefore, you can restart them during a maintenance window (or move workloads and applications between compute nodes and restart them sequentially to have all updates applied).

   Note: When you apply firmware and driver updates to network adapters installed in a compute node, a port might be temporarily closed and reopened. Depending on your application, this might cause a disruption to your workload.
4. Update the firmware for the FSP on Power Systems compute nodes. When you update the FSP firmware, the compute node does not need to be restarted for activation unless you are updating across firmware release boundaries.

   Tip: If the compute nodes are set up in a virtualized environment, consider moving workloads while updating firmware. Before updating firmware for a compute node that is running PowerVM, make sure that you enable maintenance mode. For information about enabling maintenance mode, see the documentation that is provided with PowerVM.

For all other updates to the firmware for Power Systems compute nodes, you can apply the updates and then activate them at a later time by restarting the compute node.

Note: When you apply firmware and driver updates to network adapters installed in a compute node, a port might be temporarily closed and reopened. Depending on your application, this might cause a disruption to your workload.

5. Update the IBM Flex System V7000 storage node, selecting to **Automatically restart as needed during installation**.
6. Assuming that all I/O modules are configured for redundant network paths, update each I/O module sequentially to ensure that you do not lose network connectivity while the firmware for an I/O module is being updated.

Chapter 2. Updating firmware from an IBM FSM that is connected to the Internet

Use the IBM FSM user interface to obtain, import, and install all updates for all chassis components.

Important Considerations

- Use this document to upgrade firmware if the IBM FSM that you have installed is currently at version 1.3.0 or higher. If the IBM FSM version is earlier than 1.3.0, make sure that you review 1.1, "Upgrading from an earlier version of Flex System firmware," on page 3.
- If you did not previously follow the steps to update the IBM FSM to version 1.3.1.1 (to resolve the OpenSSL Heartbleed vulnerability), apply the updates for version 1.3.2 to the IBM FSM and all components in all managed chassis. Then, from the IBM FSM, replace the TLS certificate and private key for the IBM FSM user registry, and change passwords according to the Remediation/Fixes section of the Security Bulletin referenced below:

  http://www.ibm.com/support/entry/portal/docdisplay?lndocid=MIGR-5095202
- If the Flexible Service Process (FSP) firmware on the Power Systems compute nodes installed in your chassis is earlier than the December, 2012 release (AF763_043), you must update the FSP firmware on the Power Systems compute nodes before updating the CMM. Follow the update procedure listed in 2.1.1, "Steps to update for Power Systems compute nodes running FSP firmware versions earlier than AF763_043," on page 19.
- IBM FSM does not support updating x440 M5 (MT 7167, 2590) and x240 M5 (MT 9532, 2588) ITEs. As an alternative, you can use the UpdateXpress System Packs (UXSPs) and the UpdateXpress System Pack Installer (UXSPI) to update these ITEs as described in 4.3, "Updating X-Architecture compute nodes," on page 124.

  Note: Lenovo UXSPI supports the updating of x440 M5 (MT 7167, 2590) and x240 M5 (MT 9532, 2588) ITEs.
- IBM FSM version 1.3.3 manages both IBM and Lenovo manufactured System x and BladeCenter. Lenovo System x and BladeCenter have their own firmware updates, therefore, use Lenovo UXSPi to update both Lenovo system x and BladeCenter. Ensure that the latest version of IBM UXSPi is used to update when the target system is IBM System x or IBM BladeCenter. If the targeted systems are manufactured by Lenevo, then acquire the latest version of Lenovo UXSPi to update the systems.

  Note: Use the latest IBM UXSPi to update firmware for FSM management server.

2.1 Steps to update from an IBM FSM

Make sure that you review the steps in this table carefully before you begin updating the firmware for IBM Flex System or IBM PureFlex system components using the IBM FSM.

Important considerations:

Before you begin updating the components:

- Make sure that you verify the part number of the fan logic modules in your chassis and replace them if necessary.

  ECA083 (Engineering Change Announcement) provides for proactive replacement of the fan logic module in a limited number of IBM PureFlex systems. Details of this announcement and instructions for determining the part number of installed fan logic modules are available at the following location:

  http://www.ibm.com/support/entry/portal/docdisplay?lndocid=MIGR-5093506
- Make sure that the IBM FSM is managing the chassis, that all components are accessible from the IBM FSM, and that a full inventory has been performed for all components (including operating systems). See 2.3.1, “Making sure that the IBM FSM is managing the chassis,” on page 25.
- Perform a backup of the IBM FSM. See 2.3.2, “Backing up the IBM FSM,” on page 29.
- If you are updating firmware for Power Systems compute nodes running FSP firmware 01AF773, you must update the Flexible Service Processor (FSP) for Power Systems compute node to 01AF773_058 before you begin ghe uupdate the CMM. See 2.1.2, “Steps to update for Power Systems compute nodes running FSP firmware version 01AF773,” on page 20 for the update order to follow in this case.

The following table enumerates the high level steps with the corresponding section required to update IBM Flex System or IBM PureFlex system components using the IBM FSM. Follow the detailed instructions in each section as you update.

Table 3. High-level steps to update components.

Note: The total amount of time required to update a system depends on the number of devices in system (one chassis versus multiple chassis) and the configuration of the system (virtualized environments versus non-virtualized environments).

Step	Activity	How much time does it take?	Is a restart required?	More information
1	**Update the IBM FSM** After updating the IBM FSM, restart the IBM FSM to have the changes take effect. **Tip:** After restarting the IBM FSM, make sure that you clear the cache for your browser before accessing the IBM FSM Web interface. **Important consideration:** If the IMM firmware level on the X-Architecture compute nodes installed in your chassis is earlier than the December, 2012 release (v1.60, build 1AOO32P), install the updates for the X-Architecture compute nodes before you enable centralized user management on the IBM FSM. For more information about centralized user management through the IBM FSM, see the following website: http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/centralized_user_management.html	2 hours per IBM FSM	Yes	2.4, "Updating the IBM FSM," on page 30
2	**Update the CMM** After updating the CMM, restart the CMM to have the changes take effect. **Important consideration:** If you are updating firmware for Power Systems compute nodes running FSP firmware that is earlier than the December, 2012 release (AF763_043), you must update the Flexible Service Processor (FSP) for Power Systems compute node before you update the CMM. See 2.1.1, "Steps to update for Power Systems compute nodes running FSP firmware versions earlier than AF763_043," on page 19 for the update order to follow in this case. Updating older version FSPs after updating the CMM might leave your compute nodes unusable (in a status 'pending' condition). If this happens, see 7.9, "Power Systems compute node remains at a status pending state after an update," on page 142.	30 minutes per CMM	Yes	2.5, "Updating the CMM," on page 33

Table 3. High-level steps to update components (continued).

Note: The total amount of time required to update a system depends on the number of devices in system (one chassis versus multiple chassis) and the configuration of the system (virtualized environments versus non-virtualized environments).

Step	Activity	How much time does it take?	Is a restart required?	More information
3	**Update Power Systems compute nodes** The firmware update for a Power Systems compute node can be applied even if the operating system has not been discovered by the FSM. However, you need to discover the Power Systems operating system to update the network adapters and the hard disk drives. See 2.6.1, "Discovering operating systems from the IBM FSM," on page 37. **Important consideration:** If you are updating firmware for Power Systems compute nodes running FSP firmware that is earlier than the December, 2012 release (AF763_043), you must update the Flexible Service Processor (FSP) for Power Systems compute node before you update the CMM. See 2.1.1, "Steps to update for Power Systems compute nodes running FSP firmware versions earlier than AF763_043," on page 19 for the update order to follow in this case. Updating older version FSPs after updating the CMM might leave your compute nodes unusable (in a status 'pending' condition). If this happens, see 7.9, "Power Systems compute node remains at a status pending state after an update," on page 142.	1 hour to 3 hours per compute node **Note:** • The amount of time required for an update depends on the operating system that is installed and whether you are running in a virtualized environment (you are moving VMs between compute nodes as you perform updates). • You can perform all compute nodes updates concurrently, which will reduce the overall amount of time needed for updating the entire system.	Yes **Note:** If you are updating only the firmware for the FSP and not changing the release version, a restart is not required. A restart is required if you are updating the firmware for adapters or hard disk drives.	2.6.2, "Updating Power Systems compute nodes," on page 38

Table 3. High-level steps to update components (continued).

Note: The total amount of time required to update a system depends on the number of devices in system (one chassis versus multiple chassis) and the configuration of the system (virtualized environments versus non-virtualized environments).

Step	Activity	How much time does it take?	Is a restart required?	More information
4	**Update X-Architecture compute nodes** The operating system must be discovered by the IBM FSM before updating the firmware (see 2.6.1, "Discovering operating systems from the IBM FSM," on page 37). VMware ESXi update considerations are described in 2.6.3.1, "VMware ESXi update considerations," on page 48. After updating the compute node, you must restart it for the updates to take effect.	1.5 hours to 3.5 hours per compute node **Note:** • The amount of time required for an update depends on the operating system that is installed and whether you are running in a virtualized environment (you are moving VMs between compute nodes as you perform updates). • You can perform all compute nodes updates concurrently, which will reduce the overall amount of time needed for updating the entire system.	Yes **Note:** If you are updating only the IMM and pDSA firmware for the X-Architecture compute node, you do not need to restart the compute node to apply the updates.	2.6.3, "Updating X-Architecture compute nodes," on page 46
5	**Update IBM Flex System V7000 storage nodes** Some updates, such as hard disk drive updates cannot be applied through the IBM FSM. See 2.7.2, "Obtaining additional updates for the IBM Flex System V7000 storage node," on page 56. After updating the storage node, you must restart it for the updates to take effect.	1 hour	Yes	2.7, "Updating storage nodes," on page 55

Table 3. High-level steps to update components (continued).

Note: The total amount of time required to update a system depends on the number of devices in system (one chassis versus multiple chassis) and the configuration of the system (virtualized environments versus non-virtualized environments).

Step	Activity	How much time does it take?	Is a restart required?	More information
6	**Update I/O modules** Make sure that you update I/O modules sequentially, restarting each I/O module and ensuring that it is functioning before updating the next I/O module. If you are updating the firmware for the Flex System CN4093 10Gb Converged Scalable Switch, the Flex System Fabric EN4093/EN4093R 10Gb Scalable Switches, or the Flex System EN2092 1Gb Ethernet Scalable Switch, check the firmware level before updating. If the firmware level currently installed on the I/O module is less than version 7.7.5.0, you must use a Trivial File Transfer Protocol (TFTP) server to host updates before they are applied to these switches. **Tip:** To update a single I/O module, consider updating it directly through the Web interface for the I/O module.	1 hour	Yes	2.8, "Updating I/O modules," on page 57
7	**Update IBM Storwize V7000 devices** Firmware updates to the IBM Storwize V7000 must be done through the IBM Storwize V7000 interface.	1 hour	Yes	Chapter 5, "Updating the IBM Storwize V7000," on page 133
8	**Update top-of-rack switches** Firmware updates to top-of-rack switches must be done through directly through the switch interface.	1 hour	Yes	Chapter 6, "Updating Top-of-Rack (TOR) switches," on page 135

If you have issues during the update process, see Chapter 7, "Troubleshooting update issues," on page 137 to resolve those issues.

2.1.1 Steps to update for Power Systems compute nodes running FSP firmware versions earlier than AF763_043

If the Flexible Service Process (FSP) firmware on the Power Systems compute nodes installed in your chassis is earlier than the December, 2012 release (AF763_043), you must update the FSP firmware on the Power Systems compute nodes before updating the CMM.

Note: Updates can be applied to an active, running system. However, typically the system needs to be restarted for updates to take effect.

Updates must be applied in the following order:

1. IBM Flex System Manager (FSM)

   Important consideration:

   Before updating the IBM FSM management node, create a backup image of the IBM FSM. For information about backing up the IBM FSM, see 2.3.2, "Backing up the IBM FSM," on page 29.
2. Service processor on each Power Systems compute node that is currently running firmware version earlier than AF763_043

   You must update the firmware for the Flexible Service Processor (FSP) ***before*** you update the firmware for the CMM. The updates for the adapters and hard drives installed in a Power Systems compute node can be installed later in the update process.

   Updating older version FSPs after updating the CMM might leave your compute nodes unusable (in a status 'pending' condition). If this happens, see 7.9, "Power Systems compute node remains at a status pending state after an update," on page 142.
3. Chassis Management Module (CMM)
4. Network adapters and hard drives for the Power Systems compute nodes
5. X-Architecture compute nodes

   If the IMM firmware level on the X-Architecture compute nodes installed in your chassis is earlier than the December, 2012 release (v1.60, build 1AOO32P), install the updates for the X-Architecture compute nodes before you enable centralized user management on the IBM FSM.

   For more information about centralized user management through the IBM FSM, see the following website:

   http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/centralized_user_management.html
6. IBM Flex System V7000 Storage Node
7. I/O modules

Depending on your configuration, you might also need to update the following components. These components must be updated directly; you cannot update them through the IBM FSM.

1. IBM Storwize V7000
2. Top-of-rack switches

2.1.2 Steps to update for Power Systems compute nodes running FSP firmware version 01AF773

If the Flexible Service Process (FSP) firmware on the Power Systems compute nodes installed in your chassis is version 01AF773, you must update the FSP firmware on the Power Systems compute nodes to 01AF773_058 before updating to 01AF783 (Flex Version 1.3.2).

Note: Updates can be applied to an active, running system. However, typically the system needs to be restarted for updates to take effect.

Updates must be applied in the following order:

1. Power Systems Flexible Service Processor (FSP) firmware. Update the FSP firmware to level 01AF773_058.
2. IBM Flex System Manager (FSM)

   Important consideration:

   Before updating the IBM FSM management node, create a backup image of the IBM FSM. For information about backing up the IBM FSM, see 2.3.2, “Backing up the IBM FSM,” on page 29.
3. Chassis Management Module (CMM)
4. Update the Power Systems firmware to 01AF783

   You must update the firmware for the Flexible Service Processor (FSP) ***before*** you update the firmware for the CMM. The updates for the adapters and hard drives installed in a Power Systems compute node can be installed later in the update process.

   Updating older version FSPs after updating the CMM might leave your compute nodes unusable (in a status 'pending' condition). If this happens, see 7.9, “Power Systems compute node remains at a status pending state after an update,” on page 142.
5. Network adapters and hard drives for the Power Systems compute nodes
6. X-Architecture compute nodes

   If the IMM firmware level on the X-Architecture compute nodes installed in your chassis is earlier than the December, 2012 release (v1.60, build 1AOO32P), install the updates for the X-Architecture compute nodes before you enable centralized user management on the IBM FSM.

   For more information about centralized user management through the IBM FSM, see the following website:

   http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/centralized_user_management.html
7. IBM Flex System V7000 Storage Node
8. I/O modules

Depending on your configuration, you might also need to update the following components. These components must be updated directly; you cannot update them through the IBM FSM.

1. IBM Storwize V7000
2. Top-of-rack switches

2.2 Prerequisites

Review the prerequisites before updating components in a chassis through the IBM FSM.

The following prerequisites must be met to update the components in a chassis through the IBM FSM:

- To update chassis components, the chassis and all components within the chassis must be managed by the IBM FSM. For information about managing components through the IBM FSM, see the following website:

  http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/managing_chassis.html

- If Platform Agent is installed on compute nodes, you must update the Platform Agent on each compute node before you update the firmware for that compute node.

  Note: If you installed Common Agent, you do not need to update the Common Agent before you update the firmware for the compute node.

  To obtain the Platform Agent for the operating system that is installed on the compute node and to add it to the IBM FSM updates library, see 3.4.1, "Downloading the IBM FSM updates," on page 81. Use the procedures described in the Readme for the Platform Agent update to update the Platform Agent for compute nodes.

- At a minimum, you must apply VMware vSphere ESXi 5.0.x/5.1.x/5.5.x with IBM Customization Patch 1.2 or later for each compute node running the IBM customized image.

  If you are running VMware vSphere ESXi 5.5.x (update 1) or earlier, you must apply both the Lenovo and the Independent Hardware Vendor (IHV) customization patches (Patch 1.2) on every compute node. If you are running VMware vSphere ESXi 5.5.x (update 2), you need not apply Patch 1.2.

  In addition to the IBM Customization Patch 1.2, make sure that you install one of the following updates to the VMware vSphere ESXi operating system:

  – If you are running VMware vSphere ESXi 5.0, make sure that you install update 5.0u2 (update 2)
  – If you are running VMware vSphere ESXi 5.1, make sure that you install update 5.1u1 (update 1)
  – VMware vSphere ESXi 5.5.x

  When you install an IMM update on an X-Architecture compute node, the Integrated Management Module (IMM) is reset, which can cause a VMware vSphere ESXi system failure (host purple diagnostic screen) if you attempt to update an X-Architecture compute node on which the minimum level of VMware is not installed (5.0u2, 5.1u1, or 5.5.x).

  For information about obtaining the IBM Customization Patch 1.2, see the following location:

  http://www.ibm.com/support/entry/portal/docdisplay?lndocid=MIGR-5092679

  Make sure that you review the information provided in the readme for the patch. It contains instructions for installing the patch on a compute node.

- Make sure that SCP is installed on the Power Systems compute nodes before running Discovery or Inventory Collection from the IBM FSM so that the network adapters are discovered and inventoried by the IBM FSM. For more information about installing SCP, which is available with the OpenSSH software tools, see the following website:

  http://pic.dhe.ibm.com/infocenter/aix/v7r1/topic/com.ibm.aix.security/doc/security/openssh_kerberosv5.htm

- Compute nodes must have an operating system installed. The operating system must have a network IP address and the operating system must have been discovered by the IBM FSM. For information about installing operating systems on X-Architecture compute nodes, see the following websites:

  – Using the Deploy Images task from the IBM FSM:

    http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/deploying_compute_node_images.html

  – Quick Start Guides:

http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.commontasks.doc/commontasks_install_os.html

– Update considerations regarding a specific operating system, such as the requirement for 32-bit compatibility libraries when running the 64-bit Linux operating system:

  http://pic.dhe.ibm.com/infocenter/flexsys/information/index.jsp?topic=%2Fcom.ibm.acc.8731.doc%2Fcom.ibm.director.updates.helps.doc%2Ffqm0_c_um_platform_extensions.html

Note: The firmware update for a Power Systems compute node can be applied even if the operating system has not been discovered by the IBM FSM. However, you need to discover the Power Systems operating system to update the network adapters and the hard disk drives.

- The IBM FSM must have full access to any component that is being updated, including discovered operating systems.

  Note: If you are updating X-Architecture compute nodes running Microsoft Windows 2012, see 2.2.1, "Enabling Windows Server 2012 systems for discovery," on page 23.

- The IBM FSM must perform at least one inventory collection on the component being managed. For information about collecting inventory, see the following website:

  http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/com.ibm.director.discovery.helps.doc/fqm0_t_performing_system_discovery.html

- The LAN-over-USB interface must be enabled for firmware updates on all X-Architecture compute nodes and for the IBM FSM.

  You can check that this is enabled by connecting to the CMM Web interface. Then:

  1. Navigate to **Chassis Management** > **Compute Nodes** to see a list of all compute nodes currently managed by the CMM.
  2. For ***each*** compute node:
     a. Click the compute node.
     b. Select the General tab.
     c. Make sure that **Enable Ethernet Over USB** is checked.

  Note: The LAN-over-USB interface should not be disabled on the IBM FSM but if it is, you must log in to the IMM user interface for the IBM FSM to check the setting and to change it. You cannot change the LAN-over-USB interface for the IBM FSM through the CMM interface. To check the LAN-over-USB setting for the IBM FSM, complete the following steps:

  1. Log in to the IMM Web interface for the IBM FSM.
  2. Select **IMM Management** > **Network**.
  3. From the USB tab, make sure that **Enable Ethernet over USB** is selected.

  In your operating system, you should also see a USB Ethernet interface. For more information about setting the LAN-over-USB interface through the operating system, see the following website (the procedure is the same for all X-Architecture compute nodes):

  http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.7917.doc/configuring_lan_over_usb_manually.html

  Tip: You do not need to configure a valid IP address to that interface for the update process to work.

  For more information about the IMM and LAN over USB, see the *IMMv2 User's Guide*, which is available at the following website:

  http://www.ibm.com/support/entry/portal/docdisplay?lndocid=MIGR-5086346

For more information about the IBM FSM, see the following website:

http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/getting_started.html

2.2.1 Enabling Windows Server 2012 systems for discovery

Remote registry administration must be enabled for the IBM FSM system discovery to run commands and run scripts on the managed system. The default setting for remote registry administration on Windows systems is enabled.

Procedure

Complete the following steps to verify or change the remote registry administration setting for ***each*** system that is running Windows Server 2012:

1. Log in to the Windows server.
2. Click the Server Manager icon.
3. Make sure that Windows Server 2012 can be discovered as a Windows Distributed Component Object Model (DCOM) protocol access end point by the IBM FSM:
   a. Click **Server Manager** > **Tools** > **Local Security Policy** > **Local Policies** > **Security options** > **Network access: Shares that can be accessed anonymously**.
   b. Right-click **Network access: Shares that can be accessed anonymously** and select **Properties**.
   c. In the **Network access: Shares that can be accessed anonymously** properties window, specify **Enabled** in the properties field.
4. Click **Tools** > **Services**.
5. In the list of services in the Services window, right-click the **Remote Registry** service and select **Properties** from the menu.
6. On the General page, set the Startup type to **Automatic**.
7. If the Service status is not started, click **Start** to start the service.
8. Click **OK** to apply the new settings and close the window.

   Refer to the following website for more information:

   http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/com.ibm.director.install.helps.doc/fqm0_t_preparing_windows_server_2012_managed_systems.html

   For considerations related to the discovery of other Microsoft Windows operating systems, see the following website:

   http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/com.ibm.director.install.helps.doc/fqm0_t_preparing_windows_managed_systems.html

2.2.2 Updating Linux firmware and drivers

If you are updating firmware and drivers for compute nodes that have Linux installed, make sure that you meet the prerequisites.

Firmware prerequisites

When updating firmware, the following prerequisites are required:

- If you are running a 64-bit version of Linux, make sure that the 32-bit compatibility libraries are installed (i.e. 32 bit libstdc++.so). For example, on RHEL 6, this is libstdc++-4.4.4.13.el6.i686.rpm.
- Updates require the Ncurses library (i.e. libncurses.so). For example, on RHEL 6, this is ncurses-libs-5.7-3.20090208.el6.i686.rpm.
- Make sure that the following commands are installed on each compute node that will receive the update (depending on the version of Linux that is installed):
  - zip
  - gunzip
  - rug (for SUSE Linux Enterprise Server 10 with the service pack)
  - zypper (for SUSE Linux Enterprise Server 11)
  - yum (for Red Hat Enterprise Linux versions 5.x and 6.x)

Driver prerequisites

Additionally, the following packages are required for installing Linux drivers from IBM update packages:

- /bin/sh
- /usr/bin/perl
- bash
- perl
- perl(Cwd)
- perl(Getopt::Long)
- perl(Getopt::Std)
- perl(strict)
- rpm-build
- rpm-libs
- rpmlib(CompressedFileNames) - must be version 3.0.4-1 or earlier
- rpmlib(PayloadFilesHavePrefix) - must be version 4.0-1 or earlier

2.3 Preparing for updates

Before updating the IBM FSM and all chassis components, make sure that the IBM FSM is managing the chassis, that all chassis components have been discovered and inventoried, and that the IBM FSM is backed up.

2.3.1 Making sure that the IBM FSM is managing the chassis

If you have not already set up the IBM FSM to manage your chassis, complete the following steps to manage a chassis, discover the operating systems for all compute nodes, and gain full access to all resources being managed by the IBM FSM (also known as managed endpoints).

Before you begin

Remember that a chassis can be managed by only one IBM FSM at a time. Attempting to manage a chassis from multiple IBM FSM management nodes is not supported.

Important: Flex System x222 compute node provides two separate compute nodes, upper and lower, in a single node bay. However, you will not be able to discover and manage both compute nodes until you have updated the software and firmware for the IBM FSM and CMM to Flex version 1.3.0 or later.

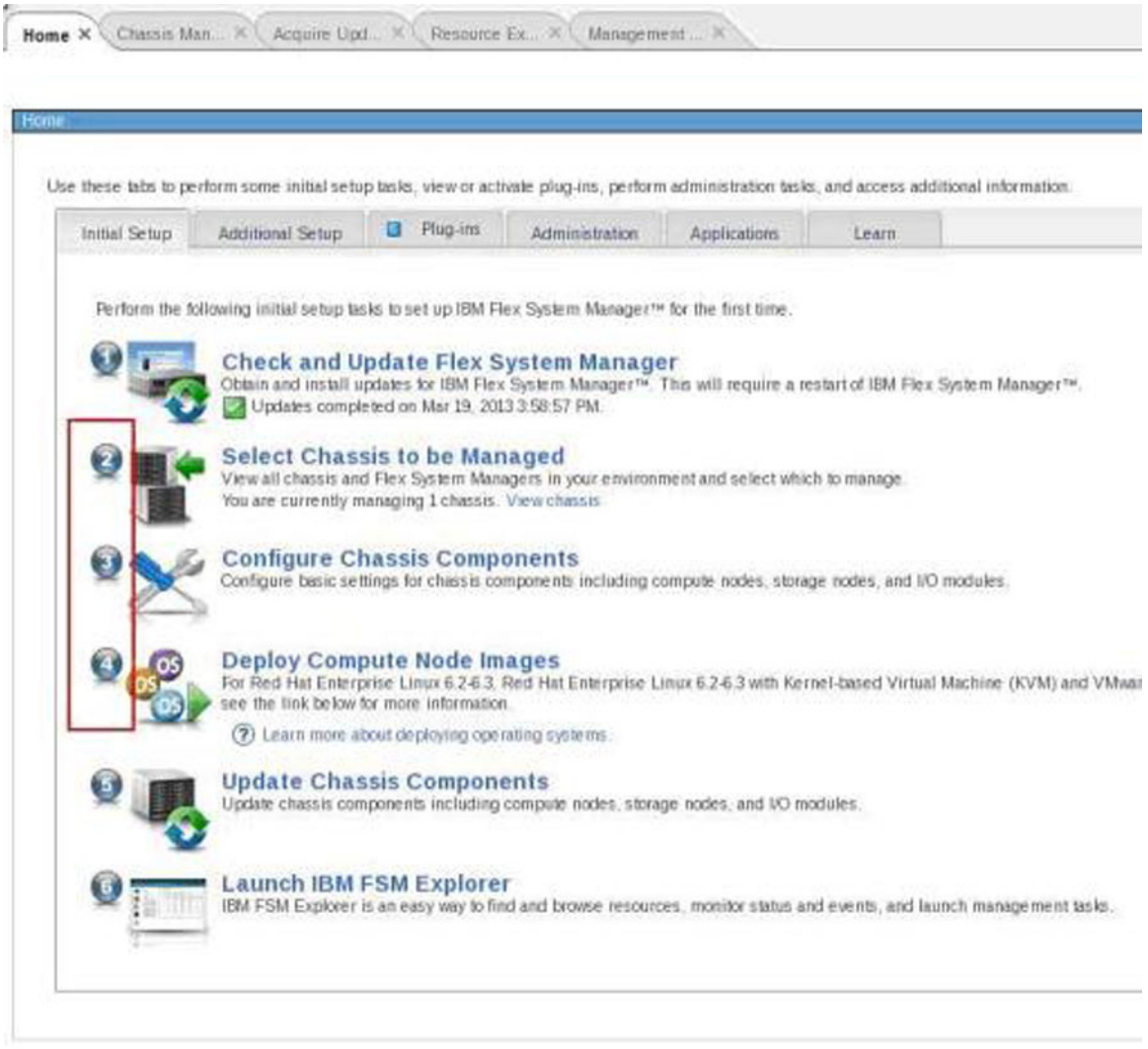
Tip: If you do not know the IP address of the operating system on an X-Architecture compute node, you can determine it by selecting the compute node from the **Chassis Manager**. Then select the common action **Remote Access** > **Remote Control** to start a remote login session to the operating system and determine the IP address.

Procedure

1. From the Home page, select the **Initial Setup** tab.
2. Follow Steps 2, 3, and 4 on the Initial Setup tab.

   Do not perform 

. You will perform that step in 2.4, “Updating the IBM FSM,” on page 30.



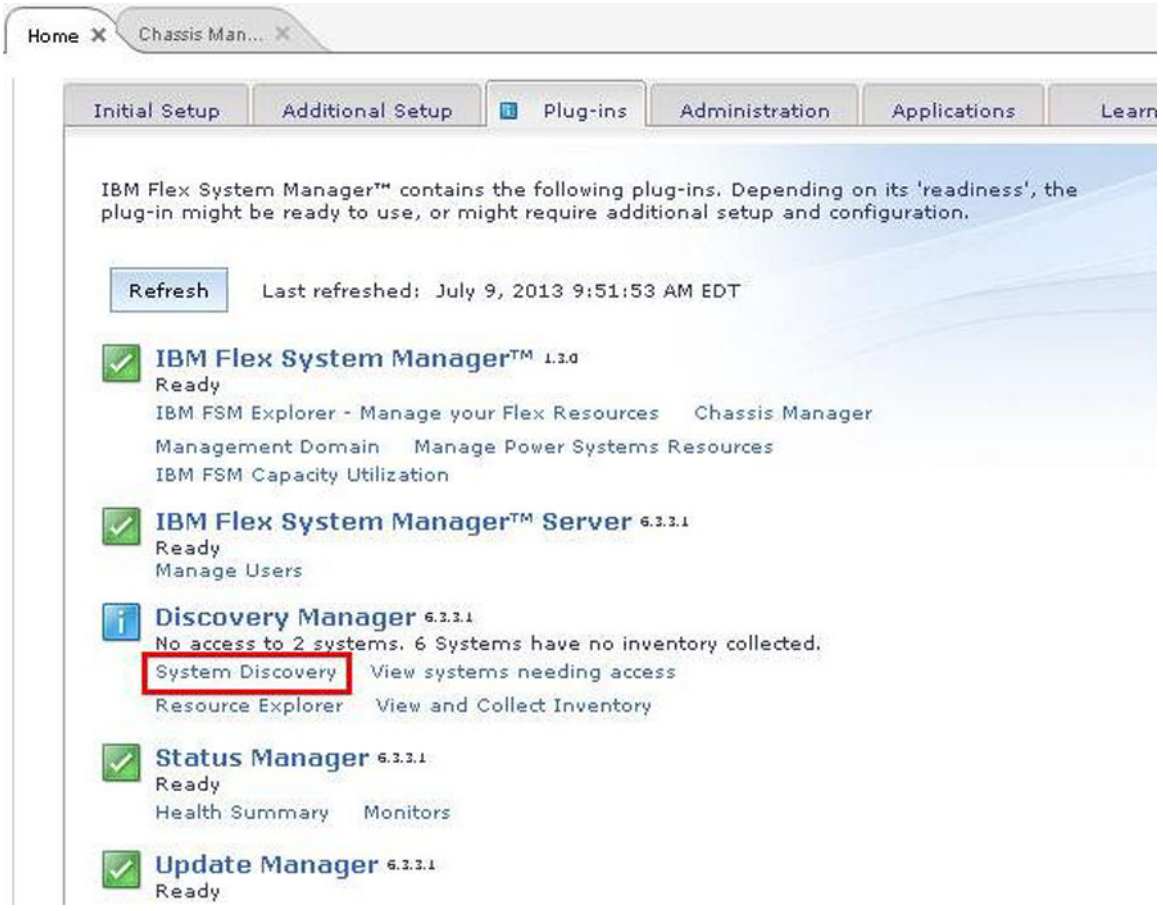
3. Discover the operating systems for all compute nodes in the chassis. It is important to discover the operating systems through the IBM FSM. Complete the following steps for each compute node on which you installed an operating system:

   Important consideration:

   Make sure that SCP is installed on the Power Systems compute nodes before running Discovery or Inventory Collection from the FSM so that the network adapters are discovered and inventoried by the FSM. For more information about installing SCP, which is available with the OpenSSH software tools, see the following website:

   http://pic.dhe.ibm.com/infocenter/aix/v7r1/topic/com.ibm.aix.security/doc/security/openssh_kerberosv5.htm

a. From the Plugins tab, locate the heading for Discovery Manager and click **System Discovery**.



b. From the System Discovery wizard, select a discovery option, such as **Single IPv4 address**.

   Tip: Rather than type in a single address, you can choose to discover a range of IP addresses, which will make the discovery process easier.

c. Enter the IP address of the operating system.

d. For the field Select the resource type to discover, select **Operating System**.

e. Click **Discover Now**. Discovering systems is a job task. For more information about job tasks within the IBM FSM, see A.1, “Starting a job task,” on page 155.

For more information about discovering operating systems through the IBM FSM, see the following website:

http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/com.ibm.director.discovery.helps.doc/fqm0_t_performing_system_discovery.html

4. Make sure that you have access to all compute nodes and that the compute nodes are unlocked. From the Chassis Manager, you can verify that you have access to all compute nodes. If not, use the information provided at the following website to request access from the IBM FSM:

   http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/com.ibm.director.security.helps.doc/fqm0_t_requesting_access_to_a_secured_system.html

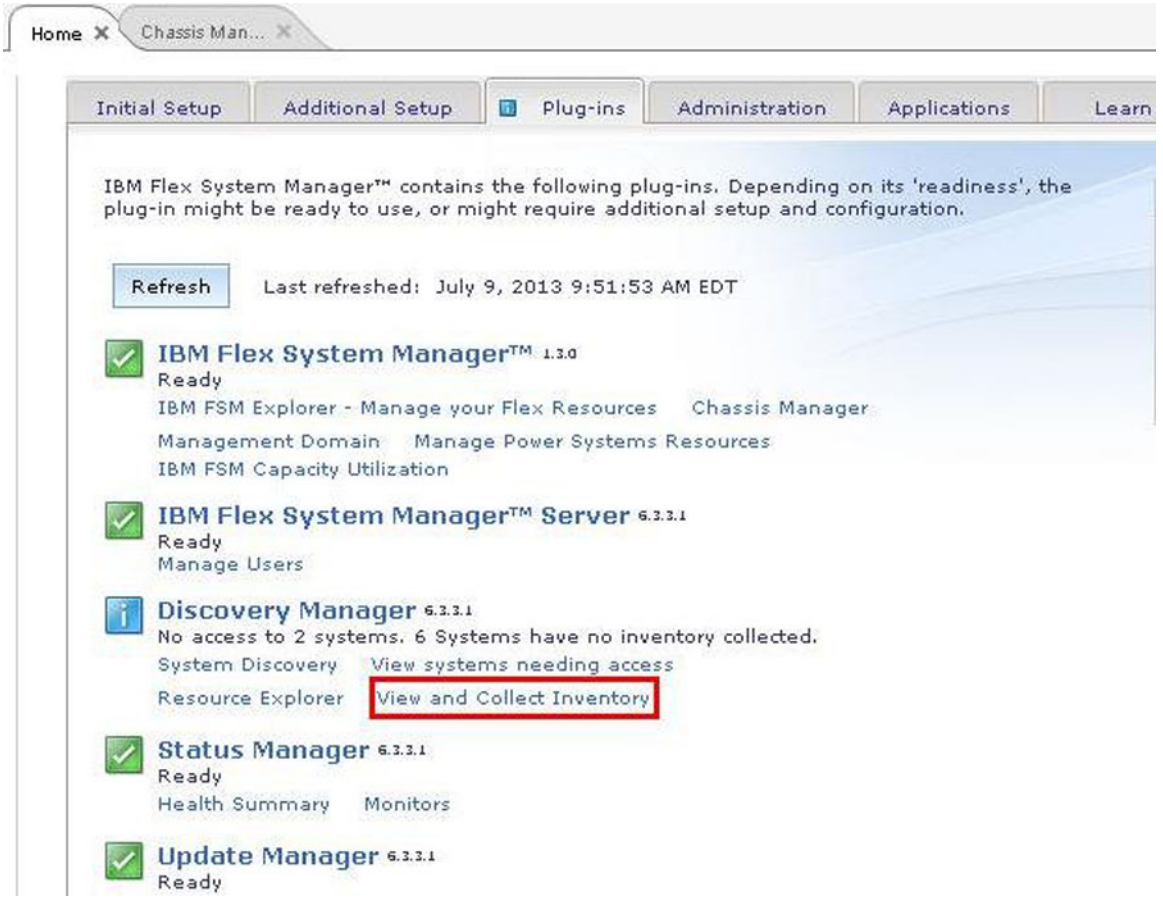
5. After all components, including the operating systems, have been discovered, perform a full inventory for all components in the chassis. Complete the following steps to discover all components, including operating systems:

   Important considerations:

   - Even if you are currently managing the chassis through the IBM FSM, you must still do a full inventory of the components (including operating systems) in the chassis before updating components.
   - Make sure that SCP is installed on the Power Systems compute nodes before running Discovery or Inventory Collection from the FSM so that the network adapters are discovered and inventoried by the FSM. For more information about installing SCP, which is available with the OpenSSH software tools, see the following website:

     http://pic.dhe.ibm.com/infocenter/aix/v7r1/topic/com.ibm.aix.security/doc/security/openssh_kerberosv5.htm

   a. From the Plugins tab, locate the heading for Discovery Manager and click **View and Collect Inventory**.



   b. Under Target Systems, click **Browse**.
   c. When the list is displayed, click **Actions** > **Select All**.
   d. Click **Add** to add the systems to the selected area.
   e. Click **OK**.
   f. On the summary page, click **Collect Inventory**.

g. Select **Run Now** and click **OK**.

Tip: Collecting inventory is a job task. If you are not familiar with job tasks in the IBM FSM, see A.1, “Starting a job task,” on page 155.

For more information about collecting inventory on components in a chassis, see the following website:

http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/com.ibm.director.discovery.helps.doc/fqm0_t_collecting_inventory.html

2.3.2 Backing up the IBM FSM

Create a backup of the IBM FSM before updating the system.

Before you begin

Make sure that the IBM FSM has network access to a secure FTP (SFTP) server. To backup the management software to an SFTP server, the destination server must have Linux with Secure Shell (SSH) enabled. Otherwise, the backup operation might fail.

Procedure

Important: Do not power off the IBM FSM management node while a backup operation is in process. Otherwise, the backup will fail.

Complete the following steps to back up the IBM FSM image to the SFTP server:

1. From the Home page, click the **Administration** tab.
2. On the Administration tab under Serviceability tasks, click **Backup and Restore** to display the Backup and Restore page.
3. From the Backup and Restore page, click **Backup Now** to display the Backup page.
4. From the Backup page, select **SFTP**.
5. Enter the location on the SFTP server where the backup file should reside (you must enter the SFTP server name as well).
6. Enter the User ID and password for the SFTP server (must have sufficient permissions to write to the server).
7. Click **OK**.

What to do next

After you have updated the IBM FSM management node, perform another backup of the system.

Additional information about backing up the IBM FSM is available at the following website:

http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/backing_up_frm.html

2.4 Updating the IBM FSM

This procedure explains how to update the IBM FSM through the IBM FSM Web interface when the IBM FSM is connected to the Internet.

Before you begin

Important considerations:

- Use this document to upgrade firmware if the IBM FSM that you have installed is currently at version 1.3.0 or higher. If the IBM FSM version is earlier than 1.3.0, make sure that you review 1.1, "Upgrading from an earlier version of Flex System firmware," on page 3.
- If you did not previously follow the steps to update the IBM FSM to version 1.3.1.1 (to resolve the OpenSSL Heartbleed vulnerability), apply the updates for version 1.3.2 to the IBM FSM and all components in all managed chassis. Then, from the IBM FSM, replace the TLS certificate and private key for the IBM FSM user registry, and change passwords according to the Remediation/Fixes section of the Security Bulletin referenced below:

  http://www.ibm.com/support/entry/portal/docdisplay?lndocid=MIGR-5095202
- Do not attempt to check for updates, import updates, and install updates (either install updates or installed needed updates) at the same time. Instead, when performing any of these tasks, make sure that the task being perform has completed before starting the next task.
- Before updating the IBM FSM management node, create a backup image of the IBM FSM. See 2.3.2, "Backing up the IBM FSM," on page 29.

Before updating the IBM FSM management node, make sure that you have completed the procedures in 2.3, "Preparing for updates," on page 25 and that you hare performed any requisite updates in 2.1, "Steps to update from an IBM FSM," on page 14 (including any steps related to Power Systems firmware updates, if required).

Make sure that you have sufficient space in the updates library on the IBM FSM before you begin. You need a minimum of 20 Gb of space available.

To increase the size of the updates library on the IBM FSM, complete the following steps:

1. From the IBM FSM Home page, select the **Plug-ins** tab, and then click **Update Manager**.
2. On the Update Manager panel, click **Configure settings** in the list of Common tasks.
3. On the Settings panel, select the **Location** tab.
4. Enter `30234` (the maximum size), and click **OK**.

Procedure

Complete the following steps to update the IBM FSM from the IBM FSM Web interface:

1. Log in to the IBM FSM Web interface using a user account with sufficient privileges to update IBM FSM software.
2. From the Home page, select the **Initial Setup** tab.
3. From the Initial Setup tab, click **Check and Update Flex System Manager**. The IBM FSM management node accesses the IBM website and searches for IBM FSM updates that are later than the currently installed software and firmware.
4. Click the **Download and Install** to initiate the download and installation of the update.

   Note: Depending on the Internet connection that you have, the download process could take up to 2 hours.
5. When the update has been downloaded, you can start the update task to install the IBM FSM update.

Tip: The update task is referred to as a job task. If you are not familiar with job tasks in the IBM FSM, see A.1, “Starting a job task,” on page 155.

The time required to update also depends on the specific chassis configuration that is being managed by the IBM FSM.

If the update task completes with errors, see Chapter 7, “Troubleshooting update issues,” on page 137

What to do next

You need to restart the IBM FSM for the update to take effect. Use the link provided under **Flex System Manager - Check and Update** to restart the IBM FSM. The IBM FSM takes a further 30 to 90 minutes to fully restart.

Tip: As an alternative, to restart the IBM FSM, complete the following steps:

1. From the Home page, click the **Administration** tab.
2. Under Restart or Shut Down tasks, click **Shut down or Restart IBM Flex System Manager**.

Note: You need to restart the entire system for updates to take effect. Do not use Restart IBM Flex System Manager Server, which restarts the software only.

After the IBM FSM has restarted, you can use the **who** command to validate that the IBM FSM has been restarted. Establish an SSH session with the IBM FSM and log in to the IBM FSM CLI. The run the following command:

```
who -b
```

The result will be similar to:

```
system boot 2014-06-24 11:57
```

Important Considerations

- When the IBM FSM has restarted, make sure that you clear your browser cache before accessing the IBM FSM Web interface.
- Do **not** restart the IBM FSM until the IBM FSM update completes successfully. If you have trouble updating the IBM FSM firmware (pDSA, IMM, or UEFI) through the IBM FSM, you can log in to the IMM user interface for the IBM FSM to apply those updates. Complete the following steps:
  1. Make sure that FSMApplianceUpdate-1-3-2-ImportFirst.zip is on your computer. See 3.4, “Obtaining all updates,” on page 79 for information about the location of the updates.
  2. Unzip FSMApplianceUpdate-1-3-2-ImportFirst.zip
  3. Find the pDSA, IMM, and UEFI updates. The file name of the updates change each release, but you can search for the following strings to find the updates:
     - pDSA (Diagnostics). Search for ibm_fw_dsa_dsyt*_anyos_32-64.uxz
     - IMMv2. Search for ibm_fw_imm2_1aoo*_anyos_noarch.uxz
     - UEFI. Search for ibm_fw_uefi_bde*-1.21_anyos_32-64.uxz
  4. Use the IMM interface to apply those updates.

  Note: After applying IMM, pDSA, and UEFI updates, you will need to reset the IMM. To reset the IMM, establish an SSH session to the IMM for the compute node and use the **resetsp** command. Alternatively, you can restart the IBM FSM to reset the IMM.

For other issues related to the IBM FSM update, see Chapter 7, “Troubleshooting update issues,” on page 137

To update IBM Network Advisor (SMIA), go to Select fixes page in the Fix Central website, download the latest version of the fix, and then follow the instructions in the readme file.

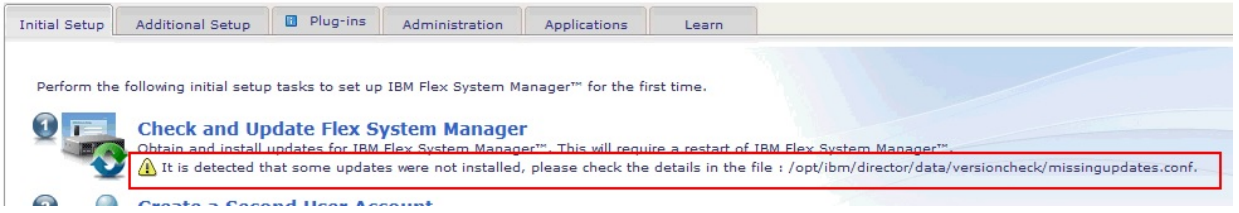
2.4.1 Validating that the IBM FSM is updated

Verify that the IBM FSM was updated successfully.

Procedure

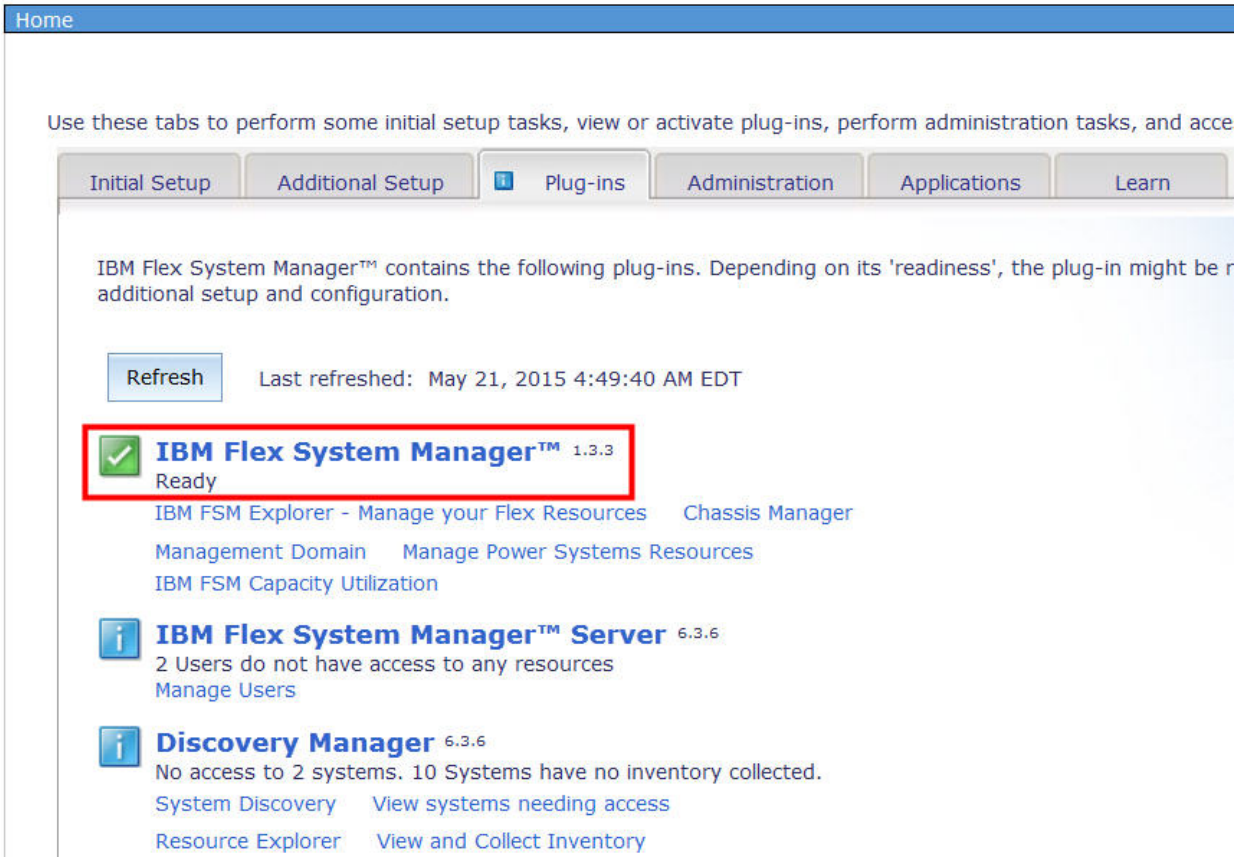
Complete the following steps to ensure that the IBM FSM update has completed successfully.

1. From the Home page, click the **Initial Setup** tab.



   If you see the indication that some of the updates were not installed, see 7.1, "IBM FSM software update causes warning on Initial Setup tab," on page 137.

2. To check the version of the IBM FSM that is installed, from the Home page, click the **Plugins** tab.



3. Select **IBM Flex System Manager**. Under the IBM FSM Status, the installed version is displayed.

What to do next

After validating that the IBM FSM was updated successfully, perform another backup of the IBM FSM. See 2.3.2, “Backing up the IBM FSM,” on page 29.

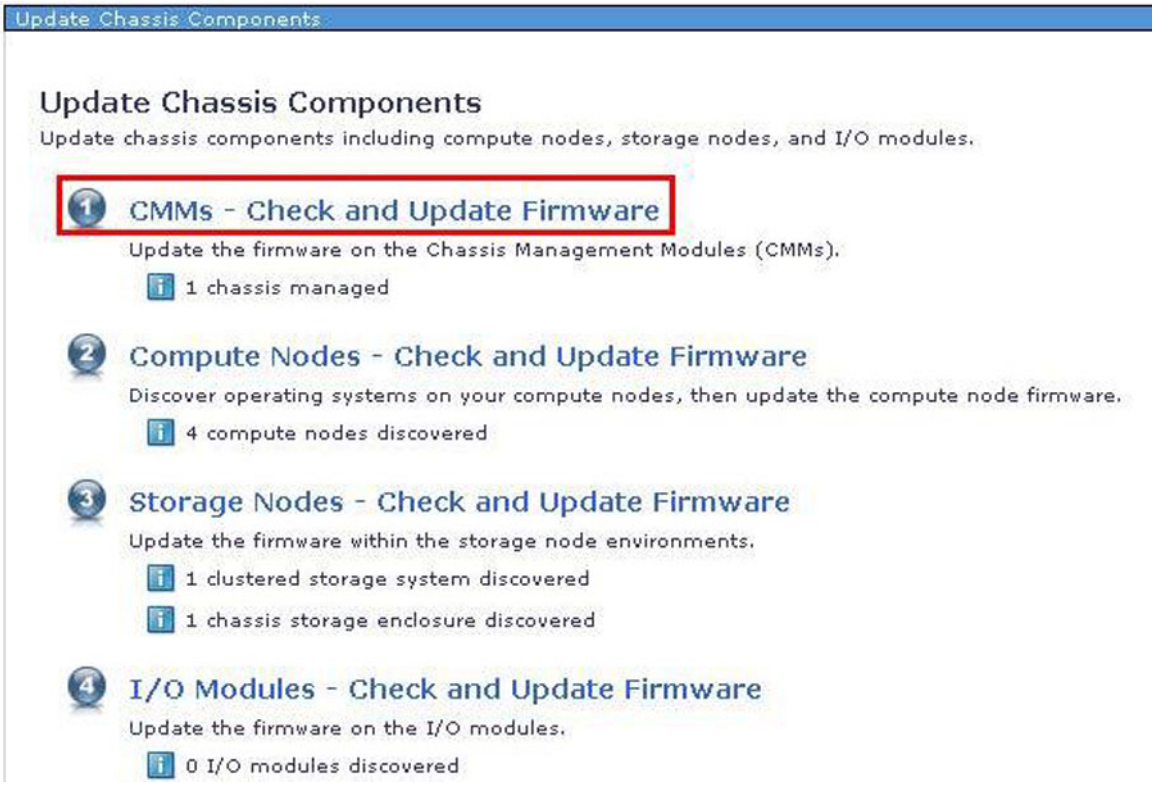
2.5 Updating the CMM

If you are updating the system that is managed by an IBM FSM, version 1.1.1 or earlier, you must update the Flexible Service Processor (FSP) for each Power Systems compute node ***before*** you update the CMM.

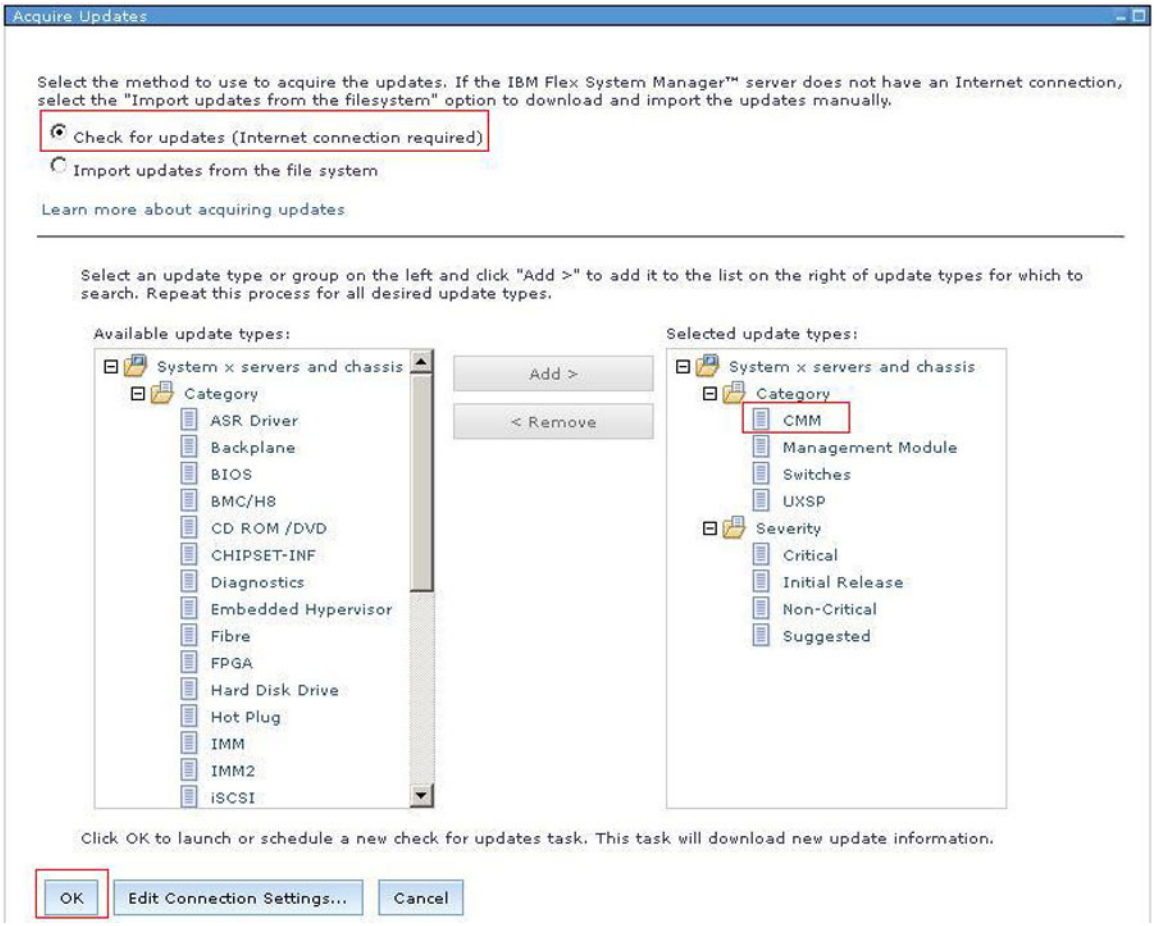
Procedure

Complete the following steps to update the firmware for ***each*** CMM in the chassis:

1. From the Home page, click the **Initial Setup** tab.
2. Click **Update Chassis components**. Then click **CMMs – Check and update Firmware**.



3. Check for available updates.
   a. From the Acquire Updates page, select **Check for updates (Internet connection required)**. Make sure that the CMM is listed in the Selected update types field and click **OK**.



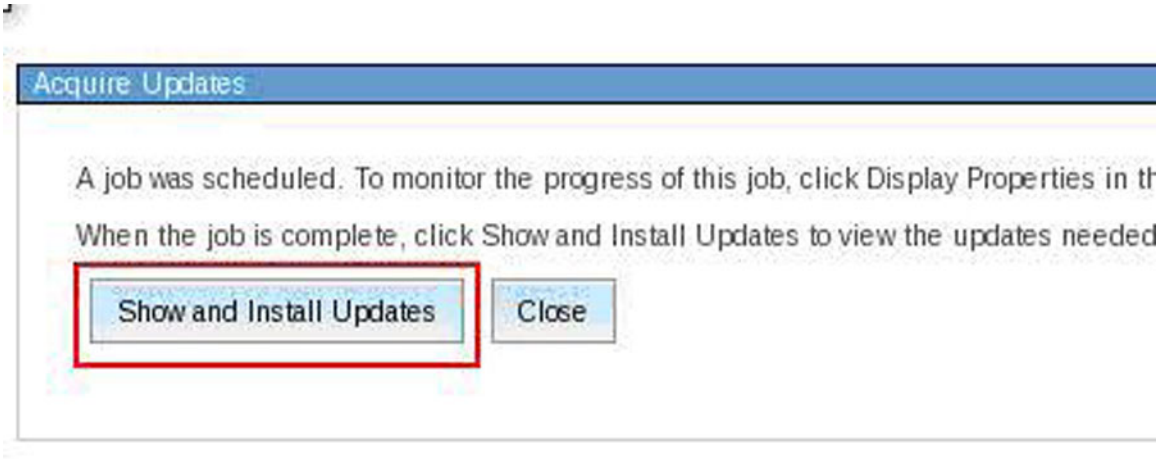
b. From the Schedule tab on the Launch Job window, select **Run Now**.

c. From the message confirming that the job was created and started successfully, click **Display Properties** to monitor the job status (displays the Active and Scheduled Jobs page).

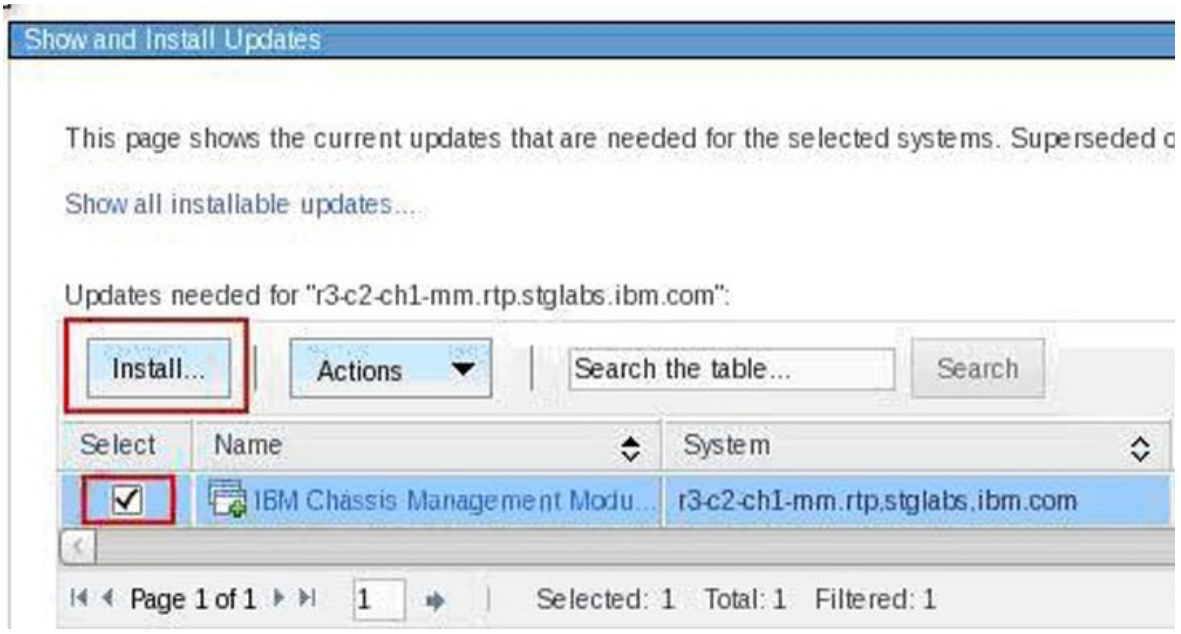
d. After the update has been imported successfully, close the **Active and Scheduled Jobs** page.

4. Install the updates

a. Click **Show and Install Updates** button in the Acquire Updates page.



b. From the Show and Install updates page, select the update in the Select column and click **Install** to start the Install Wizard.



Tip: In the Install Wizard, consider selecting the option **Automatically restart during installation as needed**. The CMM must be restarted for the update to take effect. However, you might lose your connection to the FSM temporarily while the CMM is restarting.

If you do not select the option **Automatically restart during installation as needed**, the update task will show as completing with errors (because the update task is not complete until the CMM is restarted).

c. Proceed to summary screen which summarizes the updates that will be installed. Click **Finish**.

d. In the Launch Job window, go to the Schedule tab and select **Run Now**. Then click **OK**.

Tip: The update task is referred to as a job task. If you are not familiar with job tasks in the IBM FSM, see A.1, “Starting a job task,” on page 155.

Results

You can verify the update completed successfully by looking in the Task Log Steps and verifying that each step completed with status Complete. For information about validating that the job completed successfully, see A.4, “Verifying an update completed successfully,” on page 161.

2.6 Updating compute nodes

Use the IBM FSM to update the firmware for Power Systems compute nodes and X-Architecture compute nodes.

The prerequisites for updating compute nodes can be found in the following website:

http://pic.dhe.ibm.com/infocenter/flexsys/information/index.jsp?topic=%2Fcom.ibm.acc.8731.doc%2Fcom.ibm.director.updates.helps.doc%2Ffqm0_c_um_platform_extensions.html

If you have configured a virtual environment, make sure that you relocated virtual servers before updating the compute nodes. More information about relocating virtual servers is available at the following location:

http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/com.ibm.director.vim.helps.doc/fqm0_t_relocating_a_virtual_server.html

To update System x compute nodes and the network adapters on Power Systems compute nodes, you must first discover the operating system running on the compute node from the IBM FSM.

Important consideration:

The IBM Flex System Manager management node Eth1 port must be connected to the chassis switch modules that are installed in I/O bay 1 or bay 2. This is referred to as the data network. You can configure a switch module in bay 1 or bay 2 to map Eth1 to one of its external Ethernet ports, as you would configure the other nodes in the chassis that are connected to the external network. The data network is used by applications and operating systems and can support data transfer rates up to 10 Gbps if a chassis switch module that is capable of 10 Gbps is installed.

One of the key functions that the data network supports is discovery of operating systems on the various network endpoints. Discovery of operating systems by the IBM Flex System Manager is required to support software and firmware updates on an endpoint such as a compute node. The IBM Flex System Manager Checking and Updating Compute Nodes wizard assists you in discovering operating systems as part of the initial setup.

IBM FSM does not support updating x440 M5 (MT 7167, 2590) and x240 M5 (MT 9532, 2588) ITEs. As an alternative, you can use the UpdateXpress System Packs (UXSPs) and the UpdateXpress System Pack Installer (UXSPI) to update these ITEs.

Important: There are no lifecycle UXSP releases in December 2014 (except for x440 M5 and x240 M5). However, you can apply the existing individual Mezzanine updates to these ITE end points.

2.6.1 Discovering operating systems from the IBM FSM

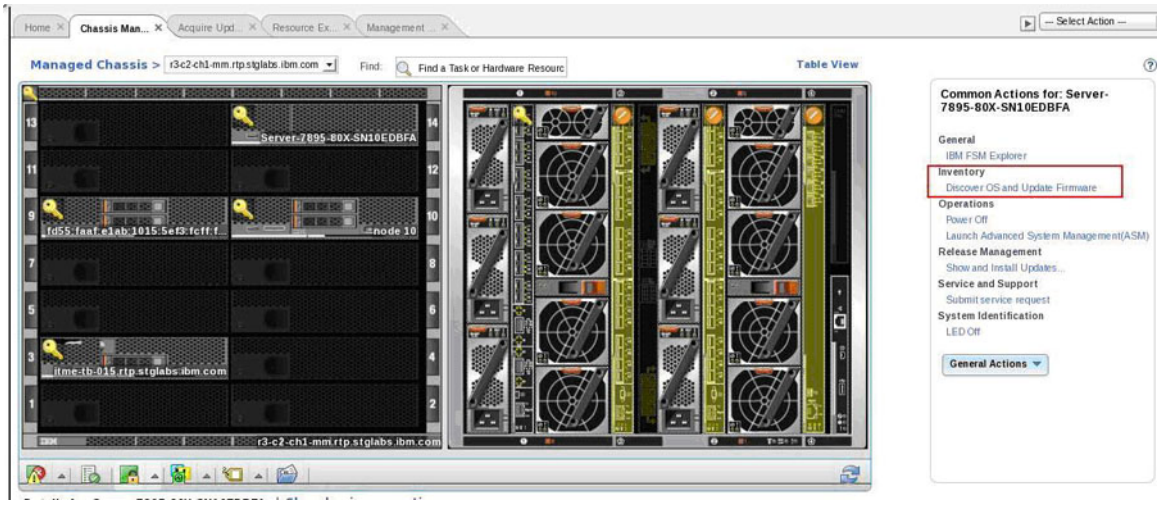
You need to ensure that all operating systems have been discovered by the IBM FSM.

If you followed the procedures in 2.3.1, “Making sure that the IBM FSM is managing the chassis,” on page 25, all operating systems should be discovered by the IBM FSM and you can proceed to one of the following sections:

- 2.6.2, “Updating Power Systems compute nodes,” on page 38
- 2.6.3.2, “Installing X-Architecture compute node updates,” on page 50

If you have not already discovered the operating system for a compute node, complete the following steps:

1. From the Chassis Manager tab, select the compute node for which the operating system is to be discovered.
2. Under Common Actions, select **Discover OS and Update Firmware**:



More information about updating compute nodes is available in the *Updating firmware on a compute node from the IBM Flex System Manager user interface Quick Start Guide* at the following website:

http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.commontasks.doc/commontasks_managing_hw.html

The IBM FSM operating system discovery process can fail if the compute node is configured with VMware vSphere Hypervisor 5.5 with IBM Customization Installable, any model, any update and there are multiple VMK interfaces. To resolve the issue, see the following website:

http://www-947.ibm.com/support/entry/portal/docdisplay?brandind=5000008&indocid=MIGR-5095635

2.6.2 Updating Power Systems compute nodes

Before updating the firmware for the FSP on Power Systems compute nodes, make sure that you have read the prerequisites.

Before you begin

Prerequisites are listed in 2.2, “Prerequisites,” on page 21. In addition, make sure that you have performed the procedures described in 2.3, “Preparing for updates,” on page 25.

Important considerations:

- If you are updating firmware for Power Systems compute nodes running FSP firmware that is earlier than the December, 2012 release (AF763_043), you must update the Flexible Service Processor (FSP) for each Power Systems compute node before you update the CMM.

  Updating older version FSPs after updating the CMM might leave your compute nodes unusable (in a status 'pending' condition). If this happens, see 7.9, “Power Systems compute node remains at a status pending state after an update,” on page 142.
- If you are updating firmware for Power Systems compute nodes running FSP firmware 01AF773, you must update the Flexible Service Processor (FSP) for each Power Systems compute node to 01AF773_058 before you update the firmware for the IBM FSM. See 2.1.2, “Steps to update for Power Systems compute nodes running FSP firmware version 01AF773,” on page 20 for more information.
- Make sure that SCP is installed on the Power Systems compute nodes before running Discovery or Inventory Collection from the IBM FSM so that the network adapters are discovered and inventoried by the IBM FSM. For more information about installing SCP, which is available with the OpenSSH software tools, see the following website:

  http://pic.dhe.ibm.com/infocenter/aix/v7r1/topic/com.ibm.aix.security/doc/security/openssh_kerberosv5.htm

Procedure

Complete the following steps to update firmware for the FSP on Power Systems compute nodes:

1. From the Chassis Manager, click **General Actions** > **Manage Power Systems Resources**.
2. Click **Actions** > **Select All** to select all of the Power Systems hosts.
3. Acquire the updates to be applied. Click **Actions** > **Release Management** > **Acquire Updates**.
4. Select **Actions** > **Release Management** > **Show and Install Updates**.

   Note: If the expected updates do not display, see 7.11, “Power Systems firmware update does not display as needed,” on page 143 for information about showing all updates.
5. Select the FSP update, start the task, and wait for it to complete.

   Tip: The update task is referred to as a job task. If you are not familiar with job tasks in the IBM FSM, see A.1, “Starting a job task,” on page 155.

   Important consideration

   Updates to the Power Systems FSP cannot be selected at the same time as the Power Systems updates that run in-band from the operating system. Update the Power Systems compute nodes in the following order:

   a. Update the FSP.
   b. After updating all other components in the chassis, see the following sections to continue with the updates for the Power Systems compute node:
      - 2.6.2.2, “Updating Power Systems network adapters and hard disk drives,” on page 39.
      - 2.6.2.3, “Updating the IBM Flex System EN4054 4-port 10Gb Ethernet Adapter,” on page 41.

What to do next

Ensure that all Power System updates complete successfully before continuing to update the remaining components in the chassis.

If you did not update the FSP on Power Systems compute nodes before updating the CMM, and the Power Systems compute node remains at a status pending state after an update, see 7.9, "Power Systems compute node remains at a status pending state after an update," on page 142 to resolve the issue.

2.6.2.1 Activating the Power FSP update on the Permanent boot side

FSP updates for Power Systems are deployed on the Temporary boot side of the Power Systems compute node. After you have determined that FSP update is working correctly in your environment, apply the update to the Permanent boot side.

Procedure

Complete the following steps to apply the firmware update to the permanent boot side:

1. From the Chassis Manager, click **General Actions** > **Manage Power Systems Resources**.
2. From the Manage Power Systems Resource menu, select all **Power Systems**.
3. Click **Actions** > **Release Management** > **Power Firmware Management**.
4. Click **Actions** > **Power Firmware Management** > **Accept**.
5. Click the **Start Accept Task** and start the job task.

   Tip: If you are not familiar with job tasks in the IBM FSM, see A.1, "Starting a job task," on page 155.
   .

2.6.2.2 Updating Power Systems network adapters and hard disk drives

Use this procedure to update the firmware for network adapters and hard disk drives.

Procedure

If you are updating firmware for the IBM Flex System EN4054 4-port 10Gb Ethernet Adapter, see 2.6.2.3, "Updating the IBM Flex System EN4054 4-port 10Gb Ethernet Adapter," on page 41.

Note: Before updating firmware on Ethernet adapters, make sure that all ports are inactive.
Complete the following steps to update firmware for Power Systems compute nodes:

1. From the Chassis Manager, click **General Actions** > **Manage Power Systems Resources**.
2. From the Manage Power Systems Resources menu, click **Operating Systems**.
3. Click **Actions** > **Select All** to select all of the Power Systems operating systems.
4. Acquire the updates to be applied. Click **Actions** > **Release Management** > **Acquire Updates**.
5. Select **Actions** > **Release Management** > **Show and Install Updates** to start the Install Wizard.
6. From the Welcome page, click **Next**.
7. On the Device Options page, select all devices to be updated.

   Note: If a device has multiple ports, such as the FC3172 2-port 8Gb Fiber Adapter, make sure that you check all ports (for example: fcs0 and fcs1).

   Click **Next**.
8. On the Restarts page, note any restart requirements. Then click **Next**.
9. On the Summary page, confirm the updates to be installed. Then click **Finish**.
10. From the Schedule tab in the Launch Job window, select **Run Now**. Then click **OK**.

Tip: The update task is referred to as a job task. If you are not familiar with job tasks in the IBM FSM, see A.1, “Starting a job task,” on page 155.

2.6.2.3 Updating the IBM Flex System EN4054 4-port 10Gb Ethernet Adapter

Complete the following steps to update the firmware for the IBM Flex System EN4054 4-port 10Gb Ethernet Adapter through VIOS and AIX.

Before you begin

Note: Before the IBM Flex System EN4054 4-port 10Gb Ethernet Adapter firmware update can occur, any non-native Ethernet devices (i.e. Etherchannel, SEA, VLAN psuedo device) must be reconfigured to use one of the native Ethernet adapter ports. This process will disrupt Ethernet traffic to any client LPARs and will require a reboot of VIOS. Therefore, this procedure should be performed during a maintenance window.

Procedure

The steps are written such that there is no need to save any non-native Ethernet device configuration information prior to execution. Upon reboot of VIOS, the original non-native Ethernet device configuration will be restored automatically.

1. Complete the following steps to log in to VIOS:

   Note: Do not attempt to open a console to VIOS using a method that depends on the Ethernet connection, such as SSH. Ethernet connectivity will be disrupted during the firmware update process.

   a. From the Chassis Manager, click **General Actions** > **Manage Power System Resources**.
   b. From the Manage Power Systems Resources menu, click **Virtual Servers**.
   c. Put a check mark in the box beside the VIO server to select it. Then click **Actions** > **Operations** > **Console Window** > **Open Terminal Console**.
2. Run the following command to obtain root access:

   ```
   oem_setup_env
   ```
3. Save the existing network configuration:
   a. Run the following command:

      ```
      ifconfig –a
      ```

      Note the IP address and interface where the IP address is configured. If multiple IP addresses are configured, make a note of each IP address and interface.
   b. Run the following command:

      ```
      netstat -rn
      ```

      Make a note of the routing information.
4. Determine how the adapter port that requires the firmware update is configured. Run the following commands to determine how the adapter port is configured.
   - `lsdev -c adapter` - to list all adapters
   - `lsdev -t ibm_ech` - to list all EtherChannel adapters
   - `lsdev -t sea` - to list all Shared Ethernet Adapters
   - `lsdev -s vlan` - to list all VLAN devices
   - `lsattr -El entX` - to list attributes of a given adapter (e.g. `lsattr -El ent7`)

   Adapter ports can be configured in one of the following ways:
   - Natively where the IP address is configured on the port.
   - Part of EtherChannel.
   - Part of Shared Ethernet Adapter (SEA)
   - Part of EtherChannel, which is configured as part of SEA.
   - Part of SEA (either directly or via EtherChannel) and the VLAN pseudo device is configured on top of SEA.

5. Prepare the ports for firmware updates, depending on how the ports are configured:
   - Natively where the IP address is configured on the port. If the adapter port is configured natively, no further action is required. You can proceed with the firmware update without making changes to the configuration.

     Go to step 7 on page 43⌂
   - Part of EtherChannel. If the adapter port is part of EtherChannel and an IP address is configured on EtherChannel, complete the following steps:
     a. Run the command "`ifconfig enX detach`" to remove the IP address where *enX* is the EtherChannel device interface (e.g. en7)
     b. Remove the EtherChannel device by running the command, "`rmdev -l entX`" where *entX* is the EtherChannel device e.g ent7
     c. Go to step 6⌂
   - Part of Shared Ethernet Adapter (SEA). If the adapter port is part of SEA and an IP address is configured on SEA, complete the following steps:
     a. Run the command "`ifconfig enX detach`" to remove the IP address where *enX* is the SEA device interface (e.g. en9)
     b. Remove the EtherChannel device by running the command, "`rmdev -l entX`" where *entX* is the SEA device (e.g ent9)
     c. Go to step 6⌂
   - Part of EtherChannel, which is configured as part of SEA. If the adapter port is part of EtherChannel, which is configured as part of SEA, and an IP address is configured on SEA. For example, ent9 is SEA which uses ent7, ent7 is EtherChannel, and the IP address is configured on en9:
     a. Run the command "`ifconfig enX detach`" to remove the IP address where *enX* is the SEA device interface (e.g. en9)
     b. Remove the SEA device by running the command, "`rmdev -l entX`" where *entX* is the SEA device (e.g. ent9)
     c. Remove the EtherChannel device by running the command, "`rmdev -l entX`" where *entX* is the EtherChannel device (e.g ent7)
     d. Go to step 6⌂
   - Part of SEA (either directly or via EtherChannel) and the VLAN pseudo device is configured on top of SEA. If the adapter port is configured as part of SEA (either directly or via EtherChannel), the VLAN pseudo device is configured on top of SEA, and the IP address is configured on top of VLAN pseudo device. For example, ent10 is VLAN pseudo device, ent9 is the SEA, ent7 is the EtherChannel, and the IP address is configured on en10:
     a. Run the command "`ifconfig enX detach`" to remove the IP address where *enX* is the VLAN pseudo device interface (e.g. en10)
     b. Remove the VLAN pseudo device by running the command, "`rmdev -l entX`" where *entX* is the VLAN device (e.g. ent10)
     c. Remove the SEA device by running the command, "`rmdev -l entX`" where *entX* is the SEA device (e.g. ent9)
     d. Remove the EtherChannel device by running the command "`rmdev -l entX`" where *entX* is the EtherChannel device (e.g ent7)
     e. Go to step 6⌂
6. Reconfigure the IP address and default gateway saved in step 3 on page 41. If the adapter was not configured natively, choose the adapter that was part of SEA or EtherChannel device to configure the IP address:
   a. To configure IP address, run the command

      `ifconfig enX <IP address> netmask <netmask value>`

where *enX* is the interface of the chosen adapter. Use the IP address and netmask value saved in step 3 on page 41.

b. Configure the default route by running the command,

```
"route add 0 <default gw>"
```

Determine the value of *default gw* from the output of netstat -rn command saved in step 3 on page 41.

c. Verify the network connectivity with the IBM FSM. If the IBM FSM is reachable, the firmware update is successful.

d. If the chosen adapter was part of EtherChannel and the IBM FSM is not reachable, try the next adapter in EtherChannel and follow steps a through c. For example, if ent0 and ent1 were in EtherChannel and ent0 did not work, try ent1.

7. After the IBM FSM is reachable from a VIOS console, the firmware update can be performed:

a. Refer to Step 1 of 2.6.2.2, "Updating Power Systems network adapters and hard disk drives," on page 39.

Note: In Step 3 of that procedure, do not select all Power Systems operating systems; select the VIOS server instead.

b. After completing Step 4, on the Acquire Updates page within the Available update types table, the only item that needs to be added to the table is **Power IO Firmware** > **Latest Update**.

c. Continue with step 5 of 2.6.2.2, "Updating Power Systems network adapters and hard disk drives," on page 39.

What to do next

After the firmware update is complete, reboot the VIOS partition.

2.6.2.4 Updating the IBM Flex System FC5052 2-port 16Gb or FC5054 4-port 16Gb Fibre Channel adapter

Complete the following steps to update the firmware for the IBM Flex System FC5052 2-port 16Gb or FC5054 4-port 16Gb Fibre Channel adapter installed in a IBM Flex System p24L Compute Node.

Before you begin

This procedure requires you to download OneCommand Manager from Emulex. In order to download the correct version, you must first determine the current microcode level. Before you begin, ensure that you have the ability to download these files, and to transfer them via USB key or SCP to the target compute node. In addition, you must download the firmware update and use a USB key or SCP to copy the update to the target compute node.

Procedure

1. Determine the current microcode level for the installed version of Linux.

Note: The following steps are for Linux systems running the 2.6 kernel (Red Hat or SuSE), which support the /sys filesystem. These steps assume you are logged in with root permissions and that at least one IBM Flex System FC5052 2-port 16Gb Fibre Channel adapter (Feature Code: EC23) or IBM Flex System FC5054 4-port 16Gb Fibre Channel adapter (Feature Code: EC2E) is installed.

a. Use SSH to establish a session to the compute node operating system.

b. Display the model description for each installed Fibre Channel adapter. The number of displayed descriptions should match the number of ports for the adapter to be displayed.

Type the following command to display a list showing the /sys/class/scsi_host/ host{n}:description for each installed adapter:

```
find -L /sys/class/scsi_host/host* -maxdepth 1 -name "modeldesc" -printf %h:
 -exec cat {} \; | grep '5052\|5054'
```

The output will be similar to the following list.

```
/sys/class/scsi_host/host0:IBM Flex System FC5054 47C9999 4-port 16Gb FC Adapter
 /sys/class/scsi_host/host1:IBM Flex System FC5054 47C9999 4-port 16Gb FC Adapter
 /sys/class/scsi_host/host2:IBM Flex System FC5054 47C9999 4-port 16Gb FC Adapter
 /sys/class/scsi_host/host3:IBM Flex System FC5054 47C9999 4-port 16Gb FC Adapter
```

Record the host{n} values for use in the next step.

Note: If the list is empty, make sure that you typed the command correctly and that there is at least one adapter installed in the compute node.

c. Display the firmware version for **each** model adapter listed in the previous step.

Type the following command, replacing *host{n}* with the value listed for each adapter in the previous step.

```
cat /sys/class/scsi_host/host{n}/fwrev
```

Note: The microcode version listed might vary but output will be similar to the following example (four numbers separated with ".", sli-4:2:b:)

```
 1.1.37.0, sli-4:2:b
```

If one or more adapter lists a microcode version that is not the latest version, then the microcode update should be applied.

d. Display the version of the Linux operating system installed on the compute node.

- If RHEL is installed, type the following command to display the version:

```
cat /etc/redhat-release
```

The output should be similar to the following:

```
Red Hat Linux Server release 6.4 ()
```

If SuSE (SLES) is installed, type the following command to display the version:

```
cat /etc/SuSE-release
```

The output should be similar to the following:

```
SUSE Linux Enterprise Server 11 (ppc64)
VERSION = 11
PATCHLEVEL = 3
```

2. Use the Emulex **hbacmd** utility to update the firmware.

a. Download OneCommand Manager

Firmware updates on Fibre Channel adapters installed in a Linux system require the use of the Emulex **hbacmd** utility. The **hbacmd** utility is included in the Emulex OneCommand CLI Applications Kit, which can be downloaded from the following website:

http://www.emulex.com/downloads/oem-qualified-downloads/ibm/drivers-for-ibm-power/

Complete the following steps:

1) In the Drivers and Management Software for Linux box, choose the operating system that is installed on the compute node.
2) Select the appropriate service pack or update (based on step 1d).
3) From the Download page, verify the operating system information. Then select the **Management and Utilities** tab.
4) Choose the link for **Application Kit <*version*>** (CLI) that matches the operating system installed on the compute node.
5) When prompted, save the Application Kit to a directory on the compute node. For example, you can save the file elxcmcore-xxxx-xxxx-x.x.x.x-x.tgz to the /tmp directory.
6) After the file has been downloaded, change directories to the location where the file was downloaded.

7) Unpack the .tgz file:

```
tar xzf elxcmcore-xxxx-xxxx-x.x.x.x-x.tgz
```

8) Change directories to elxcmcore-xxxx-xxxx-x.x.x.x-x and install the utility:

```
./install.sh
```

9) After the utility is installed, you can verify that it was installed successfully by running the following command:

```
/usr/sbin/ocmanager/hbacmd version
```

b. Make sure that all I/O activity to storage devices controlled by the adapter is stopped before proceeding. When you update the firmware, the adapter will be reset.

c. Update the firmware.

1) List the installed Emulex adapters:

```
/usr/sbin/hbacmd listhbas
```

The result of this command will be similar to the following output with one section for each discovered adapter.

Note: For each adapter, make a note of the Port WWN: value. The Port WWN values will be required as an argument for commands in next steps.

```
Manageable HBA List

Port WWN       : 10:00:00:90:fa:14:5a:f2
Node WWN       : 20:00:00:90:fa:14:5a:f2
Fabric Name    : 10:00:00:27:f8:05:68:19
Flags          : 8000e200
Host Name      : 7895-23x-1-lp2
Mfg            : Emulex Corporation
Serial No.     : 123456789
Port Number    : 0
Mode           : Initiator
PCI Bus Number : 1
PCI Function   : 0
Port Type      : FC
Model          : 47C9999
```

2) List the hba attributes for each adapter port that was listed in the previous step:

```
/usr/sbin/hbacmd hbaattributes {wwpn}
```

where *{wwpn}* is one of the port WWPN values listed in the previous step.

The result will look similar to the following and lists the current version of firmware. Record the current operational firmware values to compare against the values after the update.

```
HBA Attributes for 10:00:00:90:fa:14:5a:f2
Host Name                    : 7895-23x-1-lp2
Manufacturer                 : Emulex Corporation
Serial Number                :  123456789
Model                        : 47C9999
Model Desc                   : IBM Flex System FC5054 47C9999 4-port 16Gb FC Adapter
Node WWN                     : 20 00 00 90 fa 14 5a f2
Node Symname                 : Emulex 47C9999 FV1.1.37.0 DV8.3.5.68.5p
HW Version                   : 0000000b
FW Version                   : 1.1.37.0
Vendor Spec ID               : 10DF
Number of Ports              : 1
Driver Name                  : lpfc
Device ID                    : E200
HBA Type                     : 47C9999
Operational FW               : 1.1.37.0
IEEE Address                 : 00 90 fa 14 5a f2
Boot Code                    : Enabled
Boot Version                 : KT8.02a10
Driver Version               : 8.3.5.68.5p; HBAAPI(I) v2.3.b, 07-12-10
Board Temperature            : Normal
```

```
Function Type                : FC
Sub Device ID                : E282
PCI Bus Number               : 1
PCI Func Number              : 0
Sub Vendor ID                : 10DF
Service Processor FW Name    :  1.1.37.0
ULP FW Name                  : 1.1.37.0
FC Universal BIOS Version    : KT8.02a10
FC x86 BIOS Version          : KA6.01a12
FC EFI BIOS Version          : KD6.01a13
FC FCODE Version             : KN4.02a14
Flash Firmware Version       : 1.1.
```

d. Update microcode on each of the model adapter ports, one at a time.

   This step assumes that microcode image is located in the `/lib/firmware` folder.

   Important: Do not interrupt or power off the system while firmware updates are in progress.

   Run the following commands to update the firmware:

   `/usr/sbin/hbacmd download {wwpn} /lib/firmware/YXXXXX.grp`

   Where *{wwpn}* is one of the port WWN values listed for the Emulex adapters.

e. Repeat the previous step for each adapter port that needs the firmware update (using each of the WWPNs listed.

f. Restart the compute node to load the new firmware.

g. After restarting the compute node, verify the firmware versionsfor each adapter port using the command:

   `/usr/sbin/hbacmd hbaattributes {wwpn}`

2.6.3 Updating X-Architecture compute nodes

Before updating the firmware for X-Architecture compute nodes, make sure that you have read the prerequisites list.

The prerequisites are described in 2.2, “Prerequisites,” on page 21.

Important considerations:

- If you plan to update multiple X-Architecture compute nodes that are running different operating systems concurrently, and one or more of those compute nodes is running VMware ESXi, make sure that you update all X-Architecture compute nodes running ESXi separately from compute nodes running other operating systems. For example, if you have X-Architecture compute nodes running ESXi, Windows, and Linux:

  1. Update the compute nodes running ESXi concurrently.
  2. Update the compute nodes running Windows and Linux concurrently.

  If you do attempt to update firmware for compute nodes that are running different operating systems and you receive a "File not found" error for a compute node, attempt to update the firmware for just that compute node.

- You **must** install IBM Customization Patch 1.2 or later on each compute node running VMware vSphere ESXi 5.0.x/5.1.x/5.5.x. There is a separate customization patch for each version of VMWare.

  If you are running VMware vSphere ESXi 5.5.x (update 1) or earlier, you must apply both the Lenovo and the Independent Hardware Vendor (IHV) customization patches (Patch 1.2) on every compute node. If you are running VMware vSphere ESXi 5.5.x (update 2), you need not apply Patch 1.2.

  In addition to the IBM Customization Patch 1.2, make sure that you install one of the following updates to the VMware vSphere ESXi operating system:

  – If you are running VMware vSphere ESXi 5.0, make sure that you install update 5.0u2 (update 2)
  – If you are running VMware vSphere ESXi 5.1, make sure that you install update 5.1u1 (update 1)

When you install an IMM update on an X-Architecture compute node, the Integrated Management Module (IMM) is reset, which can cause a VMware vSphere ESXi system failure (host purple diagnostic screen) if you attempt to update an X-Architecture compute node on which the minimum level of VMware is not installed (5.0u2 or 5.1u1).

For information about obtaining the IBM Customization Patch 1.2, see the following location:

http://www.ibm.com/support/entry/portal/docdisplay?lndocid=MIGR-5092679

Make sure that you review the information provided in the readme for the patch. It contains instructions for installing the patch on a compute node.

- If you are attempting to update the ServeRAID M5115 PSoC3 update to version 68, see 7.27, "The ServeRAID M5115 PSoC3 update package cannot be installed from IBM FSM or UXSPI," on page 152.
- The Emulex firmware update requires either the Corekit or the OneCommand Manager (OCM) application to be installed on Microsoft Windows or Linux operation systems before updating compute nodes running those operating systems.
- If the IMM firmware level on X-Architecture compute nodes installed in your chassis is earlier than the December, 2012 release (v1.60, build 1AOO32P) and you want to activate centralized user management on the IBM FSM, you should update the firmware for X-Architecture compute nodes before you enable centralized user management through the IBM FSM.

  Failing to update the firmware in the X-architecture compute nodes first when activating centralized user management, will result in a situation where an X-Architecture compute node with previous IMM firmware levels will show as locked in the IBM FSM user interface. You will not be able to access the IMM externally with any account credentials. In addition, the IBM FSM will not be able to update the firmware for the X-Architecture compute node.

  To avoid this situation, do not enable centralized user management for a chassis until after X-Architecture compute nodes are updated to a firmware level equal to or later than December 2012.

  If you have already activated centralized user management on your IBM FSM, you have X-Architecture compute nodes at IMM firmware level lower than December 2012 (v1.60 build 1AOO32P), and the compute nodes are showing in a locked state in the FSM, see 7.16, "X-Architecture compute node shows as locked on the IBM FSM when using Centralized Management," on page 146 to resolve the issue.

Special considerations for scalable systems:

If you are updating the firmware for a multi-node system (also called a scalable system), such as the Flex System x280 X6, x480 X6, or x880 X6 Compute Node, the IBM FSM keeps the following system firmware at the same level on all physical servers across the system:

- DSA
- IMM
- UEFI

To achieve this, if any system firmware update is needed on the physical server, update manager on the IBM FSM marks the needed relationship on the top level system, also called the cluster system. Then, during installation, the update is applied to all the physical servers in the multi-node system.

Note: Update manager does not support multi-node systems that have ESXi installed on them. You cannot use the IBM FSM to update firmware for these systems.

Consider the following items when updating the system firmware on multi-node systems:

- Before starting any system firmware update processes, ensure that the multi-node systems are discovered with both inband mode and OOB mode. Make sure that all inventory is collected on all the scalable partition systems and the cluster system.
- When checking compliance, the DSA, IMM, and UEFI firmware is shown on the cluster manageable endpoint of the multi-node system instead of on the physical server system or partition system.

- The systems firmware updates are installed to all the physical server systems when you install the update on the multi-node system. All the partition systems are then rebooted after the installation.
- When updating a batch of update packages on multi-node systems, it would be a two-step update:
  1. Install the DSA, IMM, and UEFI firmware updates on cluster system first.
  2. After the task completes successfully, continue to install the rest of the updates on each partition system.

2.6.3.1 VMware ESXi update considerations

Read through the following considerations if you are running VMware vSphere ESXi on X-Architecture compute nodes.

- If you are updating an ESX or ESXi system that is configured for virtual switch (vswitch) and there is no physical network adapter associated with the virtual switch, inventory collection from the IBM FSM will fail. See 7.24, "Inventory collection on compute nodes running ESX or ESXi consistently fails, which means that firmware update will not be deployed," on page 150 to resolve this issue.
- Before updating the firmware for a compute node that is running ESXi, make sure that you enable maintenance mode. For information about enabling maintenance mode, see the documentation that is provided with ESXi.
- When updating a compute node running VMware ESXi, the host must be fully initialized before the update process starts. Make sure you wait for the full compute node initialization to complete, which takes approximately 20 minutes.

  If the host is not fully initialized, you might see an error with the update or an error stating that the system failed to restart, and that it must be restarted manually (even if you choose to have the compute node restarted automatically after the update). If you see this error, restart the compute node manually. If there are no other errors listed, the firmware update was successful.
- The following ESXi images are supported by the IBM FSM:
  – The standard ESXi image. If you deployed the standard ESXi image, the IBM FSM is limited to updating the UEFI, preboot DSA, and IMM firmware.

    You must be running one of the following ESXi versions:
    - VMware vSphere ESXi 5.0. Make sure that, at a minimum, you are running version 5.0u2 (update 2)
    - VMware vSphere ESXi 5.1. Make sure that, at a minimum, you are running version 5.1u1 (update 1).
    - VMware vSphere ESXi 5.5 (any version)

      Note: When you install an update to the Integrated Management Module (IMM) on an X-Architecture compute node, the IMM is reset. In this case, if you have not installed (at a minimum) update 5.0u2, 5.1u1, or 5.5.x, a VMware vSphere ESXi system failure (host purple diagnostic screen) might occur.
  – The VMware vSphere Hypervisor (ESXi) with IBM Customization. If you deployed ESXi with IBM Customization, the IBM FSM can also update firmware for network (I/O) adapters and LSI RAID controllers.

    Note: Hard drive updates from the IBM FSM are not supported.

    Note: BNX1 and BNX2 firmware updates are not supported on ESXi Customized Image with Patch 1.2

    For best performance, consider running one of the following ESXi versions:
    - VMware vSphere ESXi 5.0. Make sure that, at a minimum, you are running version 5.0u2 (update 2)
    - VMware vSphere ESXi 5.1. Make sure that, at a minimum, you are running version 5.1u1 (update 1).

If you deploy ESXi with IBM Customization through the IBM FSM operating system deployment task (IBM FSM version 1.3.0 or 1.3.1), you will be running version 5.1u1.

- VMware vSphere ESXi 5.5. (any version)

Note: When you install an update to the Integrated Management Module (IMM) on an X-Architecture compute node, the IMM is reset. In this case, if you have not installed (at a minimum) update 5.0u2 5.1u1, or 5.5.x, a VMware vSphere ESXi system failure (host purple diagnostic screen) might occur.

To validate that you are running the IBM-customized version, check that the file `/etc/cim/ibm/imm_fw_schema` exists on the image. This file should contain lines indicating that the SCHEMA_STATE is "check" and showing a version number for the FW_VERSION field. To review the list of custom providers, use the command "**`esxcli software vib list`**" on your ESXi server.

Tip: You can compare this list with the list provided in the readme for Patch 1.2.

Complete the following steps to update a compute node that is running VMware vSphere ESXi with IBM Customization:

1. Make sure that you are running at least VMWare ESXi version 5.0u2 5.1u1, 5.5.x. If not, you will need to upgrade to one of those versions before proceeding.
2. Install IBM Customization patch 1.2, which can be found at this location:

   Note: There is an IBM Customization patch 1.2 for each VMWare version 5.0.x, 5.1.x and 5.5.x.

   http://www.ibm.com/support/fixcentral/systemx/quickorder?parent=x220+Compute+Node&product=ibm/systemx/2585&&platform=All&function=fixId&fixids=ibm_sw_hyper_patchbundlv8_vmwaresx5_32-64&includeRequisites=0&includeSupersedes=0&downloadMethod=http&source=fc

   For more information about obtaining the IBM Customization patch 1.2, see the following location:

   http://www.ibm.com/support/entry/portal/docdisplay?lndocid=MIGR-5092679
3. Install the drivers for each of the adapters that are installed in the compute node. You can find information about these driver updates by going to the following website:

   http://www.ibm.com/support/fixcentral/

   From the Fix Central site, select the following fields:

   - **Product Group**: PureSystems
   - **Select from PureSystems**: PureFlex System
   - **Select from PureFlex System**: Compute Node
   - **Select from Compute Node**: The compute node on which the ESXi image is installed

   Select the appropriate device drivers based on the adapters that you have installed. Follow the instructions provided with the driver update to install the driver.
4. Apply the firmware updates based on the procedure listed in 2.6.3.2, "Installing X-Architecture compute node updates," on page 50.

- If storage paths are lost for any reason in a configuration with VMware, CN4022, and storage devices, the paths might recover. Paths also might recover and then fail again in about 5 to 45 minutes.

  You can recognize lost paths with the following command:

  ```
  esxcfg-mpath -L | grep dead
  ```

  The paths can be recovered by issuing the following command:

  ```
  esxcli storage filesystem rescan -a
  ```

  To reduce potential issues, update one SVC controller, making sure the paths have a chance to settle and recover with the rescan command. Then update the second SVC controller.

2.6.3.2 Installing X-Architecture compute node updates

Use this procedure to install updates for X-Architecture compute nodes

Before you begin

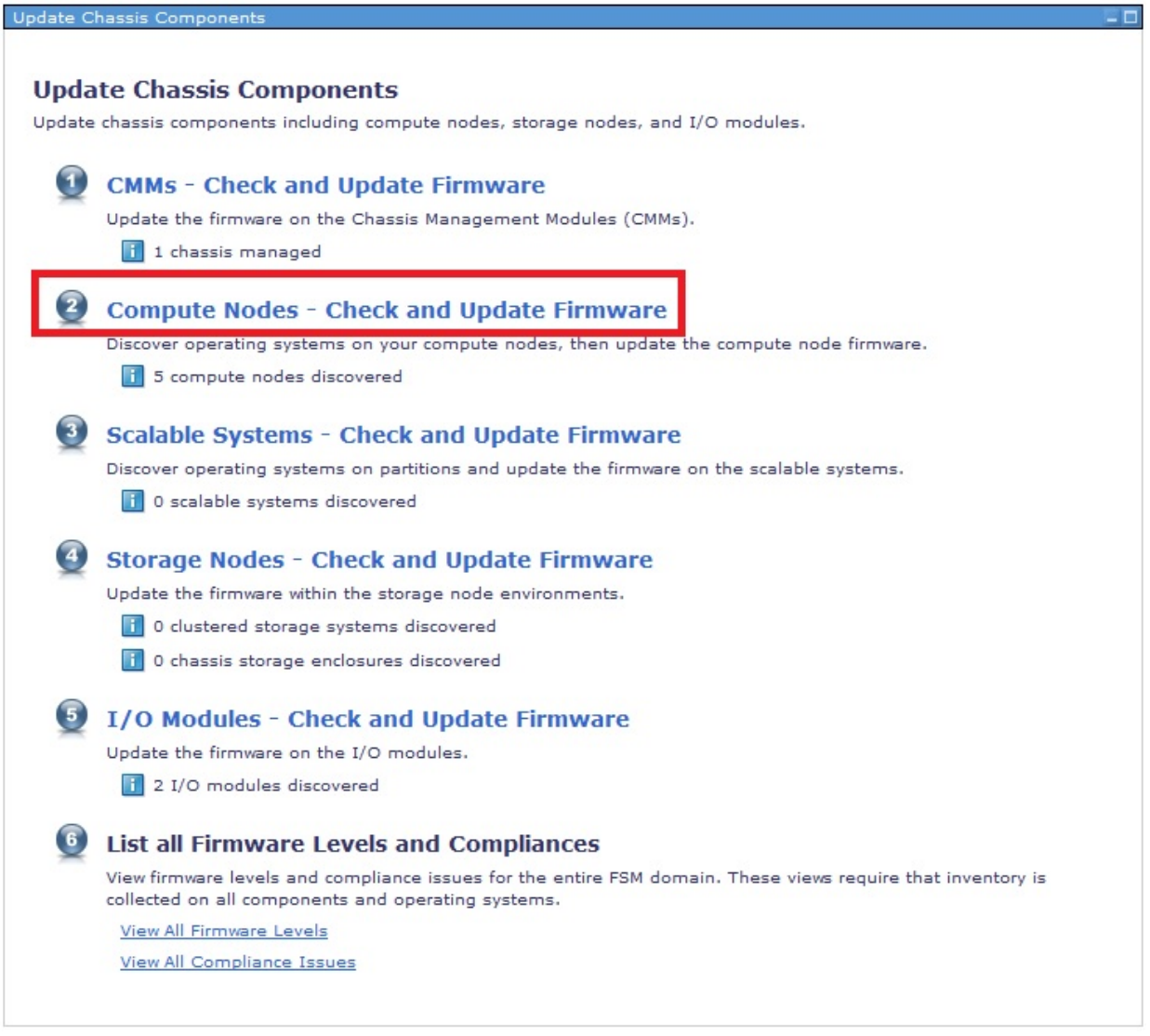
Make sure that you have read all prerequisites, which are listed in 2.2, “Prerequisites,” on page 21. In addition, make sure that you have performed the procedures described in 2.3, “Preparing for updates,” on page 25.

Procedure

Complete the following steps to install updates for X-Architecture compute nodes:

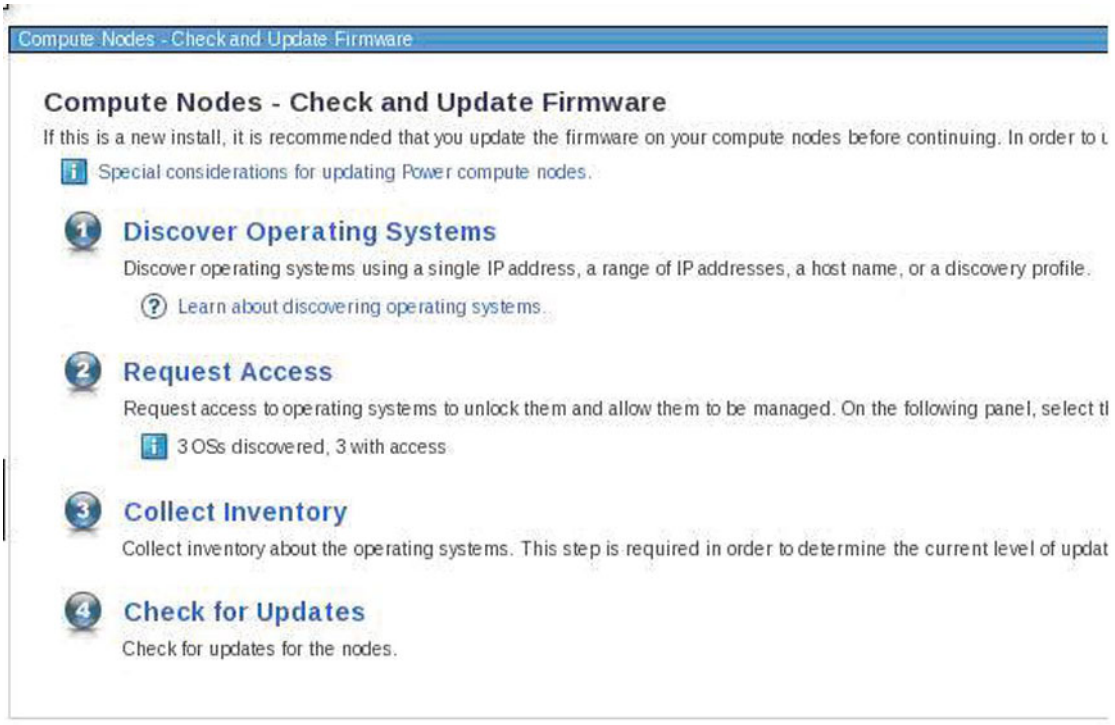
1. From the IBM FSM home page, click the **Initial Setup** tab.
2. Click **Update Chassis Components**; then click **Compute nodes - Check and Update Firmware** >

   Note: If you are updating the firmware for a multi-node system (also called a scalable system), such as the Flex System x280 X6, x480 X6, or x880 X6 Compute Node, click **Scalable Systems - Check and Update Firmware**.



For X-Architecture compute nodes, there are four steps required for checking and updating firmware:

a. Discover operating systems
b. Request access to all operating systems
c. Collect inventory for the operating systems
d. Check for updates



If you discovered the operating systems as they were installed and collected inventory on the chassis components (see 2.3.1, “Making sure that the IBM FSM is managing the chassis,” on page 25), the operating systems should already be discovered for the X-Architecture compute nodes that you will be updating. In addition, the IBM FSM should have full access to those operating systems. Therefore, you can skip to 

.
If you need to discover the operating systems or request full access to the compute nodes, you can click 

, and 

. Otherwise, proceed with 

.

Tip: The update task is referred to as a job task. If you are not familiar with job tasks in the IBM FSM, see A.1, “Starting a job task,” on page 155.
.

After the collect inventory job has completed, click 

, which will open the Acquire Updates wizard.

3. Acquire the updates.

Note: If Microsoft Windows 2012 is installed on any of the compute nodes, you cannot acquire those updates through the IBM FSM even if it is connected to the Internet. Therefore, you will need to follow the steps for updating X-Architecture compute nodes from an IBM FSM that is not connected

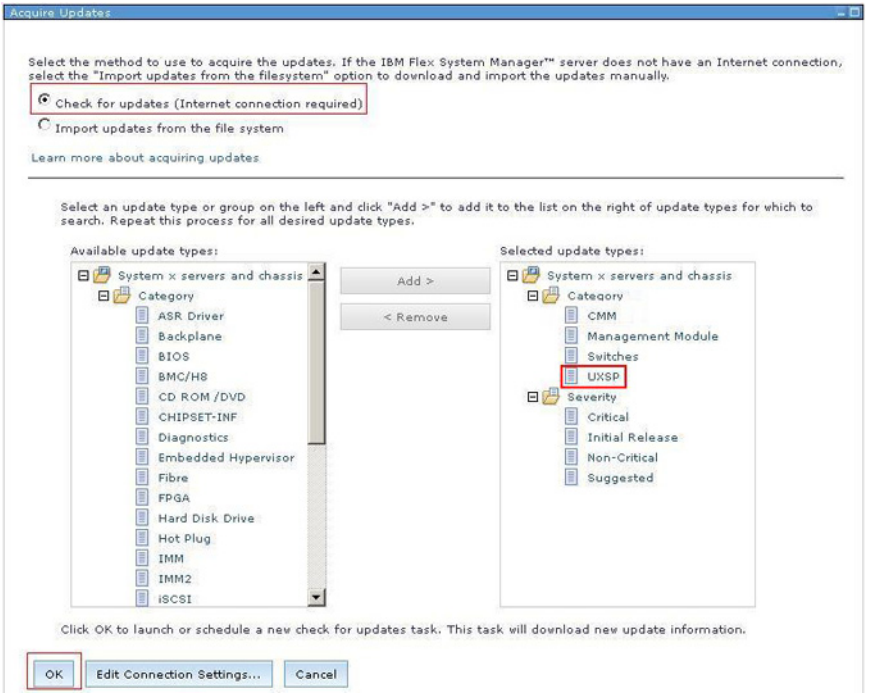
to the Internet. See Chapter 3, “Updating firmware from an FSM that is not connected to the Internet,” on page 63. Specific details for X-Architecture compute nodes are available at 3.8.3, “Updating X-Architecture compute nodes,” on page 104.

Important consideration

If Platform Agent is installed on a compute node, you must update the Platform Agent on that compute node before you update the firmware for that compute node.

a. From the Acquire Updates page, select **Check for updates (Internet connection required)**. Make sure that the UXSP is listed in the Selected update types field and click **OK**.

   Note: In addition to the UXSP, you can also select **Individual updates** from the category list that is on the left; for example, Diagnostics, IMM2. Then, click the **Add** button to add them to the selected updates.



b. From the Schedule tab on the Launch Job window, select **Run Now**.

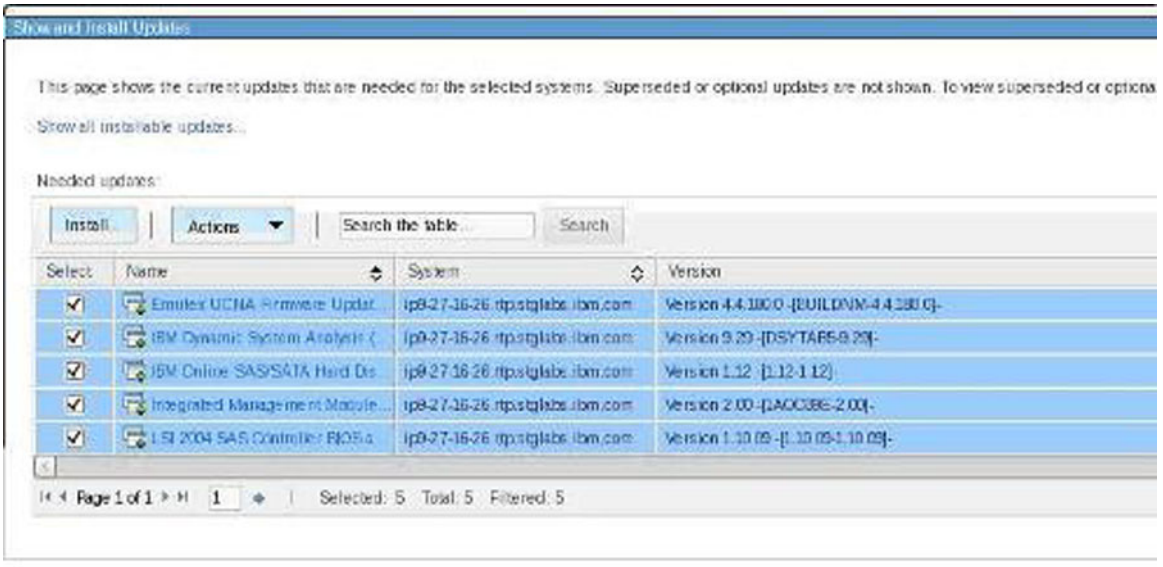
c. From the message confirming that the job was created and started successfully, click **Display Properties** to monitor the job status (displays the Active and Scheduled Jobs page).

d. After the update has been imported successfully, close the **Active and Scheduled Jobs** page.

4. Install the updates

   a. When the acquire task has completed, click **Show and Install Updates**.

b. Select the updates to apply to the X-Architecture compute nodes, and then click **Install** to start the Install wizard.



Select all the updates by selecting **Actions** > **Select All**. Then click **Install** to start the Install Wizard.

Tip: Consider selecting the option **Automatically restart as needed during installation**.

Note: If you are updating a compute node running ESXi and the host is not fully initialized, you might see an error stating that the system failed to restart, and that it must be restarted manually even if you chose **Automatically restart as needed during installation**. In you see this error, restart the compute node (if there are no other errors listed, the firmware update was successful).

c. Proceed to summary screen which summarizes the updates that will be installed. Click **Finish**.
d. In the Launch Job window, go to the Schedule tab and select **Run Now**. Then click **OK**.

Tip: The update task is referred to as a job task. If you are not familiar with job tasks in the IBM FSM, see A.1, “Starting a job task,” on page 155.

What to do next

You can verify the update completed successfully by looking in the Task Log Steps and verifying that each step completed with status Complete. For information about validating that the job completed successfully, see A.4, “Verifying an update completed successfully,” on page 161.

2.6.3.3 Determining which specific updates need to be installed

When you imported an UXSP update, the IBM FSM will show that the UXSP update needs to be installed, but it does not list the individual updates (such as IMM, UEFI, or pDSA) that are needed from the UXSP package.

Procedure

To determine the individual updates that need to be applied for a compute node, complete the following steps:

1. From the Chassis Manager, click an X-Architecture compute node to select it.
2. In the Details section at the bottom of the panel, click **Actions** > **Related Resources** > **Update** > **Server Needs**.

   Tip: Not all updates, such as driver updates will show in this list. To select the full list of available updates, click **Actions** > **Release Management** > **Show and install updates**. Then click the link **Show all installable updates** to see a full list of updates that can be installed.
3. The Resource Explorer panel is displayed, which provides a list of the specific updates that need to be applied.

2.7 Updating storage nodes

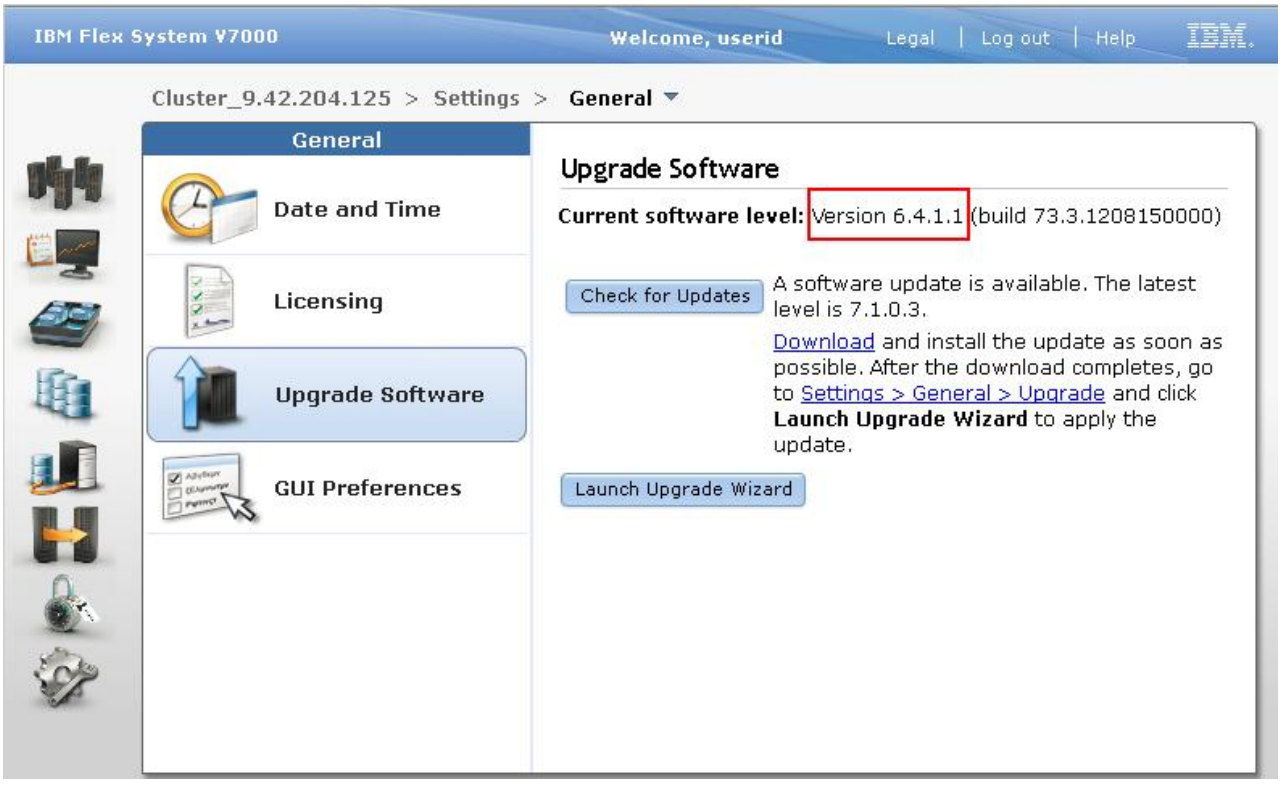
Use the IBM FSM to update the firmware and software for the IBM Flex System V7000 storage node.

Important Consideration:

Before you attempt to upgrade the Flex System V7000 storage node through the IBM FSM, you must check the version of firmware that is currently installed on the Flex System V7000 storage node.

- If the currently installed version is 6.4.1.x, you can update the Flex System V7000 storage node from the IBM FSM.
- If the currently installed version is 7.1.0.3 or greater, you can update the Flex System V7000 storage node from the IBM FSM.
- If the currently installed version is 7.1.0.x (and not 7.1.0.3), do not upgrade the Flex System V7000 storage node from the IBM FSM. Instead, follow the procedures listed in 4.4, "Updating Flex System V7000 Storage Nodes," on page 130.

To determine what version is installed, log in to the cluster management interface from the CMM. From the Flex System V7000 home page, click **Settings** > **General** to see the version number.



For more information about setting up the IBM Flex System V7000 storage node from the IBM FSM, see the following website:

http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.4939.doc/site_qicfgsys_FSM.html

For more information about managing an IBM Flex System V7000 storage node manually, see the following website:

http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/managing_flex_system_v7000_manually.html

2.7.1 Installing a storage node update

Follow the steps in this procedure to update the storage node.

Procedure

Complete the following steps for ***each*** storage node:

1. From the Chassis Manager, select the storage node.
2. Collect inventory on the selected storage node. Under Common Actions, select **Inventory** > **Collect Inventory**.

   Tip: Collecting inventory is a job task. If you are not familiar with job tasks in the IBM FSM, see A.1, "Starting a job task," on page 155.
3. Acquire the updates to be applied. Select **Release Management** > **Acquire Updates**.
4. Install the update on the storage node by selecting action **Release Management** > **Show and Install Updates** and run the Install Updates task.

   Tip: The update task is referred to as a job task. If you are not familiar with job tasks in the IBM FSM, see A.1, "Starting a job task," on page 155.
   .

What to do next

You can verify the update completed successfully by looking in the Task Log Steps and verifying that each step completed with status Complete. For information about validating that the job completed successfully, see A.4, "Verifying an update completed successfully," on page 161.

Important consideration:

Additional updates, such as hard disk drive updates can be applied to the IBM Flex System V7000 storage node, but these updates are not applied through the IBM FSM update process.

2.7.2 Obtaining additional updates for the IBM Flex System V7000 storage node

Additional updates, such as hard disk drive updates can be applied to the IBM Flex System V7000 storage node but these updates are not applied through the IBM FSM update process.

Procedure

Additional storage node updates can be found by completing the following steps:

1. Open a Web browser and navigate to the IBM Fix Central website: http://www.ibm.com/support/fixcentral/
2. In the Product Group field, select **Software** > **PureSystems** > **PureFlex System** > **Storage Node**. Then select **Flex System V7000** for the storage node and click **Continue**.
3. In Installed Version field, select **All**.
4. In Platform field select **All**; then click **Continue**.
5. Select each of the updates to be applied; then click **Continue**.
6. Sign in with your IBM ID and download the updates. Follow the directions provided in the documentation that is available with the updates to apply them to the storage node.

What to do next

Third-Party host software updates are installed on third party systems, such as Microsoft Windows Server and are not installed directly on or by the IBM FSM or the IBM Flex System V7000 Storage Node.

The IBM FSM does not support updating hard disk drives on Flex System V7000 storage nodes. Information about updating hard disk drives is available at the following website:

http://pic.dhe.ibm.com/infocenter/flexsys/information/index.jsp?topic=%2Fcom.ibm.acc.4939.doc%2Ftbrd_upgradedrivefirmware.html

2.8 Updating I/O modules

Use the IBM FSM to update the I/O modules, which includes both switches and pass-thru modules.

Important considerations:

- When updating an I/O module using the IBM FSM, do not perform configure, update, or perform SNMP operations with the CMM while the update is occurring. Otherwise, the firmware update might not be successful.
- If you use IPv4 and IPv6 for the management node Eth0 (management network interface), each managed chassis and chassis component must have an IPv4 address.
- You cannot update the firmware for the Flex System EN4023 10Gb Scalable Switch through the IBM FSM. Instead, you must use the switch interface to update firmware. More information about updating the firmware is available in the User's Guide provided for the Flex System EN4023 10Gb Scalable Switch:

  http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.networkdevices.doc/Io_module_en4023.html
- If you are attempting to update the firmware for the IB6131 Infiniband Switch or the EN4061 40Gb Ethernet Swtich, see 7.29, “IBM FSM fails to update IB6131 and EN6131 switches,” on page 154.
- The following considerations apply to the Flex System CN4093 10Gb Converged Scalable Switch, the Flex System Fabric EN4093/EN4093R 10Gb Scalable Switches, and the Flex System EN2092 1Gb Ethernet Scalable Switch:
  - If you are updating I/O modules that currently have firmware level of **version 7.7.5.0 or later** installed, you can use a Secure File Transfer Protocol (SFTP) server provided with the IBM FSM to update the firmware from the IBM FSM. Otherwise, if you update these switches through the IBM FSM, you must use a Trivial File Transfer Protocol (TFTP) server to host updates before they are applied to these switches.

    As an alternative to setting up a TFTP server and enabling the menu-based CLI on the I/O module, you can consider updating the firmware for I/O modules directly, which can be done through the Web-based user interface for the I/O module and does not require a TFTP server. In general, if you are updating several I/O modules, consider setting up a TFTP server. To update the firmware for one or two I/O modules, consider updating it directly through the I/O module Web-based user interface.

    For information about checking the firmware level of an I/O module or for information about updating the firmware directly through the I/O module interface, see the product documentation that is provided with the I/O module. You can obtain the documentation for I/O modules at this website:

    http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.networkdevices.doc/network_iomodule.html
  - The switches must be configured to use the menu-based CLI (ibmnos-cli), which is the default command-line interface. If the switch does not use the menu-based CLI, updates from the IBM FSM will fail.

Tip: You can configure switches so that the CLI mode is determined when an administrator logs in. This way, you do not have to set the CLI mode and restart the switch every time you want to change the mode from iscli to ibm-nos-cli. To configure switches so that the CLI mode is determined upon log in:

1. Start an SSH session to log in to the switch.
2. Run the following commands from the ISCLI:

   ```
   enable
   config t
   boot cli-mode prompt
   ```

   From the ibmnos-cli, run the following command:

   ```
   boot/prompt e
   ```
3. Log out of the SSH session. The next administrative user to log in sets the mode, which stays in effect until all users log out.

When updating the I/O module firmware, the IBM FSM will use the correct CLI mode.

– Additional CN4093-only considerations:
  - Before updating the firmware for the Flex System Fabric CN4093 10Gb Converged Scalable Switch through the Web interface, make sure that you use the following ISCLI command to save the startup configuration:

    ```
    copy running-config startup-config
    ```

    This will ensure that the settings remain in effect after you apply the firmware updates and restart the switch.
  - Do not perform any switch configuration actions while a CN4093 firmware update is in progress.
  - Immediately after updating the firmware for the CN4093, make sure that you configure the switch to use ISCLI to prevent storage configuration losses:
    1. Start an SSH session to log in to the switch.
    2. Choose iscli mode.
    3. Run the following commands from the ISCLI:

       ```
       enable
       config t
       boot cli-mode iscli
       ```
    4. Log out of the SSH session.

- Flex System FC3171 8 Gb SAN switches **must** be running CPLD version 0x22 or later. Switches with firmware levels of 9.1.0.26.00 and later will show the following error messages if the CPLD was not updated:

  ```
  Installed CPLD version 0x20 older than available version 0x22. See 'help cpld install'
  in the CLI for upgrade instructions.
  ```

  Complete the following steps to update the CPLD, which will require a virtual switch restart.
  1. Update the firmware level on the switch to 9.1.0.27.00 or later and restart the switch.
  2. Log in to the CLI and run the following commands:

     ```
     admin start
     set advanced on
     cpld install
     ```
  3. When CPLD install completes successfully, login to the CMM CLI and run these commands to perform a virtual reseat of the switch:

     ```
     env -T system:switch[x], where x is switch slot
     service -vr
     ```
  4. Verify the CPLD version after the virtual reseat. Run the following commands from the switch CLI:

     ```
     set advanced on
     show setup mfg
     ```

     Look for the line CPLD Revision, which should end in 0x22.

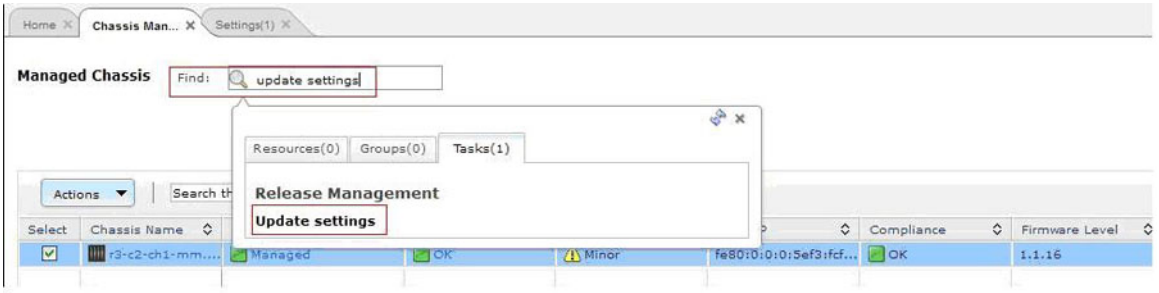
2.8.1 Configuring a TFTP server

If you are updating the firmware for the Flex System CN4093 10Gb Converged Scalable Switch, the Flex System Fabric EN4093/EN4093R 10Gb Scalable Switches, or the Flex System EN2092 1Gb Ethernet Scalable Switch, check the firmware level before updating. If the firmware level currently installed on the I/O module is less than **version 7.7.5.0**, you must use a Trivial File Transfer Protocol (TFTP) server to host updates before they are applied to these switches.

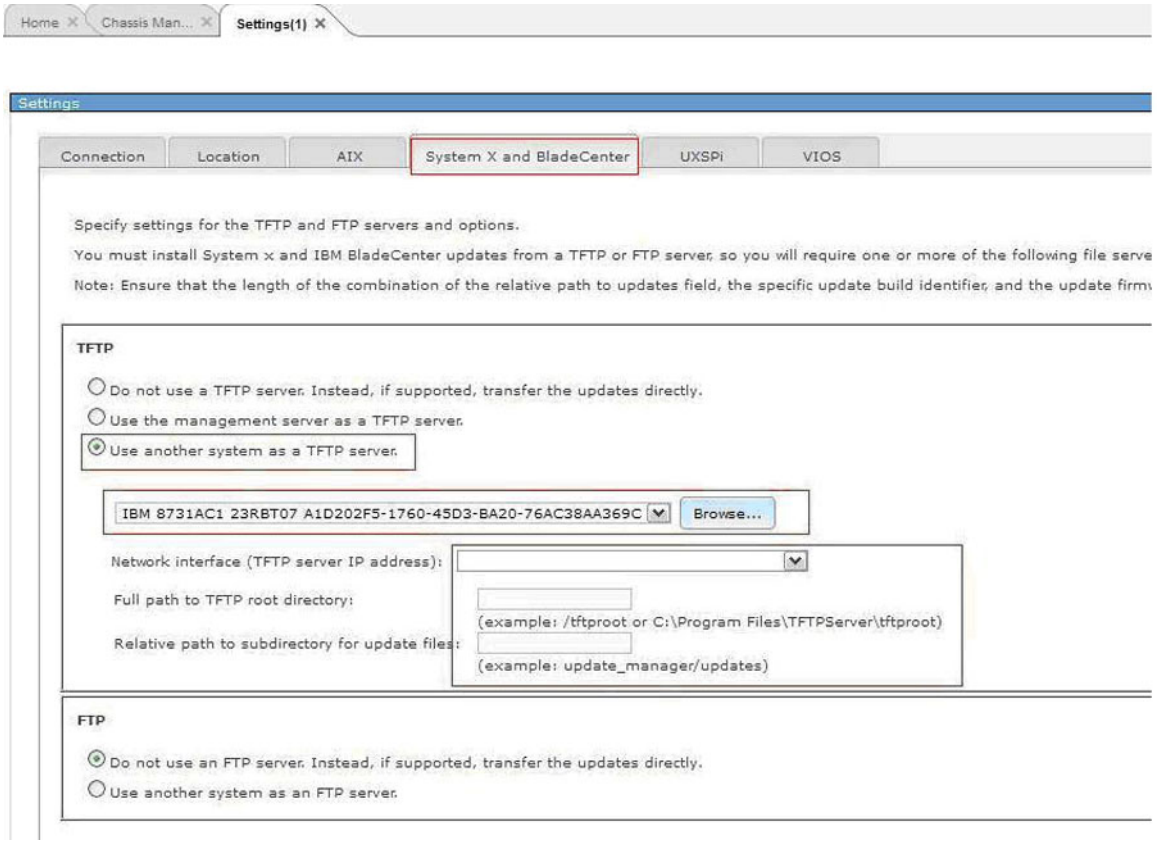
Note: If you install a TFTP on a Power Systems VIOS, make sure that you also install an unzip utility for use when applying updates.

After setting up the TFTP server, configure the IBM FSM to reference the TFTP server:

1. Enter `Update settings` in the Find field from the Chassis Manager tab and click the **Update settings** link under Release Management:



2. On the Settings page, select the **System X and BladeCenter** tab. Then select **Use another system as a TFTP server** and browse for the managed compute node that has the TFTP server installed as shown in this example:



2.8.2 Installing I/O module updates

Perform these steps to update the firmware for I/O modules. Make sure that you perform these steps for **each** I/O module.

About this task

Important consideration:

When updating the firmware for I/O modules, make sure that you update each I/O module sequentially to ensure that you do not lose network connectivity.

Procedure

Complete the following steps to install updates for **each** I/O module:

1. From the Chassis Manager, click the I/O module in the chassis. If you have previously set up full access to the I/O module through the IBM FSM and collected inventory, proceed with Step 4
2. Make sure that the IBM FSM has full access to the I/O module:
   a. In the Details section at the bottom of the Chassis Manager, click **Actions** > **Security** > **Request Access**.
   b. Enter the User ID and credentials to gain access to the I/O module.
   c. Click **Request Access**.

   If you need to request access to I/O modules, see the *Getting full access to Ethernet I/O modules* and *Getting full access to Fibre Channel I/O modules* quick start guides, which are available at the following website:

   http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.commontasks.doc/commontasks_chassis_config.html
3. Perform an inventory of the I/O module:
   a. In the Details section at the bottom of the Chassis Manager, click **Actions** > **Inventory** > **Collect Inventory**
   b. Make sure that **Run Now** is selected; then click **OK**.

   Tip: Collecting inventory is referred to as a job task. If you are not familiar with job tasks in the IBM FSM, see A.1, “Starting a job task,” on page 155.
4. In the Details section at the bottom of the Chassis Manager, click **Actions** > **Release Management** > **Acquire Updates** to start the Acquire Updates wizard.
5. Apply the update. From the Details section at the bottom of the Chassis Manager, click **Actions** > **Release Management** > **Show and install updates** to continue.
6. Select the updates to apply to the I/O module and click **Install**.
7. Proceed to summary screen which summarizes the updates that will be installed. Click **Finish** to start the process of updating the I/O module.

   Tip: The update task is referred to as a job task. If you are not familiar with job tasks in the IBM FSM, see A.1, “Starting a job task,” on page 155.

What to do next

You can verify the update completed successfully by looking in the Task Log Steps and verifying that each step completed with status Complete. For information about validating that the job completed successfully, see A.4, “Verifying an update completed successfully,” on page 161.

After you have updated all I/O modules, you can then update the following components if they are part of your configuration:

- IBM Storwize V7000. See Chapter 5, “Updating the IBM Storwize V7000,” on page 133.
- Top-of-rack switches. See Chapter 6, “Updating Top-of-Rack (TOR) switches,” on page 135.

Chapter 3. Updating firmware from an FSM that is not connected to the Internet

If the IBM FSM is not connected to the Internet, you must obtain the updates from the IBM Website, copy those updates to the IBM FSM, and import those updates into the IBM FSM updates library before installing the update for the chassis components.

Important Considerations

- Use this document to upgrade firmware if the IBM FSM that you have installed is currently at version 1.3.0 or higher. If the IBM FSM version is earlier than 1.3.0, make sure that you review 1.1, "Upgrading from an earlier version of Flex System firmware," on page 3.
- If you did not previously follow the steps to update the IBM FSM to version 1.3.1.1 (to resolve the OpenSSL Heartbleed vulnerability), apply the updates for version 1.3.2 to the IBM FSM and all components in all managed chassis. Then, from the IBM FSM, replace the TLS certificate and private key for the IBM FSM user registry, and change passwords according to the Remediation/Fixes section of the Security Bulletin referenced below:

  http://www.ibm.com/support/entry/portal/docdisplay?lndocid=MIGR-5095202
- If the Flexible Service Process (FSP) firmware on the Power Systems compute nodes installed in your chassis is earlier than the December, 2012 release (AF763_043), you must update the FSP firmware on the Power Systems compute nodes before updating the CMM. Follow the update procedure listed in 2.1.1, "Steps to update for Power Systems compute nodes running FSP firmware versions earlier than AF763_043," on page 19.
- IBM FSM does not support updating x440 M5 (MT 7167, 2590) and x240 M5 (MT 9532, 2588) ITEs. As an alternative, you can use the UpdateXpress System Packs (UXSPs) and the UpdateXpress System Pack Installer (UXSPI) to update these ITEs as described in 4.3, "Updating X-Architecture compute nodes," on page 124.

  Note: Lenovo UXSPI supports the updating of x440 M5 (MT 7167, 2590) and x240 M5 (MT 9532, 2588) ITEs.
- IBM FSM version 1.3.3 manages both IBM and Lenovo manufactured System x and BladeCenter. Lenovo System x and BladeCenter have their own firmware updates, therefore, use Lenovo UXSPi to update both Lenovo system x and BladeCenter. Ensure that you manually import the latest version of IBM UXSPi to update when the target system is IBM System x or IBM BladeCenter. If the targeted systems are manufactured by Lenevo, then manually import the latest version of Lenovo UXSPi to update the systems.

  Note: Use the latest IBM UXSPi to update firmware for FSM management server.

3.1 Steps to update from an IBM FSM that is not connected to the Internet

Make sure that you review the steps in this table carefully before you begin updating the firmware for IBM Flex System or IBM PureFlex system components using the IBM FSM.

Important considerations:

Before you begin updating the components:

- Make sure that you verify the part number of the fan logic modules in your chassis and replace them if necessary.

  ECA083 (Engineering Change Announcement) provides for proactive replacement of the fan logic module in a limited number of IBM PureFlex systems. Details of this announcement and instructions for determining the part number of installed fan logic modules are available at the following location:

  http://www.ibm.com/support/entry/portal/docdisplay?lndocid=MIGR-5093506
- Make sure that the IBM FSM is managing the chassis, all components are accessible from the IBM FSM, and a full inventory has been performed for all components (including operating systems). See 2.3.1, “Making sure that the IBM FSM is managing the chassis,” on page 25.
- Perform a backup of the IBM FSM. See 2.3.2, “Backing up the IBM FSM,” on page 29.
- Acquire the firmware updates from the IBM PureSystems Centre website, copy the updates to the IBM FSM, and load them into the IBM FSM updates library before you begin. You can obtain the updates from:

  http://www.ibm.com/software/brandcatalog/puresystems/centre/

  See 3.4, “Obtaining all updates,” on page 79 for information about obtaining updates and copying them to the IBM FSM.
- If you are updating firmware for Power Systems compute nodes running FSP firmware 01AF773, you must update the Flexible Service Processor (FSP) for Power Systems compute node to 01AF773_058 before you begin ghe uupdate the CMM. See 3.1.2, “Steps to update for Power Systems compute nodes running FSP firmware version 01AF773,” on page 69 for the update order to follow in this case.

The following table enumerates the high level steps with the corresponding section required to update IBM Flex System or IBM PureFlex system components using the IBM FSM. Follow the detailed instructions in each section as you update.

Table 4. High-level steps to update components.

Note: The total amount of time required to update a system depends on the number of devices in system (one chassis versus multiple chassis) and the configuration of the system (virtualized environments versus non-virtualized environments

Step	Activity	How much time does it take?	Is a restart required?	More information
1	**Update the IBM FSM** 1. Copy the update to the IBM FSM. 2. Import the update into the IBM FSM updates library. 3. Apply the update to the IBM FSM. After updating the IBM FSM, restart the IBM FSM to have the changes take effect. **Tip:** After restarting the IBM FSM, make sure that you clear the cache for your browser before accessing the IBM FSM Web interface. **Important consideration:** If the IMM firmware level on the X-Architecture compute nodes installed in your chassis is earlier than the December, 2012 release (v1.60, build 1AOO32P), install the updates for the X-Architecture compute nodes before you enable centralized user management on the IBM FSM. For more information about centralized user management through the IBM FSM, see the following website: http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/centralized_user_management.html	2 hours per IBM FSM	Yes	3.5, "Updating the IBM FSM when the IBM FSM is not connected to the Internet," on page 87
2	**Update the CMM** After updating the CMM, restart the CMM to have the changes take effect. **Important considerations:** If you are updating firmware for Power Systems compute nodes running FSP firmware that is earlier than the December, 2012 release (AF763_043), you must update the Flexible Service Processor (FSP) for Power Systems compute node before you update the CMM. See 3.1.1, "Steps to update for Power Systems compute nodes running FSP firmware versions earlier than AF763_043," on page 68 for the update order to follow in this case. Updating older version FSPs after updating the CMM might leave your compute nodes unusable (in a status 'pending' condition). If this happens, see 7.9, "Power Systems compute node remains at a status pending state after an update," on page 142.	30 minutes per CMM	Yes	3.7, "Updating the CMM," on page 93

Table 4. High-level steps to update components (continued).

Note: The total amount of time required to update a system depends on the number of devices in system (one chassis versus multiple chassis) and the configuration of the system (virtualized environments versus non-virtualized environments

Step	Activity	How much time does it take?	Is a restart required?	More information
3	**Update Power Systems compute nodes** The firmware update for a Power Systems compute node can be applied even if the operating system has not been discovered by the FSM. However, you need to discover the Power Systems operating system to update the network adapters and the hard disk drives. See 3.8.1, "Discovering operating systems from the IBM FSM," on page 96. Updating older version FSPs after updating the CMM might leave your compute nodes unusable (in a status 'pending' condition). If this happens, see 7.9, "Power Systems compute node remains at a status pending state after an update," on page 142. **Important consideration:** If you are updating firmware for Power Systems compute nodes running FSP firmware that is earlier than the December, 2012 release (AF763_043), you must update the Flexible Service Processor (FSP) for Power Systems compute node before you update the CMM. See 3.1.1, "Steps to update for Power Systems compute nodes running FSP firmware versions earlier than AF763_043," on page 68 for the update order to follow in this case.	1 hour to 3 hours per compute node **Note:** • The amount of time required for an update depends on the operating system that is installed and whether you are running in a virtualized environment (you are moving VMs between compute nodes as you perform updates). • You can perform all compute nodes updates concurrently, which will reduce the overall amount of time needed for updating the entire system.	Yes **Note:** If you are updating only the firmware for the FSP and not changing the release version, a restart is not required. A restart is required if you are updating the firmware for adapters or hard disk drives.	3.8.2, "Updating Power Systems compute nodes," on page 97

Table 4. High-level steps to update components (continued).

Note: The total amount of time required to update a system depends on the number of devices in system (one chassis versus multiple chassis) and the configuration of the system (virtualized environments versus non-virtualized environments

Step	Activity	How much time does it take?	Is a restart required?	More information
4	**Update X-Architecture compute nodes** The operating system must be discovered by the IBM FSM before updating the firmware (see 3.8.1, "Discovering operating systems from the IBM FSM," on page 96). VMware ESXi update considerations are described in 3.8.3.1, "VMware ESXi update considerations," on page 106 After updating the compute node, you must restart it for the updates to take effect.	1.5 hours to 3.5 hours per compute node **Note:** • The amount of time required for an update depends on the operating system that is installed and whether you are running in a virtualized environment (you are moving VMs between compute nodes as you perform updates). • You can perform all compute nodes updates concurrently, which will reduce the overall amount of time needed for updating the entire system.	Yes **Note:** If you are updating only the IMM and pDSA firmware for the X-Architecture compute node, you do not need to restart the compute node to apply the updates.	3.8.3, "Updating X-Architecture compute nodes," on page 104
5	**Update IBM Flex System V7000 storage nodes** Some updates, such as hard disk drive updates cannot be applied through the IBM FSM. See 3.9.2, "Obtaining additional updates for the IBM Flex System V7000 storage node," on page 116 After updating the storage node, you must restart it for the updates to take effect.	1 hour	Yes	3.9, "Updating storage nodes," on page 113
6	**Update I/O modules** Make sure that you update I/O modules sequentially, restarting each I/O module and ensuring that it is functioning before updating the next I/O module. If you update the I/O module through the IBM FSM, you will need to install a TFTP server and enable the menu-based CLI on the I/O module. **Tip:** To update a single I/O module, consider updating it directly through the Web interface for the I/O module.	1 hour	Yes	3.10, "Updating I/O modules," on page 116

Table 4. High-level steps to update components (continued).

Note: The total amount of time required to update a system depends on the number of devices in system (one chassis versus multiple chassis) and the configuration of the system (virtualized environments versus non-virtualized environments

Step	Activity	How much time does it take?	Is a restart required?	More information
7	**Update IBM Storwize V7000 devices** Firmware updates to the IBM Storwize V7000 must be done through the IBM Storwize V7000 interface.	1 hour	Yes	Chapter 5, "Updating the IBM Storwize V7000," on page 133
8	**Update top-of-rack switches** Firmware updates to top-of-rack switches must be done directly through the switch interface.	1 hour	Yes	Chapter 6, "Updating Top-of-Rack (TOR) switches," on page 135

If you have issues during the update process, see Chapter 7, "Troubleshooting update issues," on page 137 to resolve those issues.

3.1.1 Steps to update for Power Systems compute nodes running FSP firmware versions earlier than AF763_043

If the Flexible Service Process (FSP) firmware on the Power Systems compute nodes installed in your chassis is earlier than the December, 2012 release (AF763_043), you must update the FSP firmware on the Power Systems compute nodes before updating the CMM.

Note: Updates can be applied to an active, running system. However, typically the system needs to be restarted for updates to take effect.

Updates must be applied in the following order:

1. IBM Flex System Manager (FSM)

   Important consideration:

   Before updating the IBM FSM management node, create a backup image of the IBM FSM. For information about backing up the IBM FSM, see 3.3.2, "Backing up the IBM FSM," on page 78.
2. Service processor on each Power Systems compute node that is currently running firmware version earlier than AF763_043

   You must update the firmware for the Flexible Service Processor (FSP) ***before*** you update the firmware for the CMM. The updates for the adapters and hard drives installed in a Power Systems compute node can be installed later in the update process.

   Updating older version FSPs after updating the CMM might leave your compute nodes unusable (in a status 'pending' condition). If this happens, see 7.9, "Power Systems compute node remains at a status pending state after an update," on page 142.
3. Chassis Management Module (CMM)
4. Network adapters and hard drives for the Power Systems compute nodes
5. X-Architecture compute nodes

   If the IMM firmware level on the X-Architecture compute nodes installed in your chassis is earlier than the December, 2012 release (v1.60, build 1AOO32P), install the updates for the X-Architecture compute nodes before you enable centralized user management on the IBM FSM.

   For more information about centralized user management through the IBM FSM, see the following website:

   http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/centralized_user_management.html

6. IBM Flex System V7000 Storage Node
7. I/O modules

Depending on your configuration, you might also need to update the following components. These components must be updated directly; you cannot update them through the IBM FSM.

1. IBM Storwize V7000
2. Top-of-rack switches

3.1.2 Steps to update for Power Systems compute nodes running FSP firmware version 01AF773

If the Flexible Service Process (FSP) firmware on the Power Systems compute nodes installed in your chassis is version 01AF773, you must update the FSP firmware on the Power Systems compute nodes to 01AF773_058 before updating to 01AF783 (Flex Version 1.3.2).

Note: Updates can be applied to an active, running system. However, typically the system needs to be restarted for updates to take effect.

Updates must be applied in the following order:

1. Power Systems Flexible Service Processor (FSP) firmware. Update the FSP firmware to level 01AF773_058.
2. IBM Flex System Manager (FSM)

   Important consideration:

   Before updating the IBM FSM management node, create a backup image of the IBM FSM. For information about backing up the IBM FSM, see 2.3.2, “Backing up the IBM FSM,” on page 29.
3. Chassis Management Module (CMM)
4. Update the Power Systems firmware to 01AF783

   You must update the firmware for the Flexible Service Processor (FSP) ***before*** you update the firmware for the CMM. The updates for the adapters and hard drives installed in a Power Systems compute node can be installed later in the update process.

   Updating older version FSPs after updating the CMM might leave your compute nodes unusable (in a status 'pending' condition). If this happens, see 7.9, “Power Systems compute node remains at a status pending state after an update,” on page 142.
5. Network adapters and hard drives for the Power Systems compute nodes
6. X-Architecture compute nodes

   If the IMM firmware level on the X-Architecture compute nodes installed in your chassis is earlier than the December, 2012 release (v1.60, build 1AOO32P), install the updates for the X-Architecture compute nodes before you enable centralized user management on the IBM FSM.

   For more information about centralized user management through the IBM FSM, see the following website:

   http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/centralized_user_management.html
7. IBM Flex System V7000 Storage Node
8. I/O modules

Depending on your configuration, you might also need to update the following components. These components must be updated directly; you cannot update them through the IBM FSM.

1. IBM Storwize V7000
2. Top-of-rack switches

3.2 Prerequisites

Review the prerequisites before updating components in a chassis through the IBM FSM.

The following prerequisites must be met to update the components in a chassis through the IBM FSM:

- To update chassis components, the chassis and all components within the chassis must be managed by the IBM FSM. For information about managing components through the IBM FSM, see the following website:

  http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/managing_chassis.html

- If Platform Agent is installed on compute nodes, you must update the Platform Agent on each compute node before you update the firmware for that compute node.

  Note: If you installed Common Agent, you do not need to update the Common Agent before you update the firmware for the compute node.

  To obtain the Platform Agent for the operating system that is installed on the compute node and to add it to the IBM FSM updates library, see 3.4.1, "Downloading the IBM FSM updates," on page 81. Use the procedures described in the Readme for the Platform Agent update to update the Platform Agent for compute nodes.

- At a minimum, you must apply VMware vSphere ESXi 5.0.x/5.1.x/5.5.x with IBM Customization Patch 1.2 or later for each compute node running the IBM customized image.

  If you are running VMware vSphere ESXi 5.5.x (update 1) or earlier, you must apply both the Lenovo and the Independent Hardware Vendor (IHV) customization patches (Patch 1.2) on every compute node. If you are running VMware vSphere ESXi 5.5.x (update 2), you need not apply Patch 1.2.

  In addition to the IBM Customization Patch 1.2, make sure that you install one of the following updates to the VMware vSphere ESXi operating system:

  – If you are running VMware vSphere ESXi 5.0, make sure that you install update 5.0u2 (update 2)
  – If you are running VMware vSphere ESXi 5.1, make sure that you install update 5.1u1 (update 1)
  – VMware vSphere ESXi 5.5.x

  When you install an IMM update on an X-Architecture compute node, the Integrated Management Module (IMM) is reset, which can cause a VMware vSphere ESXi system failure (host purple diagnostic screen) if you attempt to update an X-Architecture compute node on which the minimum level of VMware is not installed (5.0u2, 5.1u1, or 5.5.x).

  For information about obtaining the IBM Customization Patch 1.2, see the following location:

  http://www.ibm.com/support/entry/portal/docdisplay?lndocid=MIGR-5092679

  Make sure that you review the information provided in the readme for the patch. It contains instructions for installing the patch on a compute node.

- Make sure that SCP is installed on the Power Systems compute nodes before running Discovery or Inventory Collection from the IBM FSM so that the network adapters are discovered and inventoried by the IBM FSM. For more information about installing SCP, which is available with the OpenSSH software tools, see the following website:

  http://pic.dhe.ibm.com/infocenter/aix/v7r1/topic/com.ibm.aix.security/doc/security/openssh_kerberosv5.htm

- Compute nodes must have an operating system installed. The operating system must have a network IP address and the operating system must have been discovered by the IBM FSM. For information about installing operating systems on X-Architecture compute nodes, see the following websites:

  – Using the Deploy Images task from the IBM FSM:

    http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/deploying_compute_node_images.html

  – Quick Start Guides:

http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.commontasks.doc/commontasks_install_os.html

– Update considerations regarding a specific operating system, such as the requirement for 32-bit compatibility libraries when running the 64-bit Linux operating system:

  http://pic.dhe.ibm.com/infocenter/flexsys/information/index.jsp?topic=%2Fcom.ibm.acc.8731.doc%2Fcom.ibm.director.updates.helps.doc%2Ffqm0_c_um_platform_extensions.html

Note: The firmware update for a Power Systems compute node can be applied even if the operating system has not been discovered by the FSM. However, you need to discover the Power Systems operating system to update the network adapters and the hard disk drives.

- The IBM FSM must have full access to any component that is being updated, including discovered operating systems.

  Note: If you are updating X-Architecture compute nodes running Microsoft Windows 2012, see 3.2.1, "Enabling Windows Server 2012 systems for discovery," on page 72.

- The IBM FSM must perform at least one inventory collection on the component being managed. For information about collecting inventory, see the following website:

  http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/com.ibm.director.discovery.helps.doc/fqm0_t_performing_system_discovery.html

- The LAN-over-USB interface must be enabled for firmware updates on all X-Architecture compute nodes and for the IBM FSM.

  You can check that this is enabled by connecting to the CMM Web interface. Then:

  1. Navigate to **Chassis Management** > **Compute Nodes** to see a list of all compute nodes currently managed by the CMM.
  2. For ***each*** compute node:
     a. Click the compute node.
     b. Select the General tab.
     c. Make sure that **Enable Ethernet Over USB** is checked.

  Note: The LAN-over-USB interface should not be disabled on the IBM FSM but if it is, you must log in to the IMM user interface for the IBM FSM to check the setting and to change it. You cannot change the LAN-over-USB interface for the IBM FSM through the CMM interface. To check the LAN-over-USB setting for the IBM FSM, complete the following steps:

  1. Log in to the IMM Web interface for the IBM FSM.
  2. Select **IMM Management** > **Network**.
  3. From the USB tab, make sure that **Enable Ethernet over USB** is selected.

  In your operating system, you should also see a USB Ethernet interface. For more information about setting the LAN-over-USB interface through the operating system, see the following website (the procedure is the same for all X-Architecture compute nodes):

  http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.7917.doc/configuring_lan_over_usb_manually.html

  Tip: You do not need to configure a valid IP address to that interface for the update process to work.

  For more information about the IMM and LAN over USB, see the *IMMv2 User's Guide*, which is available at the following website:

  http://www.ibm.com/support/entry/portal/docdisplay?lndocid=MIGR-5086346

For more information about the IBM FSM, see the following website:

http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/getting_started.html

3.2.1 Enabling Windows Server 2012 systems for discovery

Remote registry administration must be enabled for the IBM FSM system discovery to run commands and run scripts on the managed system. The default setting for remote registry administration on Windows systems is enabled.

Procedure

Complete the following steps to verify or change the remote registry administration setting for ***each*** system that is running Windows Server 2012:

1. Log in to the Windows server.
2. Click the Server Manager icon.
3. Make sure that Windows Server 2012 can be discovered as a Windows Distributed Component Object Model (DCOM) protocol access end point by the IBM FSM:
   a. Click **Server Manager** > **Tools** > **Local Security Policy** > **Local Policies** > **Security options** > **Network access: Shares that can be accessed anonymously**.
   b. Right-click **Network access: Shares that can be accessed anonymously** and select **Properties**.
   c. In the **Network access: Shares that can be accessed anonymously** properties window, specify **Enabled** in the properties field.
4. Click **Tools** > **Services**.
5. In the list of services in the Services window, right-click the **Remote Registry** service and select **Properties** from the menu.
6. On the General page, set the Startup type to **Automatic**.
7. If the Service status is not started, click **Start** to start the service.
8. Click **OK** to apply the new settings and close the window.

   Refer to the following website for more information:

   http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/com.ibm.director.install.helps.doc/fqm0_t_preparing_windows_server_2012_managed_systems.html

   For considerations related to the discovery of other Microsoft Windows operating systems, see the following website:

   http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/com.ibm.director.install.helps.doc/fqm0_t_preparing_windows_managed_systems.html

3.2.2 Updating Linux firmware and drivers

If you are updating firmware and drivers for compute nodes that have Linux installed, make sure that you meet the prerequisites.

Firmware prerequisites

When updating firmware, the following prerequisites are required:

- If you are running a 64-bit version of Linux, make sure that the 32-bit compatibility libraries are installed (i.e. 32 bit libstdc++.so). For example, on RHEL 6, this is libstdc++-4.4.4.13.el6.i686.rpm.
- Updates require the Ncurses library (i.e. libncurses.so). For example, on RHEL 6, this is ncurses-libs-5.7-3.20090208.el6.i686.rpm.
- Make sure that the following commands are installed on each compute node that will receive the update (depending on the version of Linux that is installed):
  - zip
  - gunzip
  - rug (for SUSE Linux Enterprise Server 10 with the service pack)
  - zypper (for SUSE Linux Enterprise Server 11)
  - yum (for Red Hat Enterprise Linux versions 5.x and 6.x)

Driver prerequisites

Additionally, the following packages are required for installing Linux drivers from IBM update packages:

- /bin/sh
- /usr/bin/perl
- bash
- perl
- perl(Cwd)
- perl(Getopt::Long)
- perl(Getopt::Std)
- perl(strict)
- rpm-build
- rpm-libs
- rpmlib(CompressedFileNames) - must be version 3.0.4-1 or earlier
- rpmlib(PayloadFilesHavePrefix) - must be version 4.0-1 or earlier

3.3 Preparing for updates

Before updating the IBM FSM and all chassis components, make sure that the IBM FSM is managing the chassis, all chassis components have been discovered and inventoried, and that the IBM FSM is backed up.

3.3.1 Making sure that the IBM FSM is managing the chassis

If you have not already set up the IBM FSM to manage your chassis, complete the following steps to manage a chassis, discover the operating systems for all compute nodes, and gain full access to all resources being managed by the IBM FSM (also known as managed endpoints).

Before you begin

Remember that a chassis can be managed by only one IBM FSM at a time. Attempting to manage a chassis from multiple IBM FSM management nodes is not supported.

Important: The Flex System x222 compute node provides two separate compute nodes, upper and lower, in a single node bay. However, you will not be able to discover and manage both compute nodes until you have updated the software and firmware for the IBM FSM and CMM to Flex version 1.3.0 or later.

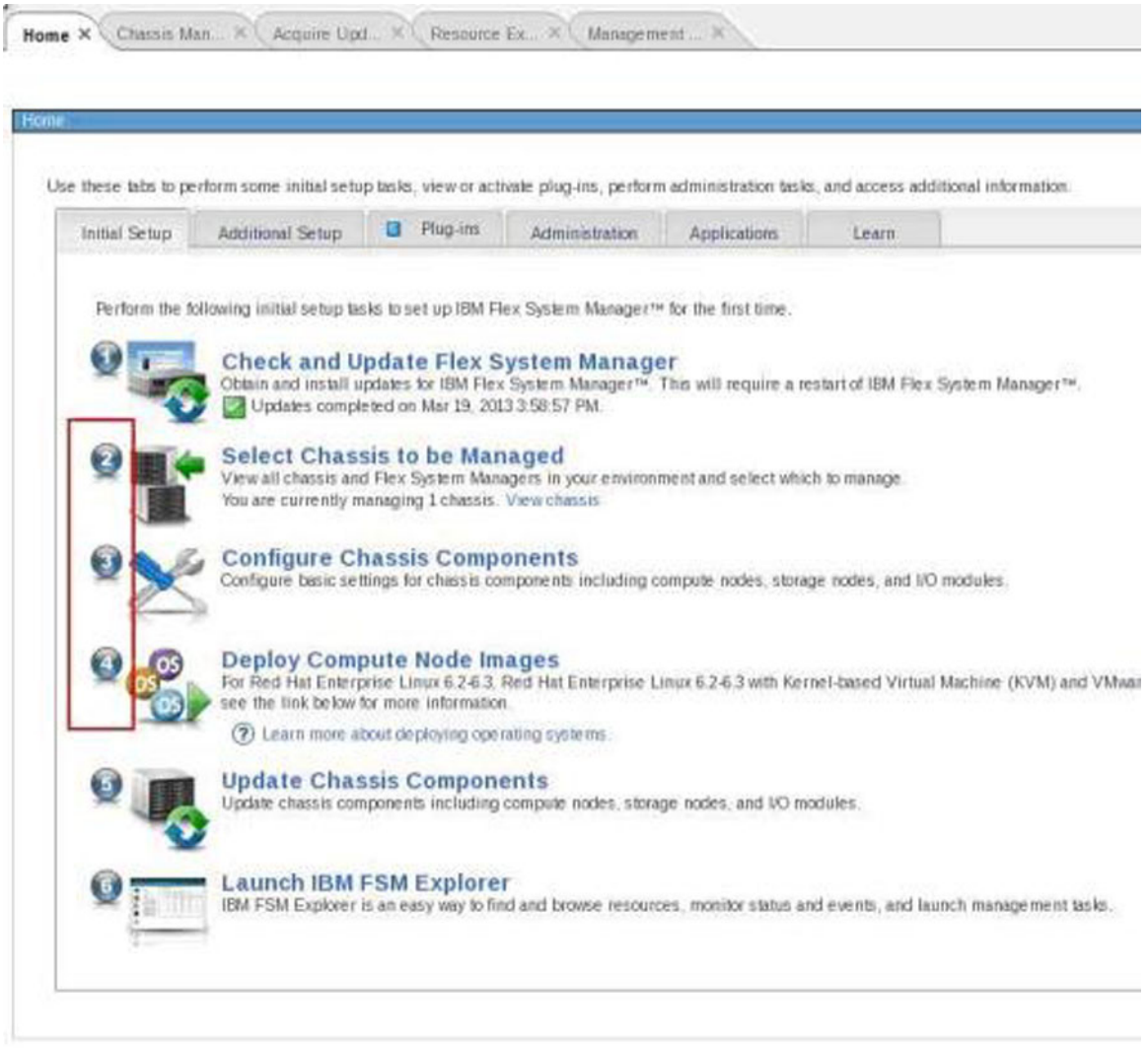
Tip: If you do not know the IP address of the operating system on an X-Architecture compute node, you can determine it by selecting the compute node from the **Chassis Manager**. Then select the common action **Remote Access** > **Remote Control** to start a remote login session to the operating system and determine the IP address.

Procedure

1. From the Home page, select the **Initial Setup** tab.
2. Follow Steps 2, 3, and 4 on the Initial Setup tab.

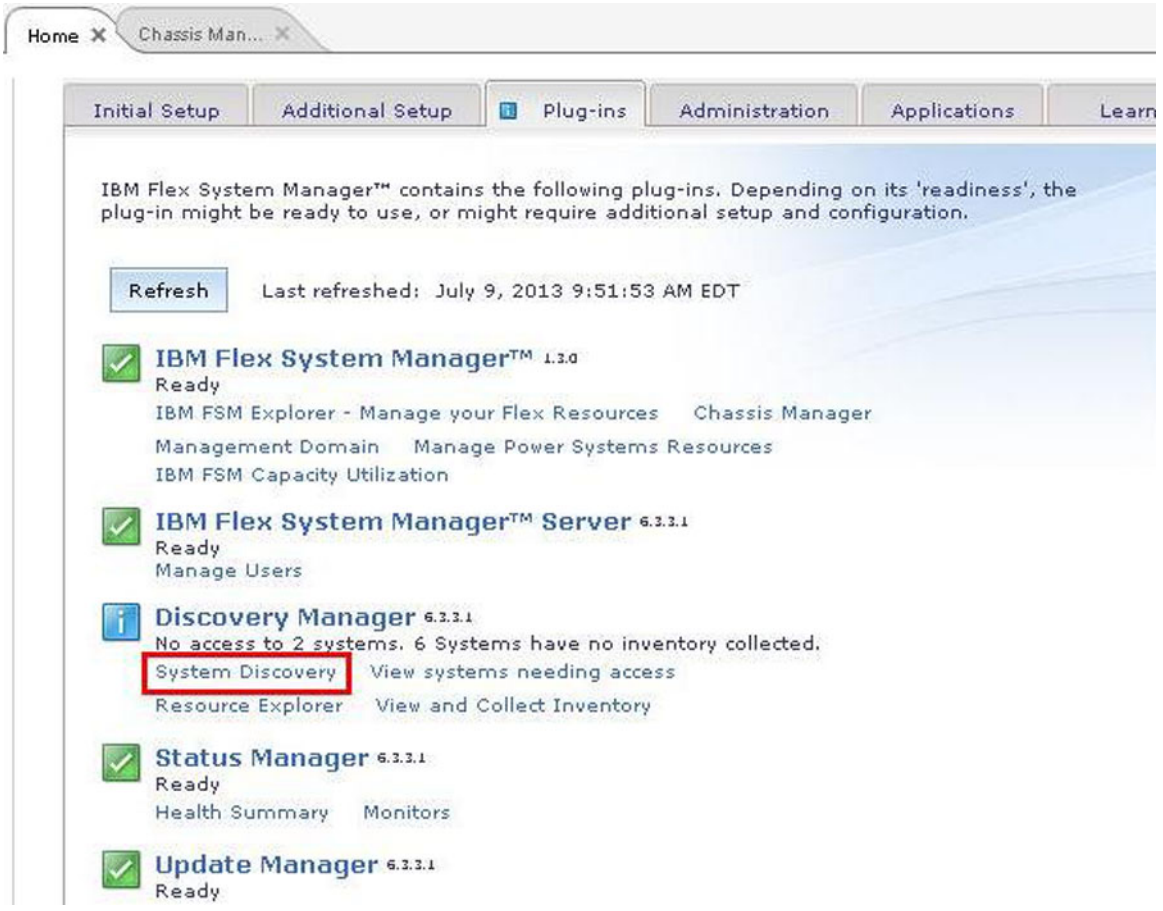
   Do not perform 

. You will perform that step in 3.5, “Updating the IBM FSM when the IBM FSM is not connected to the Internet,” on page 87.



3. Discover the operating systems for all compute nodes in the chassis. It is important to discover the operating systems through the IBM FSM. Complete the following steps for each compute node on which you installed an operating system:

a. From the Plugins tab, locate the heading for Discovery Manager and click **System Discovery**.



b. From the System Discovery wizard, select a discovery option, such as **Single IPv4 address**.

   Tip: Rather than type in a single address, you can choose to discover a range of IP addresses, which will make the discovery process easier.

c. Enter the IP address of the operating system.

d. For the field Select the resource type to discover, select **Operating System**.

e. Click **Discover Now**. Discovering systems is a job task. For more information about job tasks within the IBM FSM, see A.1, “Starting a job task,” on page 155.

For more information about discovering operating systems through the IBM FSM, see the following website:

http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/com.ibm.director.discovery.helps.doc/fqm0_t_performing_system_discovery.html

4. Make sure that you have access to all compute nodes and that the compute nodes are unlocked. From the Chassis Manager, you can verify that you have access to all compute nodes. If not, use the information provided at the following website to request access from the IBM FSM:

   http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/com.ibm.director.security.helps.doc/fqm0_t_requesting_access_to_a_secured_system.html

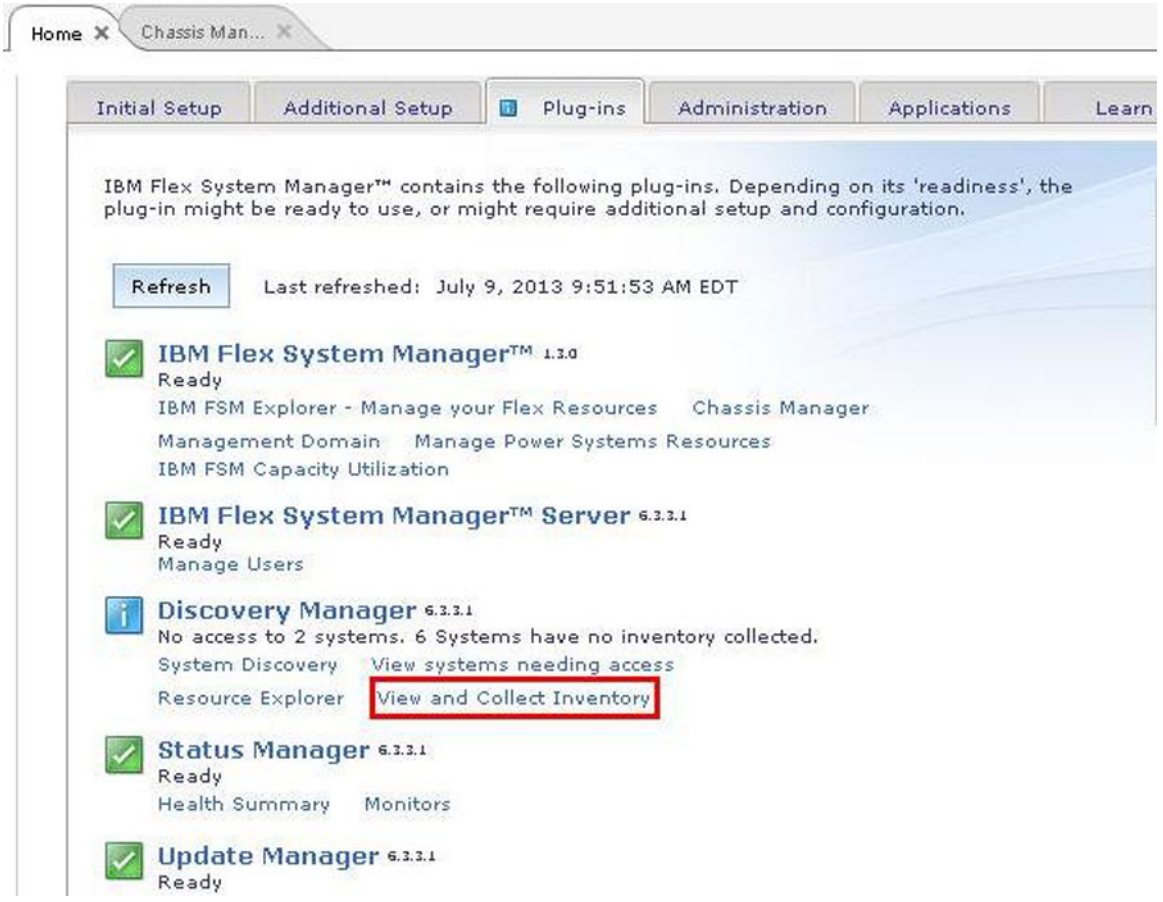
5. After all components, including the operating systems, have been discovered, perform a full inventory for all components in the chassis. Complete the following steps to discover all components, including operating systems:

   Important considerations:

   - Even if you are currently managing the chassis through the IBM FSM, you must still do a full inventory of the components (including operating systems) in the chassis before updating components.
   - Make sure that SCP is installed on the Power Systems compute nodes before running Discovery or Inventory Collection from the FSM so that the network adapters are discovered and inventoried by the FSM. For more information about installing SCP, which is available with the OpenSSH software tools, see the following website:

     http://pic.dhe.ibm.com/infocenter/aix/v7r1/topic/com.ibm.aix.security/doc/security/openssh_kerberosv5.htm

   a. From the Plugins tab, locate the heading for Discovery Manager and click **View and Collect Inventory**.



   b. Under Target Systems, click **Browse**.
   c. When the list is displayed, click **Actions** > **Select All**.
   d. Click **Add** to add the systems to the selected area.
   e. Click **OK**.
   f. On the summary page, click **Collect Inventory**.
   g. Select **Run Now** and click **OK**.

   Tip: Collecting inventory is a job task. If you are not familiar with job tasks in the IBM FSM, see A.1, "Starting a job task," on page 155.

For more information about collecting inventory on components in a chassis, see the following website:

http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/com.ibm.director.discovery.helps.doc/fqm0_t_collecting_inventory.html

3.3.2 Backing up the IBM FSM

Create a backup of the IBM FSM before updating the system.

Before you begin

Make sure that the IBM FSM has network access to a secure FTP (SFTP) server. To backup the management software to an SFTP server, the destination server must have Linux with Secure Shell (SSH) enabled. Otherwise, the backup operation might fail.

Procedure

Important: Do not power off the IBM FSM management node while a backup operation is in process. Otherwise, the backup will fail.
Complete the following steps to back up the IBM FSM image to the SFTP server:

1. From the Home page, click the **Administration** tab.
2. On the Administration tab under Serviceability tasks, click **Backup and Restore** to display the Backup and Restore page.
3. From the Backup and Restore page, click **Backup Now** to display the Backup page
4. From the Backup page, select **SFTP**.
5. Enter the location on the SFTP server where the backup file should reside (you must enter the SFTP server name as well).
6. Enter the User ID and password for the SFTP server (must have sufficient permissions to write to the server).
7. Click **OK**.

What to do next

After you have updated the IBM FSM management node, perform another backup of the system.

Additional information about backing up the IBM FSM is available at the following website:

http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/backing_up_frm.html

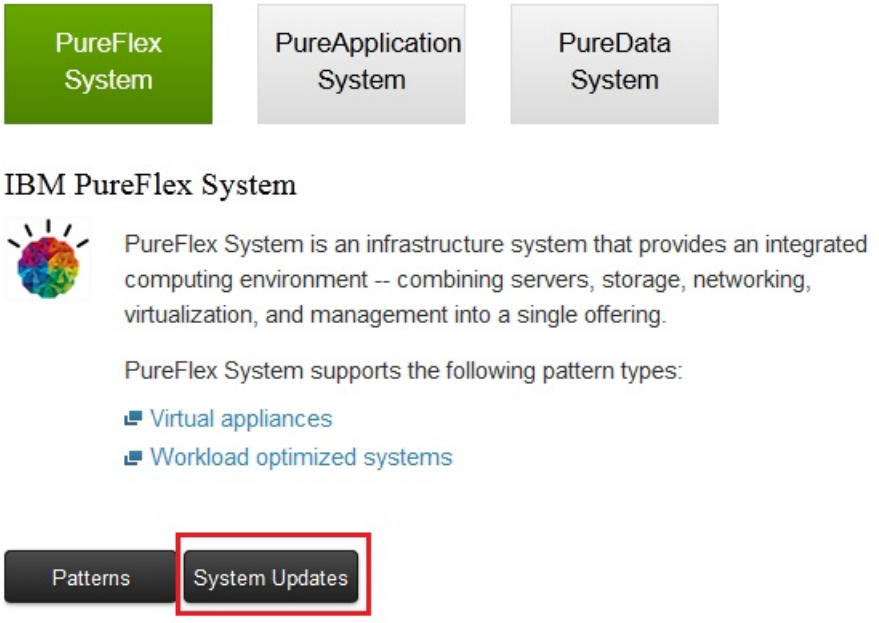
3.4 Obtaining all updates

IBM Flex System and IBM PureFlex updates are tested and released together.

The list of IBM Flex System and IBM PureFlex updates that have been tested and released together can be found at the following website:

http://www.ibm.com/software/brandcatalog/puresystems/centre/

From this site, scroll down and click **System Updates**:



When you click **System Updates**, you are directed to this location, where a list of updates is displayed:

http://www.ibm.com/software/brandcatalog/puresystems/centre/http://www.ibm.com/software/brandcatalog/puresystems/centre/update

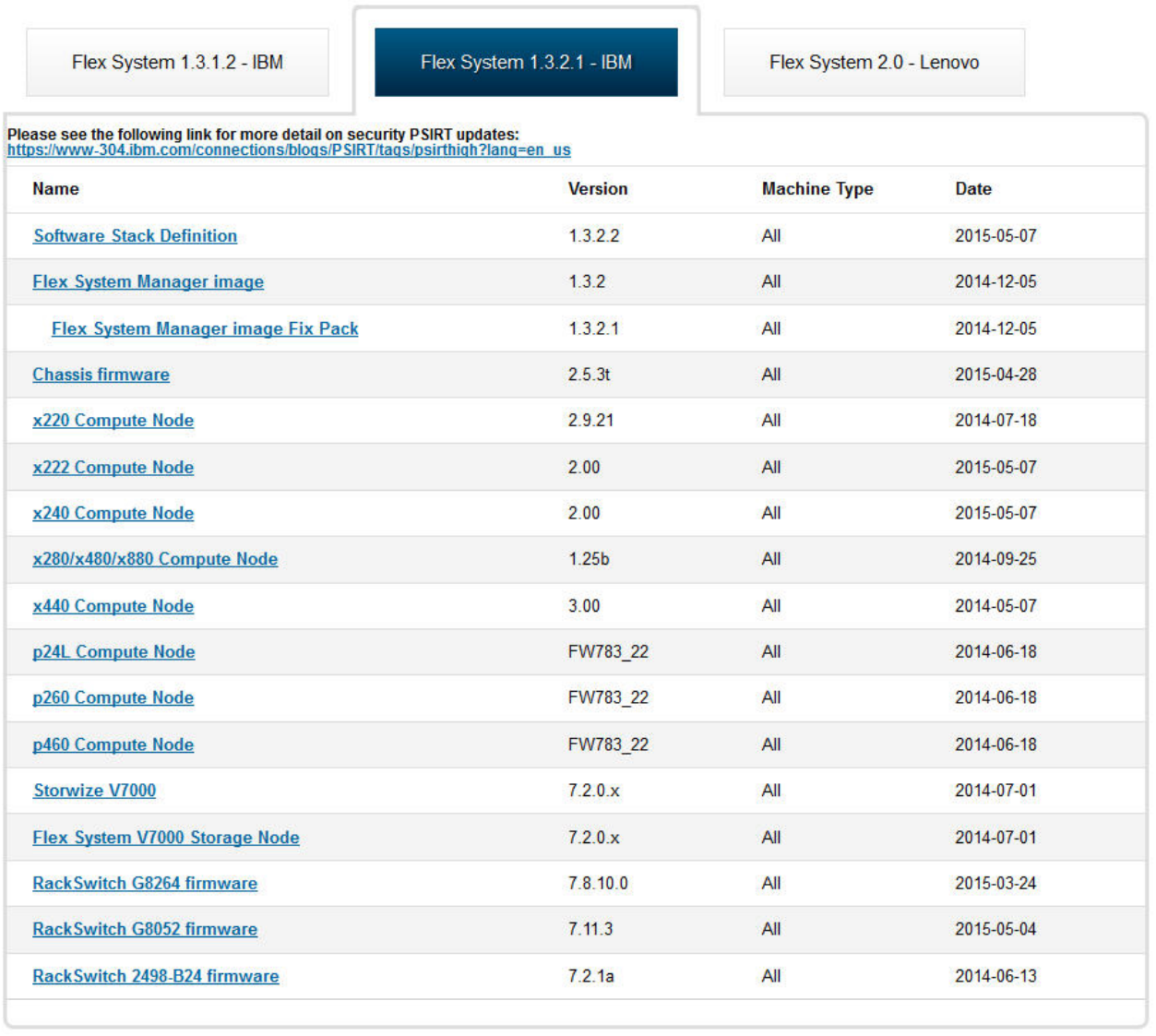
The updates are organized into groups that help you identify those updates that you need. Typically, you will not need every update on that web page. Download the updates from each group that match your installed hardware and operating systems. Then copy the updates to the IBM FSM, import the images into the IBM FSM updates library, and apply the updates.

For more information about this process, see 3.5, “Updating the IBM FSM when the IBM FSM is not connected to the Internet,” on page 87 and 3.6, “Copying and importing updates for chassis components to the IBM FSM,” on page 92.

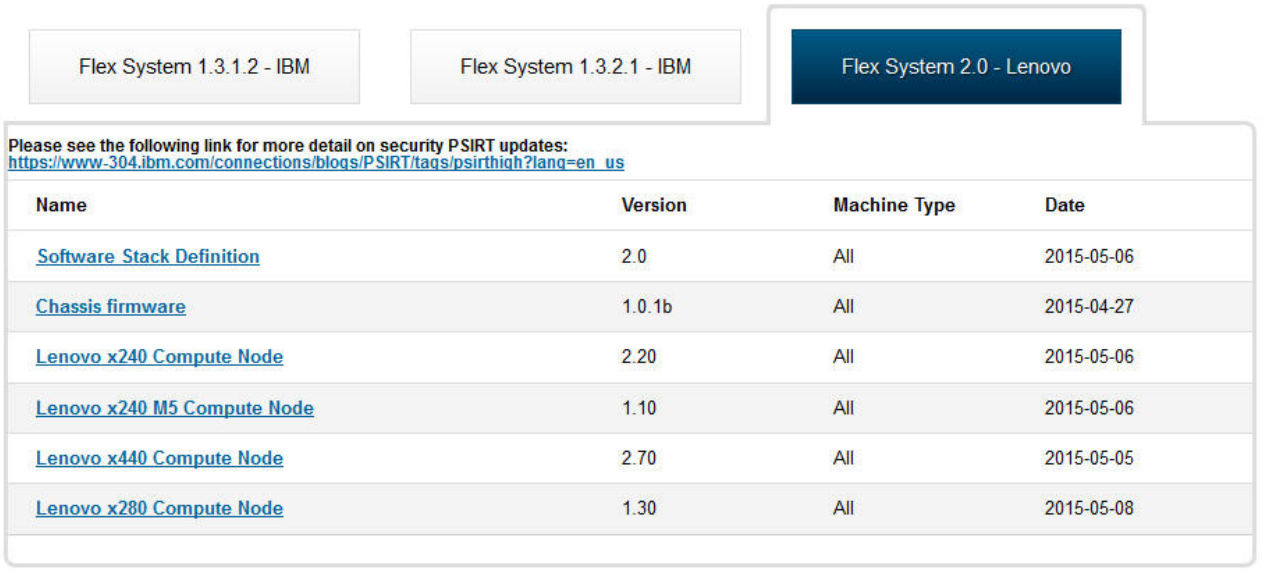
Note:

- The Flex System Manager image is required.
- You will need one or more I/O module updates; these updates are part of the Chassis Firmware group.
- You will need one or more X-Architecture compute nodes or Power Systems compute nodes.

Select the update group that matches the IBM Flex System version to which you want to update. You will select **Flex System 1.3.2.1 - IBM** tab.



Select the **Flex System 2.0 - Lenovo** tab to see the Lenovo update group.



When downloading a group it is only necessary to download those updates that match your hardware and operating system environment. If you are downloading one of the X-Architecture compute node groups (such as x220, x240, or x440), you only need to download the UpdateXpress System Pack (UXSP) that corresponds to the operating systems that you have installed on your X-Architecture compute nodes.

Note: Depending on how you have configured your update to be downloaded (whether you are using Download Director or HTTP to obtain the updates), the updates within each group might be downloaded in a zipped format.

3.4.1 Downloading the IBM FSM updates

The IBM FSM image is required and must be downloaded.

The image is downloaded as zipped files; do not unzip the files before copying it to the IBM FSM, which is described in 3.5, “Updating the IBM FSM when the IBM FSM is not connected to the Internet,” on page 87.

Important Consideration:

If Platform Agent is installed on any of the compute nodes, you must update the Platform Agent on each compute node before you update the firmware for that compute node. When you click **Flex System Manager image**, a list of the available updates for Platform Agent (and for Common Agent) are displayed.

The fixID of the agent packages on Fix Central starts with the following:

`Flex1_3_2_<agent_type>_<platform>`

where:

- *<agent_type>* is one of the following:

  For a new or update install of the agent on a remote system:

  – Common_Agent

  – Platform_Agent

  For updating the Common Agent or Platform Agent that is already installed on a remote system:

  – CAS (for Common Agent)

  - PA (for Platform Agent)
- <*platform*> is one of the following:
  - AIX
  - Linux_Power
  - Linux_x86
  - Linux_RHEL6KVM_x86_64
  - Windows_x86
  - Windows

The readme file provided with each update provides additional instructions for applying and activating the update. After a Platform agent upgrade it is recommended that a the Verify Connection action be run against the endpoint with the Query Vital Properties option selected to assure that communications are in a proper state.

3.4.2 Downloading the CMM updates

The Chassis Management Module (CMM) image is part of the Chassis firmware group.

3.4.3 Downloading X-Architecture compute node updates

When downloading UXSPs, make sure that you also download the UpdateXpress System Pack Installer (UXSPI) for the operating system that is running on your X-Architecture compute node. Both the UXSPs and the UXSPIs are available when you select the X-Architecture compute node from the IBM PureSystems Centre website. In addition, if you have Platform Agent installed on the compute nodes, you must update the Platform Agent before you update the firmware for the compute node.

Attention: IBM FSM version 1.3.3 manages both IBM and Lenovo manufactured System x and BladeCenter. Lenovo System x and BladeCenter have their own firmware updates, therefore, use Lenovo UXSPi to update both Lenovo system x and BladeCenter. Ensure that you manually import the latest version of IBM UXSPi to update when the target system is IBM System x or IBM BladeCenter. If the targeted systems are manufactured by Lenevo, then manually import the latest version of Lenovo UXSPi to update the systems. Use the latest IBM UXSPi to update firmware for FSM management server.

Note: You do not need to download a UXSPI application for the VMware vSphere 5 operating system.

Important considerations:

- The Emulex firmware update requires either the Corekit or the OneCommand Manager (OCM) application to be installed on Microsoft Windows or Linux operation systems before updating compute nodes running those operating systems.
- If you downloaded the UXSPs in a zipped format, make sure that you unzip them before copying the updates to the IBM FSM, which is described in 3.6, “Copying and importing updates for chassis components to the IBM FSM,” on page 92.
- At a minimum, you must apply VMware vSphere ESXi 5.0.x/5.1.x/5.5.x with IBM Customization Patch 1.2 or later for each compute node running the IBM customized image.

  If you are running VMware vSphere ESXi 5.5.x (update 1) or earlier, you must apply both the Lenovo and the Independent Hardware Vendor (IHV) customization patches (Patch 1.2) on every compute node. If you are running VMware vSphere ESXi 5.5.x (update 2), you need not apply Patch 1.2.

  In addition to the IBM Customization Patch 1.2, make sure that you install one of the following updates to the VMware vSphere ESXi operating system:
  - If you are running VMware vSphere ESXi 5.0, make sure that you install update 5.0u2 (update 2)
  - If you are running VMware vSphere ESXi 5.1, make sure that you install update 5.1u1 (update 1)
  - VMware vSphere ESXi 5.5.x

When you install an IMM update on an X-Architecture compute node, the Integrated Management Module (IMM) is reset, which can cause a VMware vSphere ESXi system failure (host purple diagnostic screen) if you attempt to update an X-Architecture compute node on which the minimum level of VMware is not installed (5.0u2, 5.1u1, or 5.5.x).

For information about obtaining the IBM Customization Patch 1.2, see the following location:

http://www.ibm.com/support/entry/portal/docdisplay?lndocid=MIGR-5092679

Make sure that you review the information provided in the readme for the patch. It contains instructions for installing the patch on a compute node.

- After installing patch 1.2, install the drivers for each of the adapters that are installed in the compute node. You can find information about these driver updates by going to the following website:

  http://www.ibm.com/support/fixcentral/

  From the Fix Central site, select the following fields:

  – **Product Group**: PureSystems
  – **Select from PureSystems**: PureFlex System
  – **Select from PureFlex System**: Compute Node
  – **Select from Compute Node**: The compute node on which the ESXi image is installed

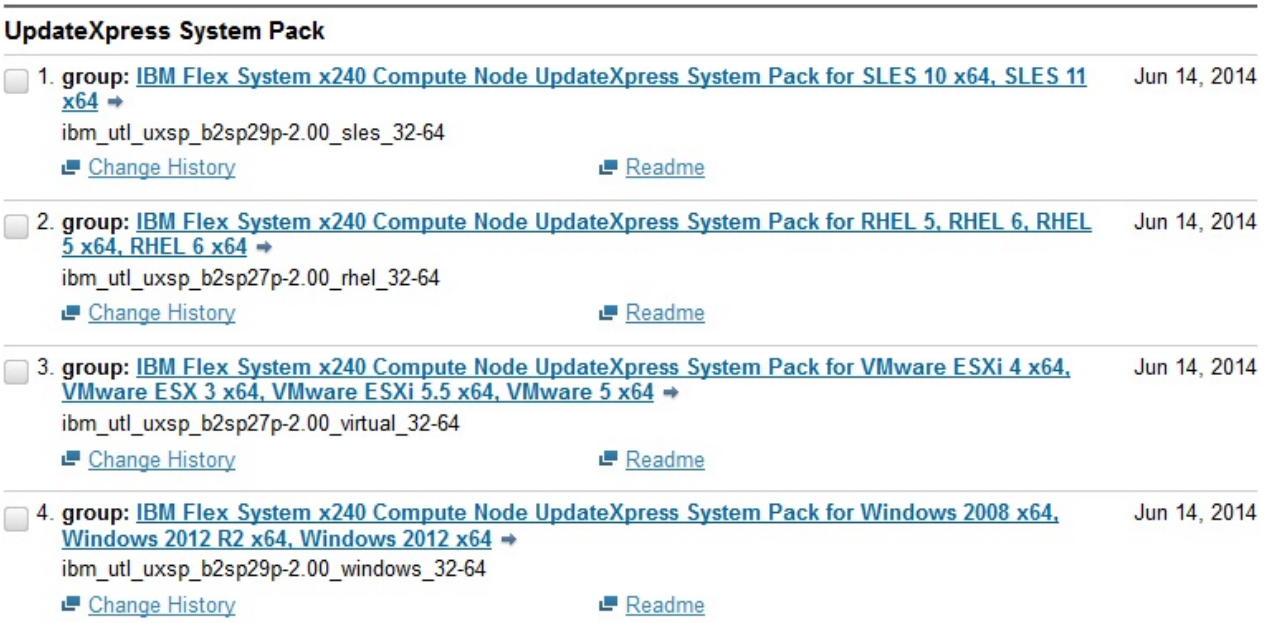
  Select the appropriate device drivers based on the adapters that you have installed. Follow the instructions provided with the driver update to install the driver.
- If Platform Agent is installed on compute nodes, you must update the Platform Agent on each compute node before you update the firmware for that compute node. Make sure that you download the Platform Agent that matches the operating system on which the compute node is installed.

  Note: If Common Agent is installed, you are not required to update Common Agent before updating the firmware on a compute node.

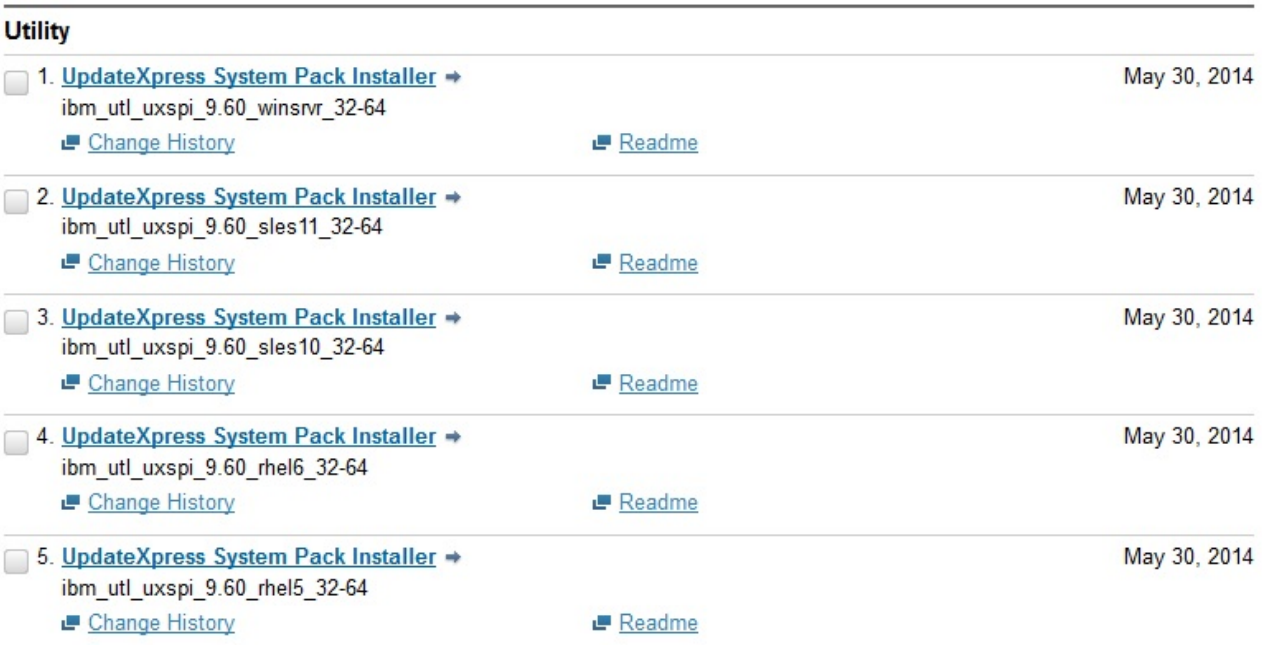
  Tip: The downloads for Platform Agent are listed under IBM Flex System Manager. Make sure that you download the updates that apply to the specific operating systems on each of the compute nodes. See 3.4.1, “Downloading the IBM FSM updates,” on page 81 for information about downloading IBM Flex System Manager updates.

For example, if you are using only the SLES and Windows operating systems, select only those UXSPs as shown in the following list (if you are using Download Director to obtain the updates):

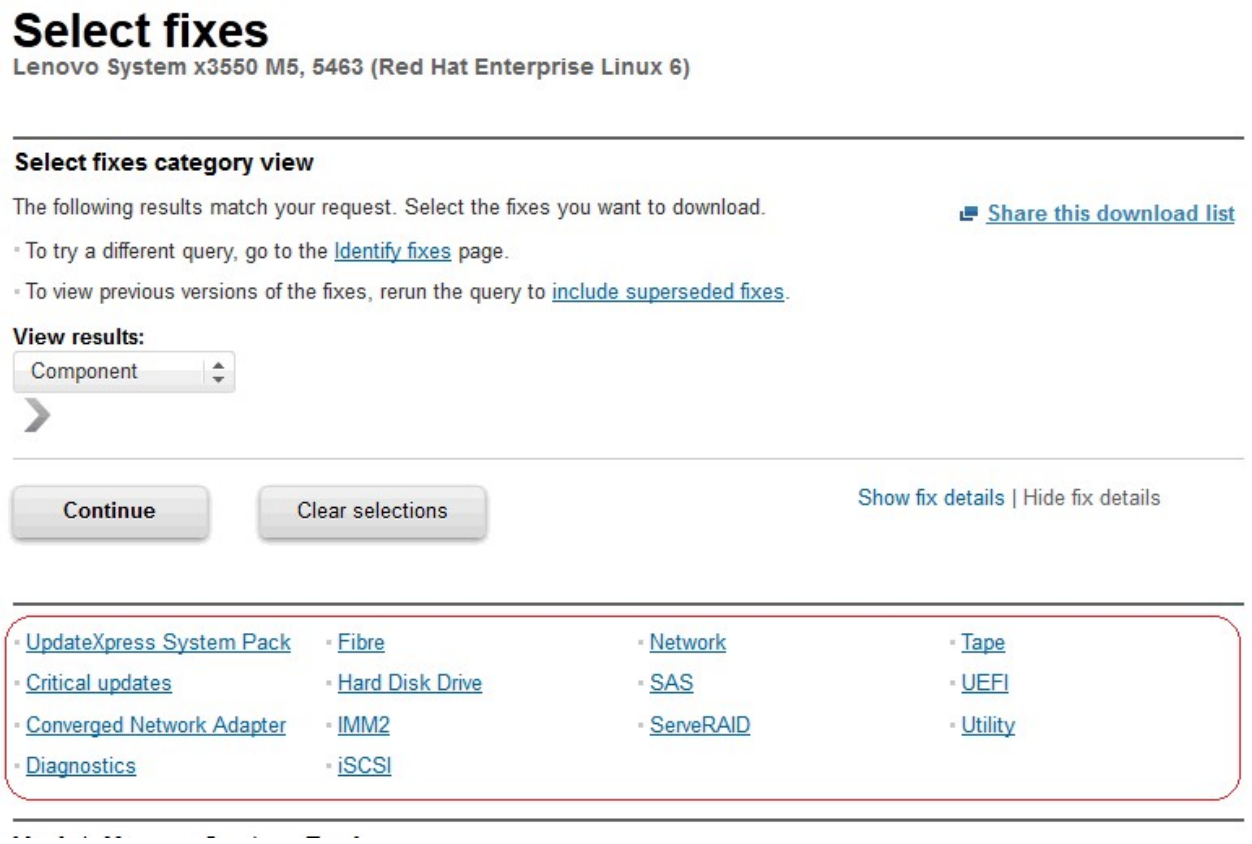
Note: The following example shows the UpdateXpress System Packs available for the x240 Compute Nodes.



Continue scrolling down the page to see the UpdateXpress System Pack Installers that are available:



Note: In addition to the UXSP, you can also download **Individual updates** from the category list that is on the left; for example, Diagnostics, Fibre. You can find the categories on the Select fixes page.



Or, you can continue scrolling the page to see the individual updates that are available.

↑ Back to top

Diagnostics

1.	**Lenovo Dynamic System Analysis (DSA)** ➡ lnvgy_fw_dsa_dsala2c-10.0_anyos_32-64 Readme Change History	Oct 22, 2014

↑ Back to top

Fibre

1.	**Emulex HBA (LPe1205/LPe1200x) Firmware Update for Linux - 2.02x11-5.13a6 - Release IBM14A** ➡ elx_fw_fc_ibm14a-2.02x11-40_linux_32-64 Change History Readme	Oct 17, 2014
2.	**QLogic 16Gb Fibre Channel Adapter MultiFlash Update for System x** ➡ qlgc_fw_fc_26xx-3.20.09_linux_32-64 Change History Readme	Oct 17, 2014
3.	**Qlogic FC/FCOE Device Drivers for RHEL6** ➡ qlgc_dd_fc_qla2xxx-8.06.00.10.a_rhel6_32-64 Change History Readme	Oct 17, 2014
4.	**Emulex HBA (LPe1205/LPe1200x) Firmware Update for Linux - 2.02x11-5.30a3 - Release IBM14A** ➡ elx_fw_fc_ibm14a-2.02x11-50_linux_32-64 Change History Readme	Oct 17, 2014
5.	**Emulex HBA (LPe1600x) Firmware Update for Linux - 10.2.377.18 - Release IBM14A** ➡ elx_fw_fc_ibm14a-10.2.377.18-2_linux_32-64 Change History Readme	Oct 17, 2014
6.	**Emulex FC/FCoE (lpfc) Device Driver for RHEL6 - 10.2.375.0 - Release IBM14a** ➡ elx_dd_fc_ibm14a-10.2.375.0-5_rhel6_32-64	Oct 17, 2014

3.4.4 Downloading Power System compute node updates

When you select the updates for the IBM Flex System p260, p460, and p24L compute nodes, make sure that you download the compute node firmware and any firmware required for installed devices, such as adapters or hard disk drives.

3.4.5 Downloading storage node updates

When downloading the StorageDisk 3949 updates for Flex System V7000 update, you must also select the StorageDisk 3949 SWUpgrade TestUtility.

Important considerations:

- When you download the updates for the Flex System V7000 (including the updates for the StorageDisk 3949 SWUpgrade TestUility), make sure that you download all files, including PDFs and md5sums files. Both the updates for the Flex System V7000 and the StorageDisk 3948 SWUpgrade TestUtility have an md5sums file, so depending on which you download first, one md5sums file might overwrite the other. The important thing is that at least one md5sums file is imported to the IBM FSM updates library.
- If you are downloading the updates using FTP, make sure that you run the following command:

  ```
  mget *
  ```

  To ensure that you get the md5sums file. If you run the command `mget *.*`, the md5sums file will not be downloaded.

To import the updates into the IBM FSM updates library, see 3.6, "Copying and importing updates for chassis components to the IBM FSM," on page 92.

3.4.6 Downloading I/O module updates

The I/O module firmware updates are part of the Chassis firmware group. This includes updates for switches and pass-thru modules.

3.5 Updating the IBM FSM when the IBM FSM is not connected to the Internet

After downloading all of the updates required for your environment to your local system, you must copy those updates to the IBM FSM management node and import those updates into the IBM FSM updates library.

Before you begin

Important considerations:

- Use this document to upgrade firmware if the IBM FSM that you have installed is currently at version 1.3.0 or higher. If the IBM FSM version is earlier than 1.3.0, make sure that you review 1.1, "Upgrading from an earlier version of Flex System firmware," on page 3.
- If you did not previously follow the steps to update the IBM FSM to version 1.3.1.1 (to resolve the OpenSSL Heartbleed vulnerability), apply the updates for version 1.3.2 to the IBM FSM and all components in all managed chassis. Then, from the IBM FSM, replace the TLS certificate and private key for the IBM FSM user registry, and change passwords according to the Remediation/Fixes section of the Security Bulletin referenced below:

  http://www.ibm.com/support/entry/portal/docdisplay?lndocid=MIGR-5095202
- Do not attempt to check for updates, import updates, and install updates (either install updates or installed needed updates) at the same time. Instead, when performing any of these tasks, make sure that the task being perform has completed before starting the next task.
- Before updating the IBM FSM management node, create a backup image of the IBM FSM. See 2.3.2, "Backing up the IBM FSM," on page 29.

- Make sure that the Storage Management Initiative Agent (SMIA) Configuration tool is not running. Before you start the update process for the IBM FSM:
  1. Log in to the IBM FSM Web interface.
  2. Select the **Tools** tab.
  3. In the SMIA Configuration Tool section, click **Stop**

  Note: After updating the IBM FSM, make sure that you restart SMIA if needed.

Before updating the IBM FSM management node, make sure that you have completed the procedures in 3.3, "Preparing for updates," on page 74 and that you hare performed any requisite updates in 3.1, "Steps to update from an IBM FSM that is not connected to the Internet," on page 64 (including any steps related to Power Systems firmware updates, if required).

About this task

You can copy the updates to the IBM FSM file system using SCP or a USB key. The preferred location to which the updates should be copied is the /home/<*user*> directory; where <*user*> is the user ID that you use to log in to the IBM FSM. The default user ID is USERID and the corresponding directory is `/home/USERID`.

For more information about copying updates to the IBM FSM, see the following website:

http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/com.ibm.director.updates.helps.doc/fqm0_t_um_updates_director_manual_download.html

Important consideration:

Do not copy updates or any files to the IBM FSM `/tmp` directory. Instead use a user directory such as `/home/USERID`.

The total disk space available to users in the /home/<*user*> directory is approximately 20 GB, so you might have to copy and import the updates in stages:

1. Copy updates to a user directory on the IBM FSM.
2. Import updates to IBM FSM updates library.
3. Delete transferred updates after importing to the updates library.

Tip: When importing updates to the IBM FSM updates library, you can specify the –c parameter to delete the updates after they have been imported. For more information, see 3.6, "Copying and importing updates for chassis components to the IBM FSM," on page 92.

To determine how much space is available in the directory, run the disk usage command:

```
du -h
```

If you need to import updates in stages due to the total size of the updates, it is important that you copy and import files associated with the same update together. Typically each update has a payload, a readme, a change history and one or more metadata files, such as .xml files, .pd files, and .sdd files. Make sure that you import all files associated with the update, including any readme files.

If you do not copy and import the updates together, you will get errors when importing the update or the import process will not import the update payload file.

Tip: The best process is to copy, import, and install the updates for the IBM FSM. Then remove the update from the directory before copying the rest of the updates to the directory..

Make sure that you copy all files that you downloaded. The first update to copy is the IBM FSM update.

Note: The IBM FSM update is a zipped file. Make sure that you transfer the update to the FSM without unzipping it.

A typical scp command for copying the IBM FSM update from your laptop is:

```
scp * USERID@<management_node_host_name>:/home/USERID
```

Where <*management_node_host_name*> is the DNS name or the IP address of the IBM FSM. If you are using winscp, you must set transfer mode to binary, so that text files are not modified during transfer.

For instructions on copying files to the IBM FSM, see the following website:

http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/com.ibm.director.updates.helps.doc/fqm0_t_um_updates_director_manual_download.html

Procedure

Complete the following steps to import the IBM FSM update into the updates library and apply the IBM FSM update.

1. Copy the update for the IBM FSM.

   ```
   scp FSMApplianceUpdate*.zip USERID@<i><management_node_host_name></i>:/home/USERID
   ```

2. Use the IBM FSM command-line interface (CLI) to clean up any existing FSM updates, collect inventory from the IBM FSM, and import the IBM FSM update
   a. Log in to the IBM FSM command-line interface (CLI) using a remote-access utility, such as Secure Shell (SSH).
   b. From the CLI, run these commands

      Note: Type in the commands exactly as shown.

      ```
      smcli cleanupd -mFv -P "Platform='Director' OR Platform='DirectorAppliance'"
      smcli collectinv -p "All Inventory" -i 10.3.0.1,10.3.0.2 -t OperatingSystem
      smcli importupd -v /home/USERID/FSMApplianceUpdate-1-3-2-ImportFirst.zip
      smcli importupd -v /home/USERID/FSMApplianceUpdate-1-3-2-ImportSecond.zip
      smcli importupd -v /home/USERID/FSMApplianceUpdate-1-3-2-ImportThird.zip
      ```

      If you have issues with the update, you can attempt to perform the update again using the –o option on the **importupd** command to overwrite the existing image in the update library.

      If you are not familiar with the IBM FSM CLI, see the following website:

      http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/using_the_cli.html

3. Install the update using the following CLI command:

   ```
   smcli installneeded -v -F -I
   ```

   Tip: If the software for the IBM FSM is already updated, but you need to update the firmware only, such as when a system board is replaced, you can run the **installupd** command to update the firmware:

   ```
   smcli installupd -i 10.3.0.1 --force -u fsm_appliance_update_1.3.2 -v
   ```

   As the install task is running, messages are displayed in the console.

   The update task takes an additional 20 to 120 minutes due to the installation of Network Advisor, which can take 45 minutes. The time required to update also depends on the specific chassis configuration that is being managed by the IBM FSM.

   For other issues related to the IBM FSM update, see Chapter 7, “Troubleshooting update issues,” on page 137.

What to do next

Important Considerations

- When the IBM FSM has restarted, make sure that you clear your browser cache before accessing the IBM FSM Web interface.
- Do **not** restart the IBM FSM until the IBM FSM update completes successfully. If you have trouble updating the IBM FSM firmware (pDSA, IMM, or UEFI) through the IBM FSM, you can log in to the IMM user interface for the IBM FSM to apply those updates. Complete the following steps:
  1. Make sure that FSMApplianceUpdate-1-3-2-ImportFirst.zip is on your computer.
  2. Unzip FSMApplianceUpdate-1-3-2-ImportFirst.zip
  3. Find the pDSA, IMM, and UEFI updates. The file name of the updates change each release, but you can search for the following strings to find the updates:
     - pDSA (Diagnostics). Search for ibm_fw_dsa_dsyt*_anyos_32-64.uxz
     - IMMv2. Search for ibm_fw_imm2_1aoo*_anyos_noarch.uxz
     - UEFI. Search for ibm_fw_uefi_bde*-1.21_anyos_32-64.uxz
  4. Use the IMM interface to apply those updates.

  Note: After applying IMM, pDSA, and UEFI updates, you will need to reset the IMM. To reset the IMM, establish an SSH session to the IMM for the compute node and use the **resetsp** command. Alternatively, you can restart the IBM FSM to reset the IMM.

When the update completes successfully, you need to restart the IBM FSM. To restart the IBM FSM, run the following command from the CLI:

```
smshutdown –r –t now
```

The IBM FSM takes a further 30 to 90 minutes to fully restart.

Tip: After the IBM FSM has restarted, you can use the **who** command to validate that the IBM FSM has been restarted:

```
who -b
```

The result will be similar to:

```
system boot 2014-06-24 11:57
```

After importing and installing the IBM FSM update, you can delete the IBM FSM update zip files from the user directory to make room for transferring the remaining updates. From the IBM FSM CLI, run the following command:

```
rm FSMApplianceUpdate*.zip
```

3.5.1 Validating that the IBM FSM is updated

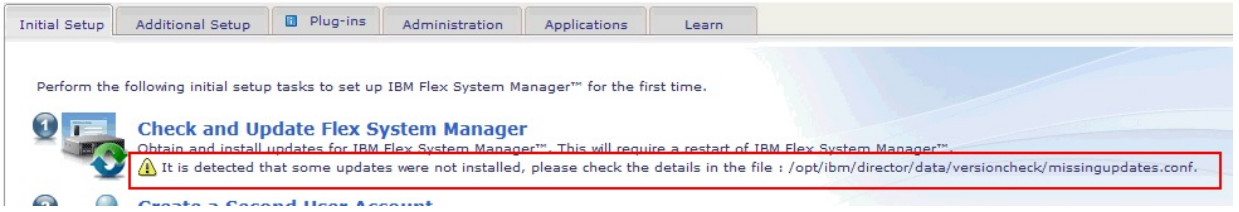
Verify that the IBM FSM was updated successfully.

Procedure

Complete the following steps to ensure that the IBM FSM update has completed successfully:

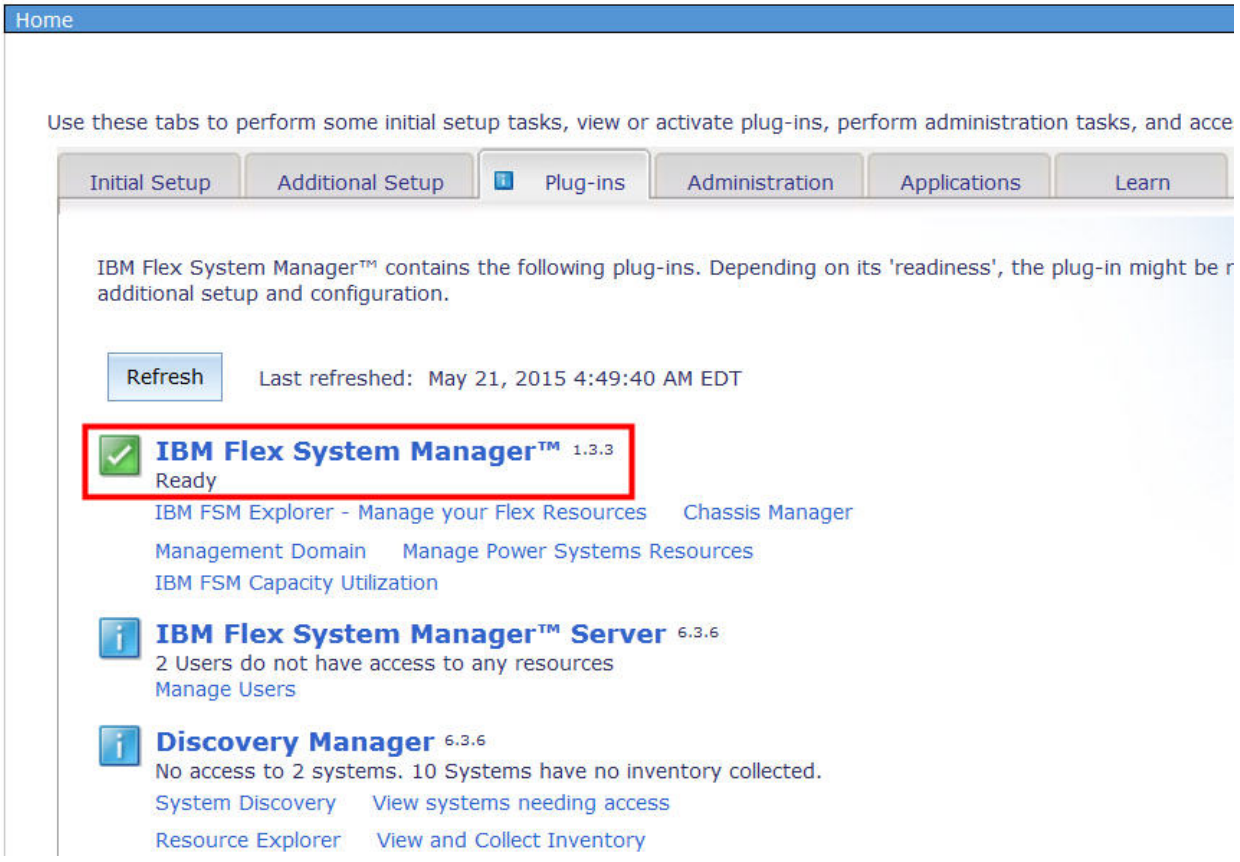
Note: You must use the web interface to ensure the successful installation of the IBM FSM (Step 1). You can use the FSM CLI command **`lsconfig`** to check the version (Step 2).

1. From the Home page, click the **Initial Setup** tab.



   If you see the indication that some of the updates were not installed, see 7.1, “IBM FSM software update causes warning on Initial Setup tab,” on page 137.

2. To check the version of the IBM FSM that is installed, from the Home page, click the **Plugins** tab.



3. Select **IBM Flex System Manager**. Under the IBM FSM Status, the installed version is displayed.

What to do next

After validating that the IBM FSM was updated successfully, perform another backup of the IBM FSM. See 3.3.2, “Backing up the IBM FSM,” on page 78.

3.6 Copying and importing updates for chassis components to the IBM FSM

Copy all remaining updates that you have already downloaded to the IBM FSM. Then, import the updates.

See 3.4, “Obtaining all updates,” on page 79 for information about copying the updates.

Import the updates into the updates library using the following command:

```
smcli importupd -v /home/USERID/
```

Repeat the above until all updates that you downloaded from IBM are imported.

Tip: The **importupd** command imports all updates from the /home/USERID/ directory into the IBM FSM updates library. Depending on the size of the updates, you might be able to copy all updates to the /home/USERID directory and then run the **importupd** command one time.

After importing the updates, remove the updates from /home/USERID using the following command:

```
rm *.*
```

3.7 Updating the CMM

Updates for the CMM are typically imported to the IBM FSM updates library when you update the IBM FSM. Therefore, you do not normally need to acquire the update before installing the update.

Before you begin

Important consideration:

If you are updating the system that is managed by an IBM FSM, version 1.1.1 or earlier, you must update the Flexible Service Processor (FSP) for each Power Systems compute node ***before*** you update the CMM.

Procedure

Complete the following steps to update the firmware for each CMM in the chassis:

1. From the Home page, click the **Initial Setup** tab.
2. Click **Update Chassis components**.
   - If the CMM update has been imported to the IBM FSM updates library, Updates are available to install is displayed. Click **Install updates** and proceed to 3.7.1, "Installing the CMM update," on page 94.

   - If you do not see Updates are available to install and you cannot click on Install Updates, click **CMMs – Check and Update Firmware** to acquire and import the updates.

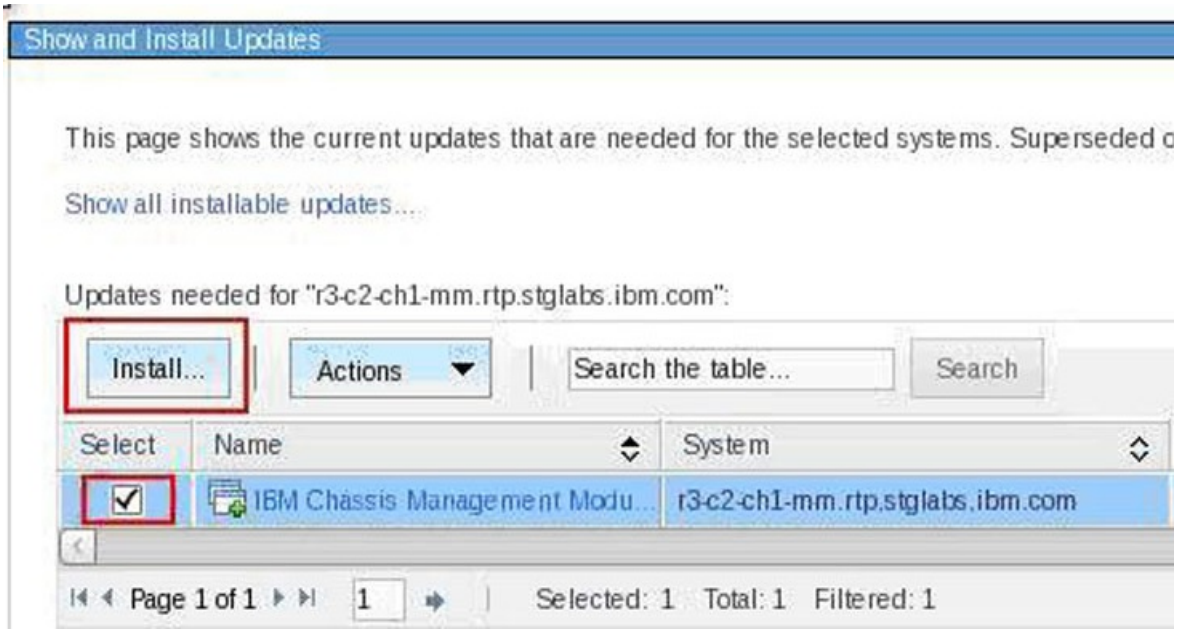
     Follow the steps in A.3, "Acquire updates wizard," on page 159 to specify where the IBM FSM can obtain the updates to be installed. When completed, click Shown and Install Updates to continue.

3.7.1 Installing the CMM update

After acquiring the update, you need to install it.

Procedure

When you clicked **Install Updates** or **Show and Install Updates**, the Show and Install Updates page is displayed.



1. From this tab, select the update in the Select column and click **Install** to start an Install Wizard.

   Tip: In the Install Wizard, consider selecting the option **Automatically restart during installation as needed**. The CMM must be restarted for the update to take effect. However, you might lose your connection to the FSM temporarily while the CMM is restarting.

   If you do not select the option **Automatically restart during installation as needed**, the update task will show as completing with errors (because the update task is not complete until the CMM is restarted).
2. In the Launch Job pop-up window, go to the Schedule tab and select **Run Now**. Then click **OK**.

Results

You can verify the update completed successfully by looking in the Task Log Steps and verifying that each step completed with status Complete. For information about validating that the job completed successfully, see A.4, “Verifying an update completed successfully,” on page 161.

3.8 Updating compute nodes from an IBM FSM that is not connected to the Internet

Use the IBM FSM to update the firmware for Power Systems compute nodes and X-Architecture compute nodes.

The prerequisites for updating compute nodes can be found in the following website:

http://pic.dhe.ibm.com/infocenter/flexsys/information/index.jsp?topic=%2Fcom.ibm.acc.8731.doc%2Fcom.ibm.director.updates.helps.doc%2Ffqm0_c_um_platform_extensions.html

If you have configured a virtual environment, make sure that you relocated virtual servers before updating the compute nodes. More information about relocating virtual servers is available at the following location:

http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/com.ibm.director.vim.helps.doc/fqm0_t_relocating_a_virtual_server.html

To update System x compute nodes and the network adapters on Power Systems compute nodes, you must first discover the operating system running on the compute node from the IBM FSM.

Important consideration:

The IBM Flex System Manager management node Eth1 port must be connected to the chassis switch modules that are installed in I/O bay 1 or bay 2. This is referred to as the data network. You can configure a switch module in bay 1 or bay 2 to map Eth1 to one of its external Ethernet ports, as you would configure the other nodes in the chassis that are connected to the external network. The data network is used by applications and operating systems and can support data transfer rates up to 10 Gbps if a chassis switch module that is capable of 10 Gbps is installed.

One of the key functions that the data network supports is discovery of operating systems on the various network endpoints. Discovery of operating systems by the IBM Flex System Manager is required to support software and firmware updates on an endpoint such as a compute node. The IBM Flex System Manager Checking and Updating Compute Nodes wizard assists you in discovering operating systems as part of the initial setup.

IBM FSM does not support updating x440 M5 (MT 7167, 2590) and x240 M5 (MT 9532, 2588) ITEs. As an alternative, you can use the UpdateXpress System Packs (UXSPs) and the UpdateXpress System Pack Installer (UXSPI) to update these ITEs.

Important: There are no lifecycle UXSP releases in December 2014 (except for x440 M5 and x240 M5). However, you can apply the existing individual Mezzanine updates to these ITE end points.

For information about updating the compute node firmware through the IMM, see the "Integrated Management Module II User's Guide," which is available at this location:

http://www.ibm.com/support/entry/portal/docdisplay?lndocid=MIGR-5086346

Make sure that you update firmware for UEFI, pDSA, IMM, and any network adapters that are installed.

Tools are available to assist you in the update process through the IMM interface:

- IBM Fast Setup
  http://www.ibm.com/support/entry/portal/docdisplay?lndocid=TOOL-FASTSET
- IBM Bootable Media Creator

http://www.ibm.com/support/entry/portal/docdisplay?lndocid=TOOL-BOMC

3.8.1 Discovering operating systems from the IBM FSM

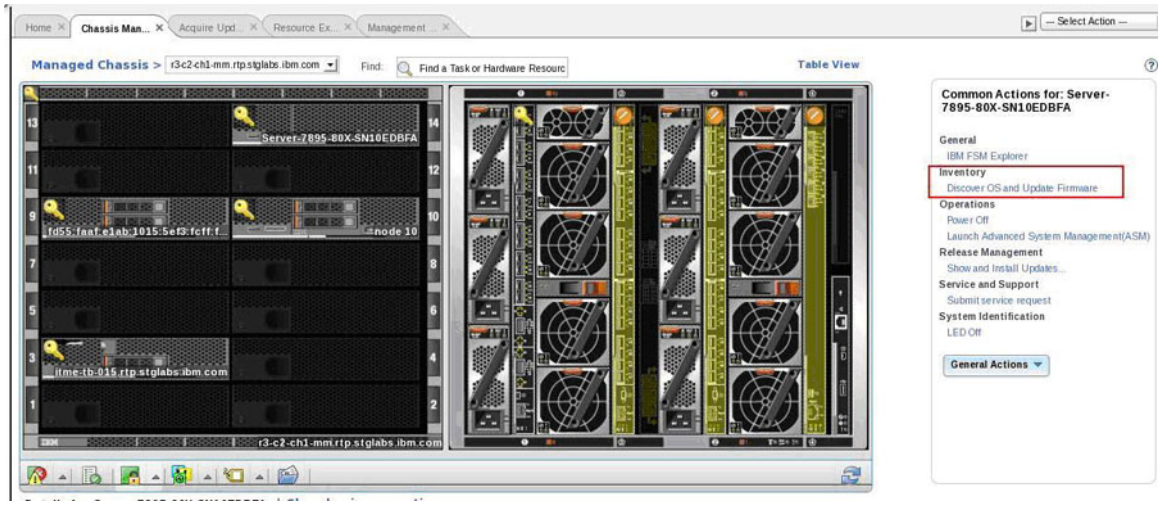
You need to ensure that all operating systems have been discovered by the IBM FSM.

If you followed the procedures in 3.3.1, "Making sure that the IBM FSM is managing the chassis," on page 74, all operating systems should be discovered by the IBM FSM and you can proceed to one of the following sections:

- 3.8.2, "Updating Power Systems compute nodes," on page 97
- 3.8.3.2, "Installing X-Architecture compute node updates," on page 108

If you have not already discovered the operating system for a compute node, complete the following steps:

1. From the Chassis Manager tab, select the compute node for which the operating system is to be discovered.
2. Under Common Actions, select **Discover OS and Update Firmware**:



More information about updating compute nodes is available in the *Updating firmware on a compute node from the IBM Flex System Manager user interface Quick Start Guide* at the following website:

http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.commontasks.doc/commontasks_managing_hw.html

The IBM FSM operating system discovery process can fail if the compute node is configured with VMware vSphere Hypervisor 5.5 with IBM Customization Installable, any model, any update and there are multiple VMK interfaces. To resolve the issue, see the following website:

http://www-947.ibm.com/support/entry/portal/docdisplay?brandind=5000008&indocid=MIGR-5095635

3.8.2 Updating Power Systems compute nodes

Before updating the firmware for the FSP on Power Systems compute nodes, make sure that you have read the prerequisites.

Before you begin

Prerequisites are listed in 3.2, “Prerequisites,” on page 70. In addition, make sure that you have performed the procedures described in 3.3, “Preparing for updates,” on page 74.

Important consideration:

- If you are updating firmware for Power Systems compute nodes running FSP firmware that is earlier than the December, 2012 release (AF763_043), you must update the Flexible Service Processor (FSP) for each Power Systems compute node before you update the CMM.

  Updating older version FSPs after updating the CMM might leave your compute nodes unusable (in a status 'pending' condition). If this happens, see 7.9, “Power Systems compute node remains at a status pending state after an update,” on page 142.
- If you are updating firmware for Power Systems compute nodes running FSP firmware 01AF773, you must update the Flexible Service Processor (FSP) for each Power Systems compute node to 01AF773_058 before you update the firmware for the IBM FSM. See 2.1.2, “Steps to update for Power Systems compute nodes running FSP firmware version 01AF773,” on page 20 for more information.
- Make sure that SCP is installed on the Power Systems compute nodes before running Discovery or Inventory Collection from the IBM FSM so that the network adapters are discovered and inventoried by the IBM FSM. For more information about installing SCP, which is available with the OpenSSH software tools, see the following website:

  http://pic.dhe.ibm.com/infocenter/aix/v7r1/topic/com.ibm.aix.security/doc/security/openssh_kerberosv5.htm

Procedure

Complete the following steps to update firmware for the FSP on Power Systems compute nodes:

1. From the Chassis Manager, click **General Actions** > **Manage Power Systems Resources**.
2. Click **Actions** > **Select All** to select all of the Power Systems hosts.
3. You should have already copied the updates to the IBM FSM and imported the updates into the updates library. If not, see 3.4, “Obtaining all updates,” on page 79 for more information.
4. Select **Actions** > **Release Management** > **Show and Install Updates**.

   Note: If the expected updates do not display, see 7.11, “Power Systems firmware update does not display as needed,” on page 143 for information about showing all updates.
5. Select the FSP update, start the task, and wait for it to complete.

   Tip: The update task is referred to as a job task. If you are not familiar with job tasks in the IBM FSM, see A.1, “Starting a job task,” on page 155.

   Important consideration

   Updates to the Power Systems FSP cannot be selected at the same time as the Power Systems updates that run in-band from the operating system. Update the Power Systems compute nodes in the following order:

   a. Update the FSP.
   b. After updating all other components in the chassis, see the following sections to continue with the updates for the Power Systems compute node:
      - 3.8.2.2, “Updating Power Systems network adapters and hard disk drives,” on page 98.
      - 3.8.2.3, “Updating the IBM Flex System EN4054 4-port 10Gb Ethernet Adapter,” on page 99.

What to do next

Ensure that all Power System updates complete successfully before continuing to update the remaining components in the chassis.

If you did not update the FSP on Power Systems compute nodes before updating the CMM, and the Power Systems compute node remains at a status pending state after an update, see 7.9, "Power Systems compute node remains at a status pending state after an update," on page 142 to resolve the issue.

3.8.2.1 Activating the Power FSP update on the Permanent boot side

FSP updates for Power Systems are deployed on the Temporary boot side of the Power Systems compute node. After you have determined that FSP update is working correctly in your environment, apply the update to the Permanent boot side.

Procedure

Complete the following steps to apply the firmware update to the permanent boot side:

1. From the Chassis Manager, click **General Actions** > **Manage Power Systems Resources**.
2. From the Manage Power Systems Resource menu, select all **Power Systems**.
3. Click **Actions** > **Release Management** > **Power Firmware Management**.
4. Click **Actions** > **Power Firmware Management** > **Accept**.
5. Click the **Start Accept Task** and start the job task.

   Tip: If you are not familiar with job tasks in the IBM FSM, see A.1, "Starting a job task," on page 155.

3.8.2.2 Updating Power Systems network adapters and hard disk drives

Use this procedure to update the firmware for network adapters and hard disk drives.

Procedure

If you are updating firmware for the IBM Flex System EN4054 4-port 10Gb Ethernet Adapter, see 3.8.2.3, "Updating the IBM Flex System EN4054 4-port 10Gb Ethernet Adapter," on page 99.

Note: Before updating firmware on Ethernet adapters, make sure that all ports are inactive.
Complete the following steps to update firmware for Power Systems compute nodes:

1. From the Chassis Manager, click **General Actions** > **Manage Power Systems Resources**.
2. From the Manage Power Systems Resources menu, click **Operating Systems**.
3. Click **Actions** > **Select All** to select all of the Power Systems operating systems.
4. Acquire the updates to be applied. Click **Actions** > **Release Management** > **Acquire Updates**.
5. Select **Actions** > **Release Management** > **Show and Install Updates** to start the Install Wizard.
6. From the Welcome page, click **Next**.
7. On the Device Options page, select all devices to be updated.

   Note: If a device has multiple ports, such as the FC3172 2-port 8Gb Fiber Adapter, make sure that you check all ports (for example: fcs0 and fcs1).

   Click **Next**.
8. On the Restarts page, note any restart requirements. Then click **Next**.
9. On the Summary page, confirm the updates to be installed. Then click **Finish**.
10. From the Schedule tab in the Launch Job window, select **Run Now**. Then click **OK**.

Tip: The update task is referred to as a job task. If you are not familiar with job tasks in the IBM FSM, see A.1, "Starting a job task," on page 155.

3.8.2.3 Updating the IBM Flex System EN4054 4-port 10Gb Ethernet Adapter

Complete the following steps to update the firmware for the IBM Flex System EN4054 4-port 10Gb Ethernet Adapter through VIOS and AIX.

Before you begin

Note: Before the IBM Flex System EN4054 4-port 10Gb Ethernet Adapter firmware update can occur, any non-native Ethernet devices (i.e. Etherchannel, SEA, VLAN psuedo device) must be reconfigured to use one of the native Ethernet adapter ports. This process will disrupt Ethernet traffic to any client LPARs and will require a reboot of VIOS. Therefore, this procedure should be performed during a maintenance window.

Procedure

The steps are written such that there is no need to save any non-native Ethernet device configuration information prior to execution. Upon reboot of VIOS, the original non-native Ethernet device configuration will be restored automatically.

1. Complete the following steps to log in to VIOS:

   Note: Do not attempt to open a console to VIOS using a method that depends on the Ethernet connection, such as SSH. Ethernet connectivity will be disrupted during the firmware update process.

   a. From the Chassis Manager, click **General Actions** > **Manage Power System Resources**.
   b. From the Manage Power Systems Resources menu, click **Virtual Servers**.
   c. Put a check mark in the box beside the VIO server to select it. Then click **Actions** > **Operations** > **Console Window** > **Open Terminal Console**.
2. Run the following command to obtain root access:

   ```
   oem_setup_env
   ```
3. Save the existing network configuration:
   a. Run the following command:

      ```
      ifconfig –a
      ```

      Note the IP address and interface where the IP address is configured. If multiple IP addresses are configured, make a note of each IP address and interface.
   b. Run the following command:

      ```
      netstat -rn
      ```

      Make a note of the routing information.
4. Determine how the adapter port that requires the firmware update is configured. Run the following commands to determine how the adapter port is configured.
   - `lsdev -c adapter` - to list all adapters
   - `lsdev -t ibm_ech` - to list all EtherChannel adapters
   - `lsdev -t sea` - to list all Shared Ethernet Adapters
   - `lsdev -s vlan` - to list all VLAN devices
   - `lsattr -El entX` - to list attributes of a given adapter (e.g. `lsattr -El ent7`)

   Adapter ports can be configured in one of the following ways:
   - Natively where the IP address is configured on the port.
   - Part of EtherChannel.
   - Part of Shared Ethernet Adapter (SEA)
   - Part of EtherChannel, which is configured as part of SEA.

- Part of SEA (either directly or via EtherChannel) and the VLAN pseudo device is configured on top of SEA.

5. Prepare the ports for firmware updates, depending on how the ports are configured:
   - Natively where the IP address is configured on the port. If the adapter port is configured natively, no further action is required. You can proceed with the firmware update without making changes to the configuration.

     Go to step 7 on page 101⌂
   - Part of EtherChannel. If the adapter port is part of EtherChannel and an IP address is configured on EtherChannel, complete the following steps:
     a. Run the command "`ifconfig enX detach`" to remove the IP address where *enX* is the EtherChannel device interface (e.g. en7)
     b. Remove the EtherChannel device by running the command, "`rmdev -l entX`" where *entX* is the EtherChannel device e.g ent7
     c. Go to step 6⌂
   - Part of Shared Ethernet Adapter (SEA). If the adapter port is part of SEA and an IP address is configured on SEA, complete the following steps:
     a. Run the command "`ifconfig enX detach`" to remove the IP address where *enX* is the SEA device interface (e.g. en9)
     b. Remove the EtherChannel device by running the command, "`rmdev -l entX`" where *entX* is the SEA device (e.g ent9)
     c. Go to step 6⌂
   - Part of EtherChannel, which is configured as part of SEA. If the adapter port is part of EtherChannel, which is configured as part of SEA, and an IP address is configured on SEA. For example, ent9 is SEA which uses ent7, ent7 is EtherChannel, and the IP address is configured on en9:
     a. Run the command "`ifconfig enX detach`" to remove the IP address where *enX* is the SEA device interface (e.g. en9)
     b. Remove the SEA device by running the command, "`rmdev -l entX`" where *entX* is the SEA device (e.g. ent9)
     c. Remove the EtherChannel device by running the command, "`rmdev -l entX`" where *entX* is the EtherChannel device (e.g ent7)
     d. Go to step 6⌂
   - Part of SEA (either directly or via EtherChannel) and the VLAN pseudo device is configured on top of SEA. If the adapter port is configured as part of SEA (either directly or via EtherChannel), the VLAN pseudo device is configured on top of SEA, and the IP address is configured on top of VLAN pseudo device. For example, ent10 is VLAN pseudo device, ent9 is the SEA, ent7 is the EtherChannel, and the IP address is configured on en10:
     a. Run the command "`ifconfig enX detach`" to remove the IP address where *enX* is the VLAN pseudo device interface (e.g. en10)
     b. Remove the VLAN pseudo device by running the command, "`rmdev -l entX`" where *entX* is the VLAN device (e.g. ent10)
     c. Remove the SEA device by running the command, "`rmdev -l entX`" where *entX* is the SEA device (e.g. ent9)
     d. Remove the EtherChannel device by running the command "`rmdev -l entX`" where *entX* is the EtherChannel device (e.g ent7)
     e. Go to step 6⌂

6. Reconfigure the IP address and default gateway saved in step 3 on page 99. If the adapter was not configured natively, choose the adapter that was part of SEA or EtherChannel device to configure the IP address:
   a. To configure IP address, run the command

```
ifconfig enX <IP address> netmask <netmask value>
```

where *enX* is the interface of the chosen adapter. Use the IP address and netmask value saved in step 3 on page 99.

b. Configure the default route by running the command,

```
"route add 0 <default gw>"
```

. Determine the value of *default gw* from the output of netstat -rn command saved in step 3 on page 99.

c. Verify the network connectivity with the IBM FSM. If the IBM FSM is reachable, the firmware update is successful.

d. If the chosen adapter was part of EtherChannel and the IBM FSM is not reachable, try the next adapter in EtherChannel and follow steps a through c. For example, if ent0 and ent1 were in EtherChannel and ent0 did not work, try ent1.

7. After the IBM FSM is reachable from a VIOS console, the firmware update can be performed:

a. Refer to Step 1 of 3.8.2.2, "Updating Power Systems network adapters and hard disk drives," on page 98.

Note: In Step 3 of that procedure, do not select all Power Systems operating systems; select the VIOS server instead.

b. After completing Step 4, on the Acquire Updates page within the Available update types table, the only item that needs to be added to the table is **Power IO Firmware** > **Latest Update**.

c. Continue with step 5 of 3.8.2.2, "Updating Power Systems network adapters and hard disk drives," on page 98.

What to do next

After the firmware update is complete, reboot the VIOS partition.

3.8.2.4 Updating the IBM Flex System FC5052 2-port 16Gb or FC5054 4-port 16Gb Fibre Channel adapter

Complete the following steps to update the firmware for the IBM Flex System FC5052 2-port 16Gb or FC5054 4-port 16Gb Fibre Channel adapter installed in a IBM Flex System p24L Compute Node.

Before you begin

This procedure requires you to download OneCommand Manager from Emulex. In order to download the correct version, you must first determine the current microcode level. Before you begin, ensure that you have the ability to download these files, and to transfer them via USB key or SCP to the target compute node. In addition, you must download the firmware update and use a USB key or SCP to copy the update to the target compute node.

Procedure

1. Determine the current microcode level for the installed version of Linux.

Note: The following steps are for Linux systems running the 2.6 kernel (Red Hat or SuSE), which support the /sys filesystem. These steps assume you are logged in with root permissions and that at least one IBM Flex System FC5052 2-port 16Gb Fibre Channel adapter (Feature Code: EC23) or IBM Flex System FC5054 4-port 16Gb Fibre Channel adapter (Feature Code: EC2E) is installed.

a. Use SSH to establish a session to the compute node operating system.

b. Display the model description for each installed Fibre Channel adapter. The number of displayed descriptions should match the number of ports for the adapter to be displayed.

Type the following command to display a list showing the /sys/class/scsi_host/host{n}:description for each installed adapter:

```
find -L /sys/class/scsi_host/host* -maxdepth 1 -name "modeldesc" -printf %h:
 -exec cat {} \; | grep '5052\|5054'
```

The output will be similar to the following list.

```
/sys/class/scsi_host/host0:IBM Flex System FC5054 47C9999 4-port 16Gb FC Adapter
 /sys/class/scsi_host/host1:IBM Flex System FC5054 47C9999 4-port 16Gb FC Adapter
 /sys/class/scsi_host/host2:IBM Flex System FC5054 47C9999 4-port 16Gb FC Adapter
 /sys/class/scsi_host/host3:IBM Flex System FC5054 47C9999 4-port 16Gb FC Adapter
```

Record the host{n} values for use in the next step.

Note: If the list is empty, make sure that you typed the command correctly and that there is at least one adapter installed in the compute node.

c. Display the firmware version for **each** model adapter listed in the previous step.

Type the following command, replacing *host{n}* with the value listed for each adapter in the previous step.

```
cat /sys/class/scsi_host/host{n}/fwrev
```

Note: The microcode version listed might vary but output will be similar to the following example (four numbers separated with ".", sli-4:2:b:)

```
 1.1.37.0, sli-4:2:b
```

If one or more adapter lists a microcode version that is not the latest version, then the microcode update should be applied.

d. Display the version of the Linux operating system installed on the compute node.

- If RHEL is installed, type the following command to display the version:

  ```
  cat /etc/redhat-release
  ```

  The output should be similar to the following:

  ```
  Red Hat Linux Server release 6.4 ()
  ```

  If SuSE (SLES) is installed, type the following command to display the version:

  ```
  cat /etc/SuSE-release
  ```

  The output should be similar to the following:

  ```
  SUSE Linux Enterprise Server 11 (ppc64)
  VERSION = 11
  PATCHLEVEL = 3
  ```

2. Use the Emulex **hbacmd** utility to update the firmware.

a. Download OneCommand Manager

Firmware updates on Fibre Channel adapters installed in a Linux system require the use of the Emulex **hbacmd** utility. The **hbacmd** utility is included in the Emulex OneCommand CLI Applications Kit, which can be downloaded from the following website:

http://www.emulex.com/downloads/oem-qualified-downloads/ibm/drivers-for-ibm-power/

From a computer with access to the internet, complete the following steps:

1) In the Drivers and Management Software for Linux box, choose the operating system that is installed on the compute node.
2) Select the appropriate service pack or update (based on step 1d).
3) From the Download page, verify the operating system information. Then select the **Management and Utilities** tab.
4) Choose the link for **Application Kit <*version*>** (CLI) that matches the operating system installed on the compute node.
5) When prompted, save the Application Kit. For example, you can save the file elxcmcore-xxxx-xxxx-x.x.x.x-x.tgz to the /tmp directory.

6) Transfer the file to a USB drive, or use SCP to transfer the file to a directory on the compute node.

7) Unpack the .tgz file:

```
tar xzf elxcmcore-xxxx-xxxx-x.x.x.x-x.tgz
```

8) Change directories to elxcmcore-xxxx-xxxx-x.x.x.x-x and install the utility:

```
./install.sh
```

9) After the utility is installed, you can verify that it was installed successfully by running the following command:

```
/usr/sbin/ocmanager/hbacmd version
```

b. Make sure that all I/O activity to storage devices controlled by the adapter is stopped before proceeding. When you update the firmware, the adapter will be reset.

c. Update the firmware.

1) List the installed Emulex adapters:

```
/usr/sbin/hbacmd listhbas
```

The result of this command will be similar to the following output with one section for each discovered adapter.

Note: For each adapter, make a note of the Port WWN: value. The Port WWN values will be required as an argument for commands in next steps.

```
Manageable HBA List

Port WWN       : 10:00:00:90:fa:14:5a:f2
Node WWN       : 20:00:00:90:fa:14:5a:f2
Fabric Name    : 10:00:00:27:f8:05:68:19
Flags          : 8000e200
Host Name      : 7895-23x-1-lp2
Mfg            : Emulex Corporation
Serial No.     : 123456789
Port Number    : 0
Mode           : Initiator
PCI Bus Number : 1
PCI Function   : 0
Port Type      : FC
Model          : 47C9999
```

2) List the hba attributes for each adapter port that was listed in the previous step:

```
/usr/sbin/hbacmd hbaattributes {wwpn}
```

where *{wwpn}* is one of the port WWPN values listed in the previous step.

The result will look similar to the following and lists the current version of firmware. Record the current operational firmware values to compare against the values after the update.

```
HBA Attributes for 10:00:00:90:fa:14:5a:f2
Host Name                     : 7895-23x-1-lp2
Manufacturer                  : Emulex Corporation
Serial Number                 :  123456789
Model                         : 47C9999
Model Desc                    : IBM Flex System FC5054 47C9999 4-port 16Gb FC Adapter
Node WWN                      : 20 00 00 90 fa 14 5a f2
Node Symname                  : Emulex 47C9999 FV1.1.37.0 DV8.3.5.68.5p
HW Version                    : 0000000b
FW Version                    : 1.1.37.0
Vendor Spec ID                : 10DF
Number of Ports               : 1
Driver Name                   : lpfc
Device ID                     : E200
HBA Type                      : 47C9999
Operational FW                : 1.1.37.0
IEEE Address                  : 00 90 fa 14 5a f2
Boot Code                     : Enabled
Boot Version                  : KT8.02a10
```

```
Driver Version               : 8.3.5.68.5p; HBAAPI(I) v2.3.b, 07-12-10
Board Temperature            : Normal
Function Type                : FC
Sub Device ID                : E282
PCI Bus Number               : 1
PCI Func Number              : 0
Sub Vendor ID                : 10DF
Service Processor FW Name    :  1.1.37.0
ULP FW Name                  : 1.1.37.0
FC Universal BIOS Version    : KT8.02a10
FC x86 BIOS Version          : KA6.01a12
FC EFI BIOS Version          : KD6.01a13
FC FCODE Version             : KN4.02a14
Flash Firmware Version       : 1.1.
```

d. Update microcode on each of the model adapter ports, one at a time.

   This step assumes that microcode image is located in the `/lib/firmware` folder.

   Important: Do not interrupt or power off the system while firmware updates are in progress.

   Run the following commands to update the firmware:

   `/usr/sbin/hbacmd download {wwpn} /lib/firmware/YXXXXX.grp`

   Where *{wwpn}* is one of the port WWN values listed for the Emulex adapters.

e. Repeat the previous step for each adapter port that needs the firmware update (using each of the WWPNs listed.

f. Restart the compute node to load the new firmware.

g. After restarting the compute node, verify the firmware versionsfor each adapter port using the command:

   `/usr/sbin/hbacmd hbaattributes {wwpn}`

3.8.3 Updating X-Architecture compute nodes

Before updating the firmware for X-Architecture compute nodes, make sure that you have read the prerequisites list.

The prerequisites are described in 3.2, “Prerequisites,” on page 70.

Important considerations:

- If you plan to update multiple X-Architecture compute nodes that are running different operating systems concurrently, and one or more of those compute nodes is running VMware ESXi, make sure that you update all X-Architecture compute nodes running ESXi separately from compute nodes running other operating systems. For example, if you have X-Architecture compute nodes running ESXi, Windows, and Linux:

  1. Update the compute nodes running ESXi concurrently.
  2. Update the compute nodes running Windows and Linux concurrently.

  If you do attempt to update firmware for compute nodes that are running different operating systems and you receive a "File not found" error for a compute node, attempt to update the firmware for just that compute node.

- You **must** install IBM Customization Patch 1.2 or later on each compute node running VMware vSphere ESXi 5.0.x/5.1.x/5.5.x. There is a separate customization patch for each version of VMWare.

  If you are running VMware vSphere ESXi 5.5.x (update 1) or earlier, you must apply both the Lenovo and the Independent Hardware Vendor (IHV) customization patches (Patch 1.2) on every compute node. If you are running VMware vSphere ESXi 5.5.x (update 2), you need not apply Patch 1.2.

  In addition to the IBM Customization Patch 1.2, make sure that you install one of the following updates to the VMware vSphere ESXi operating system:

  - If you are running VMware vSphere ESXi 5.0, make sure that you install update 5.0u2 (update 2)
  - If you are running VMware vSphere ESXi 5.1, make sure that you install update 5.1u1 (update 1)

  When you install an IMM update on an X-Architecture compute node, the Integrated Management Module (IMM) is reset, which can cause a VMware vSphere ESXi system failure (host purple diagnostic screen) if you attempt to update an X-Architecture compute node on which the minimum level of VMware is not installed (5.0u2 or 5.1u1).

  For information about obtaining the IBM Customization Patch 1.2, see the following location:

  http://www.ibm.com/support/entry/portal/docdisplay?lndocid=MIGR-5092679

  Make sure that you review the information provided in the readme for the patch. It contains instructions for installing the patch on a compute node.
- If you are attempting to update the ServeRAID M5115 PSoC3 update to version 68, see 7.27, "The ServeRAID M5115 PSoC3 update package cannot be installed from IBM FSM or UXSPI," on page 152.
- The Emulex firmware update requires either the Corekit or the OneCommand Manager (OCM) application to be installed on Microsoft Windows or Linux operation systems before updating compute nodes running those operating systems.
- If the IMM firmware level on X-Architecture compute nodes installed in your chassis is earlier than the December, 2012 release (v1.60, build 1AOO32P) and you want to activate centralized user management on the IBM FSM, you should update the firmware for X-Architecture compute nodes before you enable centralized user management through the IBM FSM.

  Failing to update the firmware in the X-architecture compute nodes first when activating centralized user management, will result in a situation where an X-Architecture compute node with previous IMM firmware levels will show as locked in the IBM FSM user interface. You will not be able to access the IMM externally with any account credentials. In addition, the IBM FSM will not be able to update the firmware for the X-Architecture compute node.

  To avoid this situation, do not enable centralized user management for a chassis until after X-Architecture compute nodes are updated to a firmware level equal to or later than December 2012.

  If you have already activated centralized user management on your IBM FSM, you have X-Architecture compute nodes at IMM firmware level lower than December 2012 (v1.60 build 1AOO32P), and the compute nodes are showing in a locked state in the FSM, see 7.16, "X-Architecture compute node shows as locked on the IBM FSM when using Centralized Management," on page 146 to resolve the issue.

Special considerations for scalable systems:

If you are updating the firmware for a multi-node system (also called a scalable system), such as the Flex System x280 X6, x480 X6, or x880 X6 Compute Node, the IBM FSM keeps the following system firmware at the same level on all physical servers across the system:

- DSA
- IMM
- UEFI

To achieve this, if any system firmware update is needed on the physical server, update manager on the IBM FSM marks the needed relationship on the top level system, also called the cluster system. Then, during installation, the update is applied to all the physical servers in the multi-node system.

Note: Update manager does not support multi-node systems that have ESXi installed on them. You cannot use the IBM FSM to update firmware for these systems.

Consider the following items when updating the system firmware on multi-node systems:

- Before starting any system firmware update processes, ensure that the multi-node systems are discovered with both inband mode and OOB mode. Make sure that all inventory is collected on all the scalable partition systems and the cluster system.

- When checking compliance, the DSA, IMM, and UEFI firmware is shown on the cluster manageable endpoint of the multi-node system instead of on the physical server system or partition system.
- The systems firmware updates are installed to all the physical server systems when you install the update on the multi-node system. All the partition systems are then rebooted after the installation.
- When updating a batch of update packages on multi-node systems, it would be a two-step update:
  1. Install the DSA, IMM, and UEFI firmware updates on cluster system first.
  2. After the task completes successfully, continue to install the rest of the updates on each partition system.

3.8.3.1 VMware ESXi update considerations

Read through the following considerations if you are running VMware ESXi on X-Architecture compute nodes.

- If you are updating an ESX or ESXi system that is configured for virtual switch (vswitch) and there is no physical network adapter associated with the virtual switch, inventory collection from the IBM FSM will fail. See 7.24, "Inventory collection on compute nodes running ESX or ESXi consistently fails, which means that firmware update will not be deployed," on page 150 to resolve this issue.
- Before updating the firmware for a compute node that is running ESXi, make sure that you enable maintenance mode. For information about enabling maintenance mode, see the documentation that is provided with ESXi.
- When updating a compute node running VMware ESXi, the host must be fully initialized before the update process starts. Make sure you wait for the full compute node initialization to complete, which takes approximately 20 minutes.

  If the host is not fully initialized, you might see an error with the update or an error stating that the system failed to restart, and that it must be restarted manually (even if you choose to have the compute node restarted automatically after the update). If you see this error, restart the compute node manually. If there are no other errors listed, the firmware update was successful.
- The following ESXi images are supported by the IBM FSM:
  – The standard ESXi image. If you deployed the standard ESXi image, the IBM FSM is limited to updating the UEFI, preboot DSA, and IMM firmware.

    You must be running one of the following ESXi versions:
    - VMware vSphere ESXi 5.0. Make sure that, at a minimum, you are running version 5.0u2 (update 2)
    - VMware vSphere ESXi 5.1. Make sure that, at a minimum, you are running version 5.1u1 (update 1).
    - VMware vSphere ESXi 5.5 (any version)

      Note: When you install an update to the Integrated Management Module (IMM) on an X-Architecture compute node, the IMM is reset. In this case, if you have not installed (at a minimum) update 5.0u2, 5.1u1, or 5.5.x, a VMware vSphere ESXi system failure (host purple diagnostic screen) might occur.
  – The VMware vSphere Hypervisor (ESXi) with IBM Customization. If you deployed ESXi with IBM Customization, the IBM FSM can also update firmware for network (I/O) adapters and LSI RAID controllers.

    Note: Hard drive updates from the IBM FSM are not supported.

    Note: BNX1 and BNX2 firmware updates are not supported on ESXi Customized Image with Patch 1.2

    For best performance, consider running one of the following ESXi versions:
    - VMware vSphere ESXi 5.0. Make sure that, at a minimum, you are running version 5.0u2 (update 2)

- VMware vSphere ESXi 5.1. Make sure that, at a minimum, you are running version 5.1u1 (update 1).

  If you deploy ESXi with IBM Customization through the IBM FSM operating system deployment task (IBM FSM version 1.3.0 or 1.3.1), you will be running version 5.1u1.
- VMware vSphere ESXi 5.5 (any version)

Note: When you install an update to the Integrated Management Module (IMM) on an X-Architecture compute node, the IMM is reset. In this case, if you have not installed (at a minimum) update 5.0u2 5.1u1, or 5.5, a VMware vSphere ESXi system failure (host purple diagnostic screen) might occur.

To validate that you are running the IBM-customized version, check that the file `/etc/cim/ibm/imm_fw_schema` exists on the image. This file should contain lines indicating that the SCHEMA_STATE is "check" and showing a version number for the FW_VERSION field. To review the list of custom providers, use the command "**`esxcli software vib list`**" on your ESXi server.

Tip: You can compare this list with the list provided in the readme for Patch 1.2.

Complete the following steps to update a compute node that is running VMware vSphere ESXi with IBM Customization:

1. Make sure that you are running at least VMWare ESXi version 5.0u2 5.1u1, or 5.5.x. If not, you will need to upgrade to one of those versions before proceeding.
2. Install IBM Customization patch 1.2, which can be found at this location:

   Note: There is an IBM Customization patch 1.2 for each VMWare version 5.0.x, 5.1.x and 5.5.x.

   http://www.ibm.com/support/fixcentral/systemx/quickorder?parent=x220+Compute+Node&product=ibm/systemx/2585&&platform=All&function=fixId&fixids=ibm_sw_hyper_patchbundlv8_vmwaresx5_32-64&includeRequisites=0&includeSupersedes=0&downloadMethod=http&source=fc

   For more information about obtaining the IBM Customization patch 1.2, see the following location:

   http://www.ibm.com/support/entry/portal/docdisplay?lndocid=MIGR-5092679
3. Install the drivers for each of the adapters that are installed in the compute node. You can find information about these driver updates by going to the following website:

   http://www.ibm.com/support/fixcentral/

   From the Fix Central site, select the following fields:
   - **Product Group**: PureSystems
   - **Select from PureSystems**: PureFlex System
   - **Select from PureFlex System**: Compute Node
   - **Select from Compute Node**: The compute node on which the ESXi image is installed

   Select the appropriate device drivers based on the adapters that you have installed. Follow the instructions provided with the driver update to install the driver.
4. Apply the firmware updates based on the procedure listed in 3.8.3.2, "Installing X-Architecture compute node updates," on page 108.

- If storage paths are lost for any reason in a configuration with VMware, CN4022, and storage devices, the paths might recover. Paths also might recover and then fail again in about 5 to 45 minutes.

  You can recognize lost paths with the following command:

  ```
  esxcfg-mpath -L | grep dead
  ```

  The paths can be recovered by issuing the following command:

  ```
  esxcli storage filesystem rescan -a
  ```

  To reduce potential issues, update one SVC controller, making sure the paths have a chance to settle and recover with the rescan command. Then update the second SVC controller.

3.8.3.2 Installing X-Architecture compute node updates

Use this procedure to install updates for X-Architecture compute nodes

Before you begin

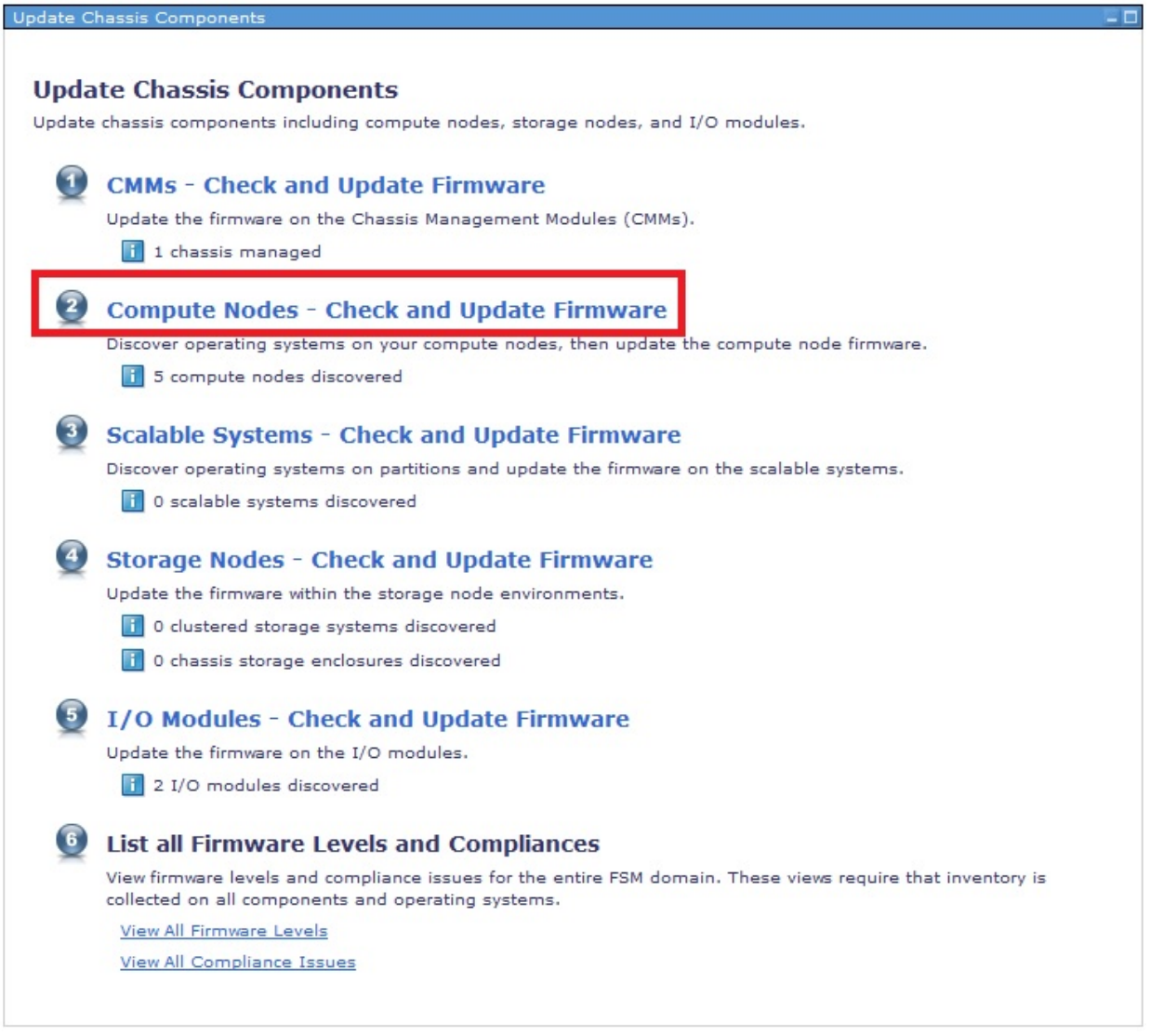
Make sure that you have read all prerequisites, which are listed in 3.2, “Prerequisites,” on page 70. In addition, make sure that you have performed the procedures described in 3.3, “Preparing for updates,” on page 74.

Procedure

Complete the following steps to install updates for X-Architecture compute nodes:

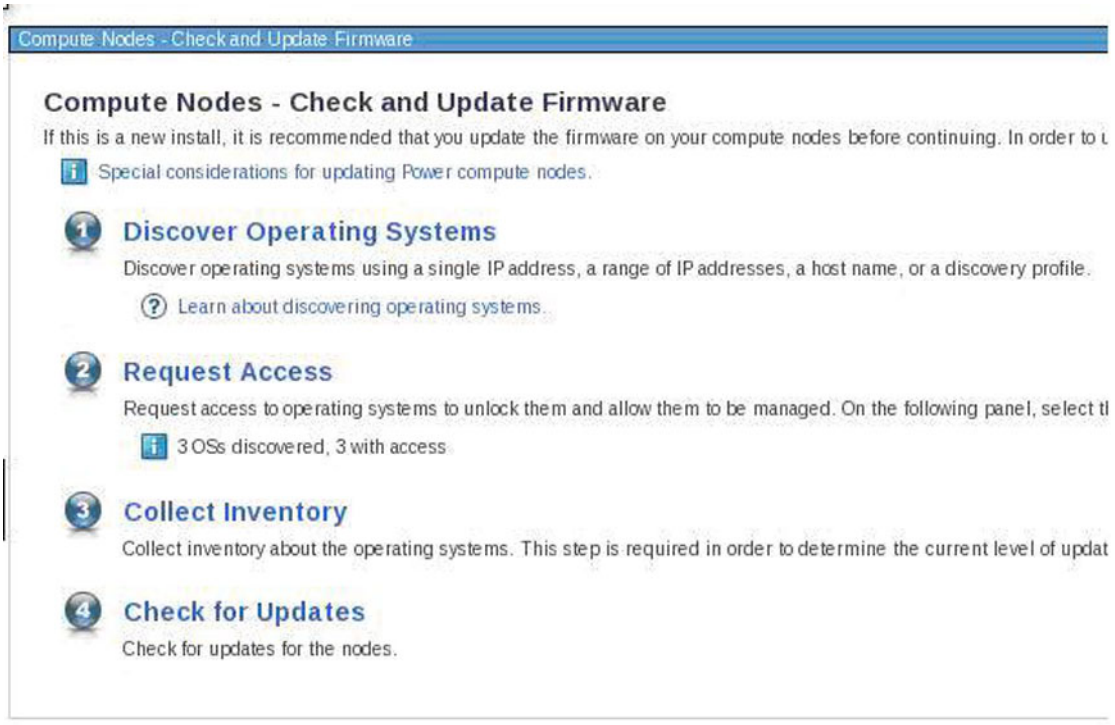
1. From the IBM FSM home page, click the **Initial Setup** tab.
2. Click **Update Chassis Components**; then click **Compute nodes** > **Check and Update Firmware**.

   Note: If you are updating the firmware for a multi-node system (also called a scalable system), such as the Flex System x280 X6, x480 X6, or x880 X6 Compute Node, click **Scalable Systems - Check and Update Firmware**.



For X-Architecture compute nodes, there are four steps required for checking and updating firmware:

a. Discover operating systems
b. Request access to all operating systems
c. Collect inventory for the operating systems
d. Check for updates



If you discovered the operating systems as they were installed and collected inventory on the chassis components (see 3.3.1, “Making sure that the IBM FSM is managing the chassis,” on page 74), the operating systems should already be discovered for the X-Architecture compute nodes that you will be updating. In addition, the IBM FSM should have full access to those operating systems. Therefore, you can skip to 

.

If you need to discover the operating systems or request full access to the compute nodes, you can click 

, and 

. Otherwise, proceed with 

.

Tip: The update task is referred to as a job task. If you are not familiar with job tasks in the IBM FSM, see A.1, “Starting a job task,” on page 155.

.

After the collect inventory job has completed, click 

, which will open the Acquire Updates wizard.

3. You should have already copied the updates to the IBM FSM and imported the updates into the updates library. If not, see 3.4, “Obtaining all updates,” on page 79 for more information.

   Important consideration

   If Platform Agent is installed on a compute node, you must update the Platform Agent on that compute node before you update the firmware for that compute node.

4. Acquire the updates.

a. From the Acquire Updates page, select **Import file from the file system** and specify a valid path. Then click **OK**.

   Note: Even though you have already copied updates over to the IBM FSM and then imported those updates to the IBM FSM updates library (and deleted the updates from the directory where you copied them), you must still enter a valid path, such as `/home/USERID` in the Acquire Updates wizard. You might receive an error stating that no updates were found, but you can ignore that error and proceed with the next step to show all updates for a component.

b. From the Schedule tab on the Launch Job window, select **Run Now**.

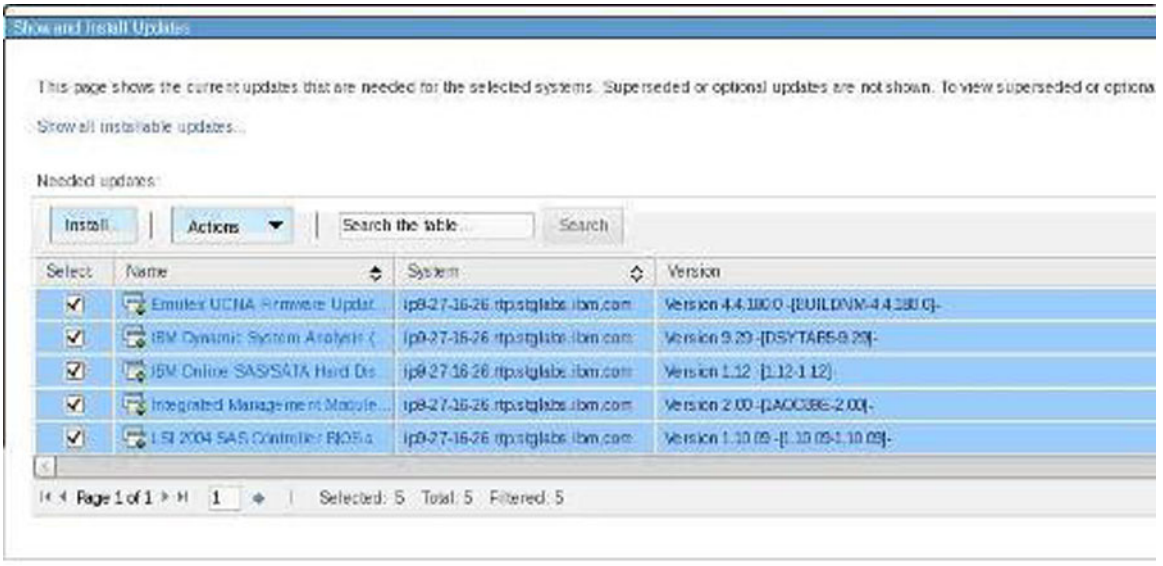
c. From the message confirming that the job was created and started successfully, click **Display Properties** to monitor the job status (displays the Active and Scheduled Jobs page).

d. After the update has been imported successfully, close the **Active and Scheduled Jobs** page.

5. Install the updates

   a. When the acquire task has completed, click **Show and Install Updates**.

   b. Select the updates to apply to the X-Architecture compute nodes, and then click **Install** to start the Install wizard.



   Select all the updates by selecting **Actions** > **Select All**. Then click **Install** to start the Install Wizard.

   Tip: Consider selecting the option **Automatically restart as needed during installation**.

   Note: If you are updating a compute node running ESXi and the host is not fully initialized, you might see an error stating that the system failed to restart, and that it must be restarted manually

even if you chose **Automatically restart as needed during installation**. In you see this error, restart the compute node (if there are no other errors listed, the firmware update was successful).

c. Proceed to summary screen which summarizes the updates that will be installed. Click **Finish**.
d. In the Launch Job window, go to the Schedule tab and select **Run Now**. Then click **OK**.

Tip: The update task is referred to as a job task. If you are not familiar with job tasks in the IBM FSM, see A.1, "Starting a job task," on page 155.

What to do next

You can verify the update completed successfully by looking in the Task Log Steps and verifying that each step completed with status Complete. For information about validating that the job completed successfully, see A.4, "Verifying an update completed successfully," on page 161.

3.8.3.2.1 Updating firmware using UXSPs:

If you are updating firmware and device drivers for an X-Architecture compute node that already has an operating system loaded on the compute node, use UpdateXpress System Packs (UXSPs) and the UpdateXpress System Pack Installer (UXSPI)

About this task

The following procedure explains how to use UXSP and UXSPI to update a compute node that is running Windows 2008. For more information about using UXSP and UXSPI, see the following Website:

http://publib.boulder.ibm.com/infocenter/toolsctr/v1r0/topic/uxspi/uspi_main.html

Procedure

1. Download the UXSP and the UXSPI (UXSP installer) that maps to the operating system being run on the Flex System x240 X-Architecture compute node to be updated. For example, if you are updating a compute node that has Windows 2008 installed, you would download the following UXSP and UXSPI.
   - Flex System x240 Compute Node UpdateXpress System Pack for Windows 2008 x64, Windows 2012 x64 (ibm_utl_uxsp_b2sp09p-1.40_windows_32-64)
   - UpdateXpress System Pack Installer (ibm_utl_uxspi_9.30_winsrvr_32-64)

   Tip: For information about obtaining these packages, see 3.4.3, "Downloading X-Architecture compute node updates," on page 82

Note: Lenovo UXSPI and ToolsCenter tools are needed to update the Lenovo components. Lenovo ToolsCenter can be downloaded from the following websites:

- http://www.ibm.com/support/entry/portal/docdisplay?lndocid=LNVO-CENTER
- http://www.ibm.com/support/entry/portal/docdisplay?lndocid=LNVO-XPRESS
- http://www.ibm.com/support/entry/myportal/docdisplay?lndocid=LNVO-BOMC

2. Use a tool like Remote Desktop to log in with Administrator privileges to copy the updates and run UXSPI.
   a. Create a directory on the compute node where the update will be stored (such as `c:\tmp\uxsp`).
   b. Use SCP to copy the UXSP and UXSPI packages to the directory that you just created.
   c. Using Remote Desktop, navigate to the directory where the files were copied and run the installation program.

      ```
      ibm_utl_uxspi_9.30_winsrvr_32-64.exe update -u
      ```

      This command will update the firmware and devices drivers in unattended mode. Information about the parameters that you can use with this command are available at the following Website:

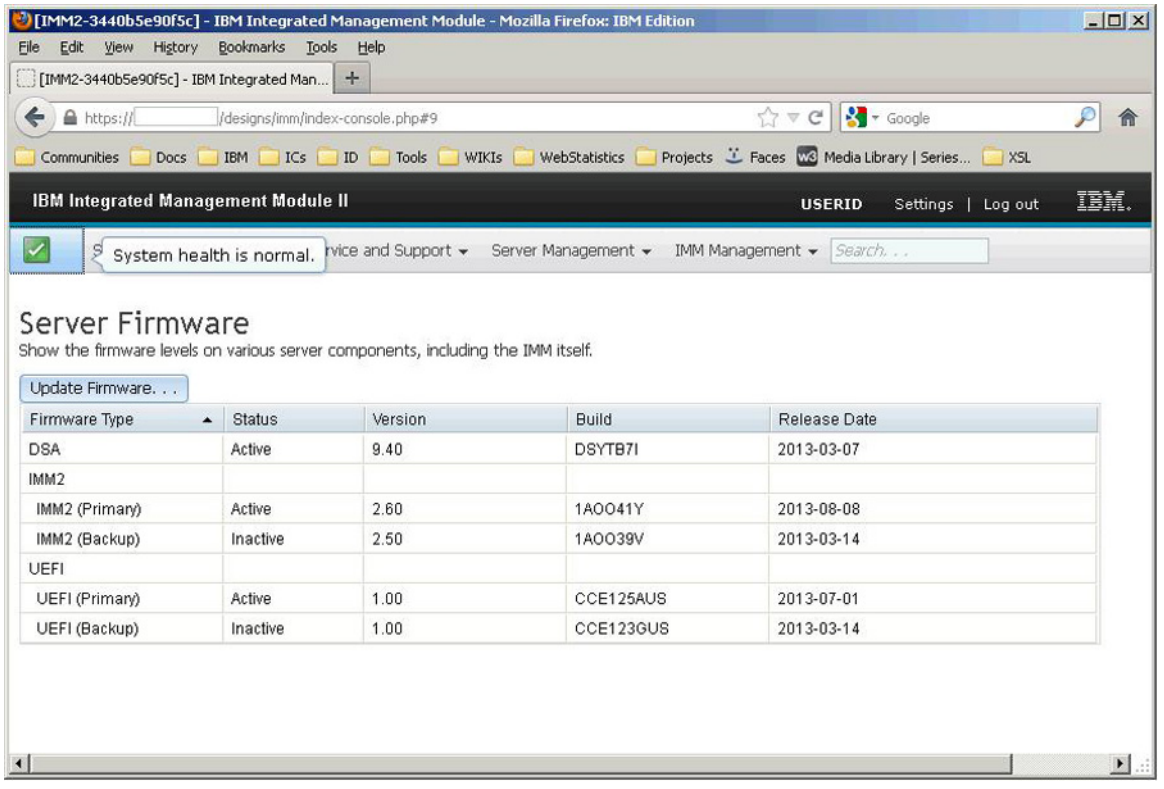
      http://publib.boulder.ibm.com/infocenter/toolsctr/v1r0/topic/uxspi/uspi_r_using_compare_update.html#uspi_r_using_compare_update

      Tip: Run `ibm_utl_uxspi_9.30_winsrvr_32-64.exe` with no parameters to start the graphical user interface.
3. Restart the X-Architecture compute node for the updates to take effect.

What to do next

Validate that the IMM, UEFI, and pDSA updates were installed successfully.

1. Log in to the IMM interface for the X-Architecture compute node.
2. Click **Server Management** > **Server Firmware** to valudate that the current versions are installed.



3.8.3.3 Determining which specific updates need to be installed

When you imported an UXSP update, the IBM FSM will show that the UXSP update needs to be installed, but it does not list the individual updates (such as IMM, UEFI, or pDSA) that are needed from the UXSP package.

Procedure

To determine the individual updates that need to be applied for a compute node, complete the following steps:

1. From the Chassis Manager, click an X-Architecture compute node to select it.
2. In the Details section at the bottom of the panel, click **Actions** > **Related Resources** > **Update** > **Server Needs**.

   Tip: Not all updates, such as driver updates will show in this list. To select the full list of available updates, click **Actions** > **Release Management** > **Show and install updates**. Then click the link **Show all installable updates** to see a full list of updates that can be installed.
3. The Resource Explorer panel is displayed, which provides a list of the specific updates that need to be applied.

3.9 Updating storage nodes

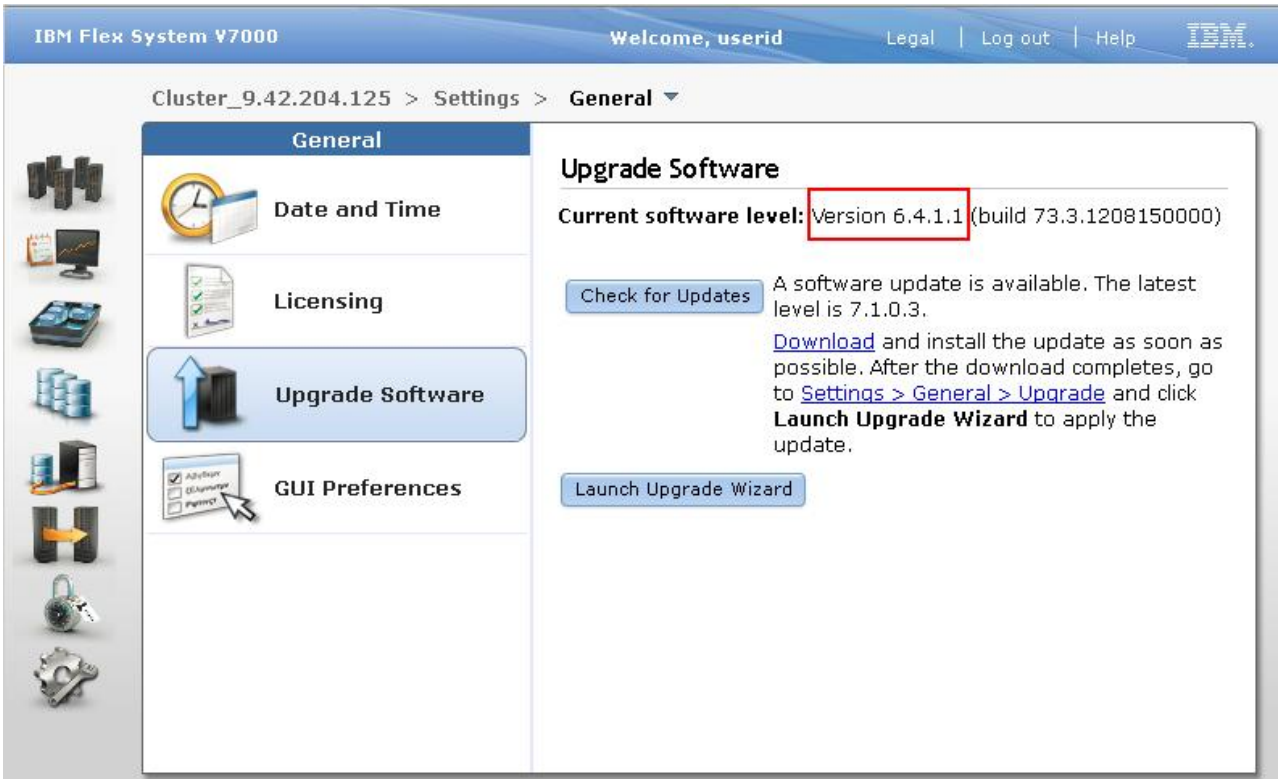
Use the IBM FSM to update the firmware and software for the IBM Flex System V7000 storage node.

Important Consideration:

Before you attempt to upgrade the Flex System V7000 storage node through the IBM FSM, you must check the version of firmware that is currently installed on the Flex System V7000 storage node.

- If the currently installed version is 6.4.1.x, you can update the Flex System V7000 storage node from the IBM FSM.
- If the currently installed version is 7.1.0.3 or greater, you can update the Flex System V7000 storage node from the IBM FSM.
- If the currently installed version is 7.1.0.x (and not 7.1.0.3), do not upgrade the Flex System V7000 storage node from the IBM FSM. Instead, follow the procedures listed in 4.4, “Updating Flex System V7000 Storage Nodes,” on page 130.

To determine what version is installed, log in to the cluster management interface from the CMM. From the Flex System V7000 home page, click **Settings** > **General** to see the version number.



For more information about setting up the IBM Flex System V7000 storage node from the IBM FSM, see the following website:

http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.4939.doc/site_qicfgsys_FSM.html

For more information about managing an IBM Flex System V7000 storage node manually, see the following website:

http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/managing_flex_system_v7000_manually.html

3.9.1 Installing a storage node update from an IBM FSM that is not connected to the Internet

Follow the steps in this procedure to update the storage node.

Procedure

Complete the following steps for ***each*** storage node:

1. From the Chassis Manager, select the storage node.
2. Collect inventory on the selected storage node. Under Common Actions, select **Inventory** > **Collect Inventory**.

   Tip: Collecting inventory is a job task. If you are not familiar with job tasks in the IBM FSM, see A.1, "Starting a job task," on page 155.
3. You should have already copied the updates to the IBM FSM and imported the updates into the updates library. See 3.4, "Obtaining all updates," on page 79 for more information..
4. Install the update on the storage node by selecting action **Release Management** > **Show and Install Updates** and run the Install Updates task.

   Tip: The update task is referred to as a job task. If you are not familiar with job tasks in the IBM FSM, see A.1, "Starting a job task," on page 155.
   .

What to do next

You can verify the update completed successfully by looking in the Task Log Steps and verifying that each step completed with status Complete. For information about validating that the job completed successfully, see A.4, "Verifying an update completed successfully," on page 161.

Important consideration:

Additional updates, such as hard disk drive updates can be applied to the IBM Flex System V7000 storage node, but these updates are not applied through the IBM FSM update process.

3.9.2 Obtaining additional updates for the IBM Flex System V7000 storage node

Additional updates, such as hard disk drive updates can be applied to the IBM Flex System V7000 storage node but these updates are not applied through the IBM FSM update process.

Procedure

Additional storage node updates can be found by completing the following steps:

1. Open a Web browser and navigate to the IBM Fix Central website: http://www.ibm.com/support/fixcentral/
2. In the Product Group field, select **Software** > **PureSystems** > **PureFlex System** > **Storage Node**. Then select **Flex System V7000** for the storage node and click **Continue**.
3. In Installed Version field, select **All**.
4. In Platform field select **All**; then click **Continue**.
5. Select each of the updates to be applied; then click **Continue**.
6. Sign in with your IBM ID and download the updates. Follow the directions provided in the documentation that is available with the updates to apply them to the storage node.

What to do next

Third-Party host software updates are installed on third party systems, such as Microsoft Windows Server and are not installed directly on or by the IBM FSM or the IBM Flex System V7000 Storage Node.

The IBM FSM does not support updating hard disk drives on Flex System V7000 storage nodes. Information about updating hard disk drives is available at the following website:

http://pic.dhe.ibm.com/infocenter/flexsys/information/index.jsp?topic=%2Fcom.ibm.acc.4939.doc%2Ftbrd_upgradedrivefirmware.html

---

3.10 Updating I/O modules

Use the IBM FSM to update the I/O modules, which includes both switches and pass-thru modules.

Important considerations:

- When updating an I/O module using the IBM FSM, do not perform configure, update, or perform SNMP operations with the CMM while the update is occurring. Otherwise, the firmware update might not be successful.
- If you use IPv4 and IPv6 for the management node Eth0 (management network interface), each managed chassis and chassis component must have an IPv4 address.
- You cannot update the firmware for the Flex System EN4023 10Gb Scalable Switch through the IBM FSM. Instead, you must use the switch interface to update firmware. More information about updating the firmware is available in the User's Guide provided for the Flex System EN4023 10Gb Scalable Switch:

  http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.networkdevices.doc/Io_module_en4023.html
- If you are attempting to update the firmware for the IB6131 Infiniband Switch or the EN4061 40Gb Ethernet Swtich, see 7.29, “IBM FSM fails to update IB6131 and EN6131 switches,” on page 154.
- The following considerations apply to the Flex System CN4093 10Gb Converged Scalable Switch, the Flex System Fabric EN4093/EN4093R 10Gb Scalable Switches, and the Flex System EN2092 1Gb Ethernet Scalable Switch:
  - If you are updating I/O modules that currently have firmware level of **version 7.7.5.0 or later** installed, you can use a Secure File Transfer Protocol (SFTP) server provided with the IBM FSM to

update the firmware from the IBM FSM. Otherwise, if you update these switches through the IBM FSM, you must use a Trivial File Transfer Protocol (TFTP) server to host updates before they are applied to these switches.

As an alternative to setting up a TFTP server and enabling the menu-based CLI on the I/O module, you can consider updating the firmware for I/O modules directly, which can be done through the Web-based user interface for the I/O module and does not require a TFTP server. In general, if you are updating several I/O modules, consider setting up a TFTP server. To update the firmware for one or two I/O modules, consider updating it directly through the I/O module Web-based user interface.

For information about checking the firmware level of an I/O module or for information about updating the firmware directly through the I/O module interface, see the product documentation that is provided with the I/O module. You can obtain the documentation for I/O modules at this website:

http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.networkdevices.doc/network_iomodule.html

– The switches must be configured to use the menu-based CLI (ibmnos-cli), which is the default command-line interface. If the switch does not use the menu-based CLI, updates from the IBM FSM will fail.

  Tip: You can configure switches so that the CLI mode is determined when an administrator logs in. This way, you do not have to set the CLI mode and restart the switch every time you want to change the mode from iscli to ibm-nos-cli. To configure switches so that the CLI mode is determined upon log in:

  1. Start an SSH session to log in to the switch.
  2. Run the following commands from the ISCLI:

     ```
     enable
     config t
     boot cli-mode prompt
     ```

     From the ibmnos-cli, run the following command:

     ```
     boot/prompt e
     ```

  3. Log out of the SSH session. The next administrative user to log in sets the mode, which stays in effect until all users log out.

  When updating the I/O module firmware, the IBM FSM will use the correct CLI mode.

– Additional CN4093-only considerations:

  - Before updating the firmware for the Flex System Fabric CN4093 10Gb Converged Scalable Switch through the Web interface, make sure that you use the following ISCLI command to save the startup configuration:

    ```
    copy running-config startup-config
    ```

    This will ensure that the settings remain in effect after you apply the firmware updates and restart the switch.

  - Do not perform any switch configuration actions while a CN4093 firmware update is in progress.
  - Immediately after updating the firmware for the CN4093, make sure that you configure the switch to use ISCLI to prevent storage configuration losses:

    1. Start an SSH session to log in to the switch.
    2. Choose iscli mode.
    3. Run the following commands from the ISCLI:

       ```
       enable
       config t
       boot cli-mode iscli
       ```

    4. Log out of the SSH session.

- Flex System FC3171 8 Gb SAN switches **must** be running CPLD version 0x22 or later. Switches with firmware levels of 9.1.0.26.00 and later will show the following error messages if the CPLD was not updated:

  ```
  Installed CPLD version 0x20 older than available version 0x22. See 'help cpld install'
  in the CLI for upgrade instructions.
  ```

  Complete the following steps to update the CPLD, which will require a virtual switch restart.

  1. Update the firmware level on the switch to 9.1.0.27.00 or later and restart the switch.
  2. Log in to the CLI and run the following commands:

     ```
     admin start
     set advanced on
     cpld install
     ```

  3. When CPLD install completes successfully, login to theCMM CLI and run these commands to perform a virtual reseat of the switch:

     ```
     env -T system:switch[x], where x is switch slot
     service -vr
     ```

  4. Verify the CPLD version after the virtual reseat. Run the following commands from the switch CLI:

     ```
     set advanced on
      show setup mfg
     ```

     Look for the line CPLD Revision, which should end in 0x22.

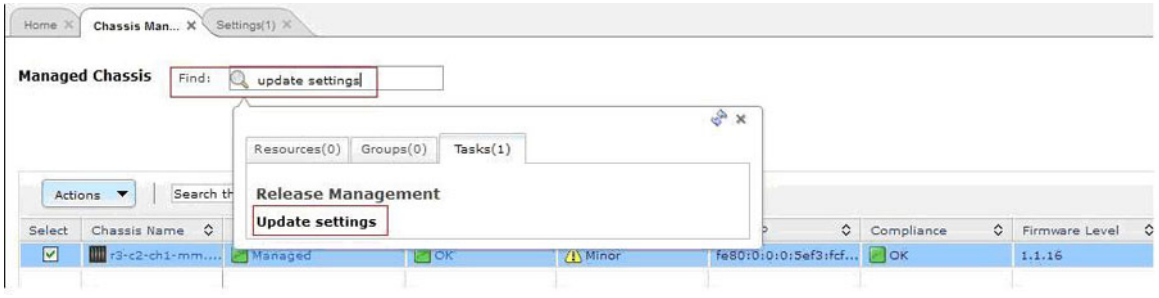
3.10.1 Configuring a TFTP server

If you are updating the firmware for the Flex System CN4093 10Gb Converged Scalable Switch, the Flex System Fabric EN4093/EN4093R 10Gb Scalable Switches, or the Flex System EN2092 1Gb Ethernet Scalable Switch, check the firmware level before updating. If the firmware level currently installed on the I/O module is less than **version 7.7.5.0**, you must use a Trivial File Transfer Protocol (TFTP) server to host updates before they are applied to these switches.

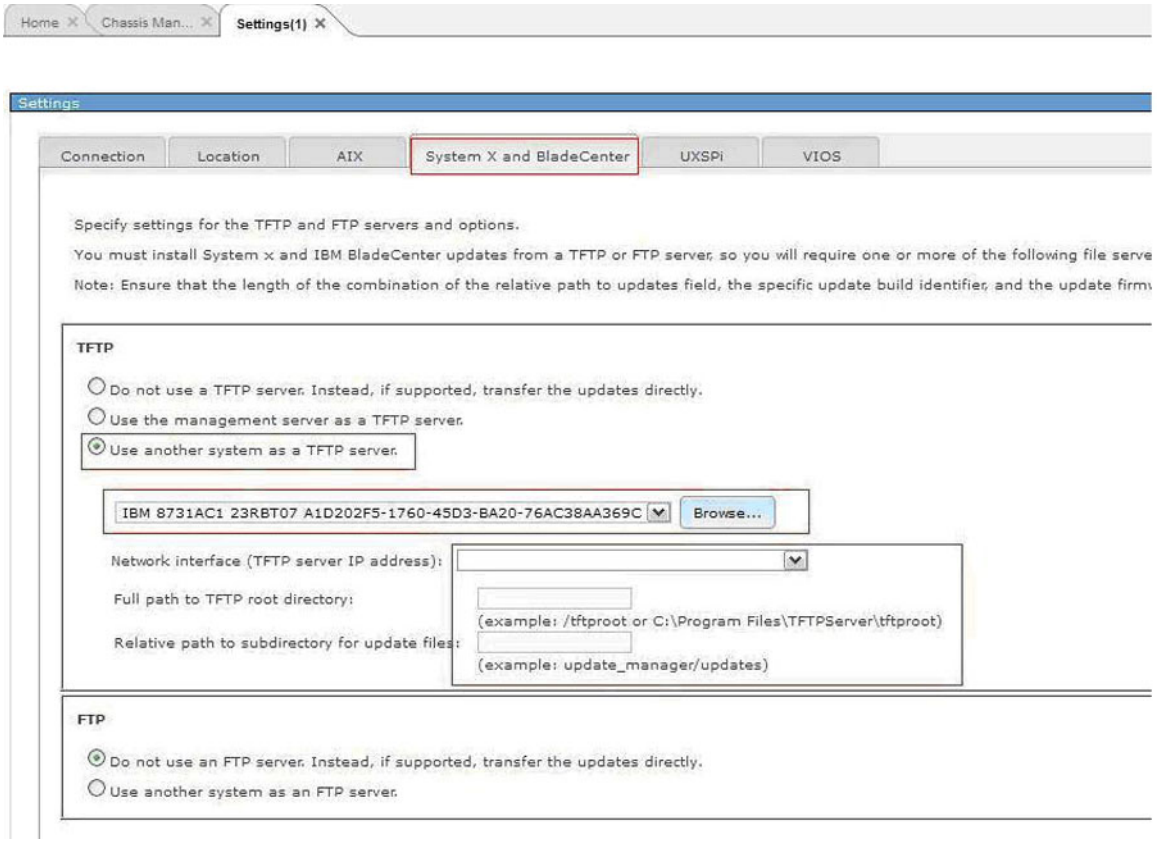
Note: If you install a TFTP on a Power Systems VIOS, make sure that you also install an unzip utility for use when applying updates.

After setting up the TFTP server, configure the IBM FSM to reference the TFTP server:

1. Enter `Update settings` in the Find field from the Chassis Manager tab and click the **Update settings** link under Release Management:



2. On the Settings page, select the **System X and BladeCenter** tab. Then select **Use another system as a TFTP server** and browse for the managed compute node that has the TFTP server installed as shown in this example:



3.10.2 Installing I/O module updates

Perform these steps to update the firmware for I/O modules. Make sure that you perform these steps for **each** I/O module.

About this task

Important consideration:

When updating the firmware for I/O modules, make sure that you update each I/O module sequentially to ensure that you do not lose network connectivity.

Procedure

Complete the following steps to install updates for **each** I/O module:

1. From the Chassis Manager, click the I/O module in the chassis. If you have previously set up full access to the I/O module through the IBM FSM and collected inventory, proceed with Step 4
2. Make sure that the IBM FSM has full access to the I/O module:
   a. In the Details section at the bottom of the Chassis Manager, click **Actions** > **Security** > **Request Access**.
   b. Enter the User ID and credentials to gain access to the I/O module.
   c. Click **Request Access**.

   If you need to request access to I/O modules, see the *Getting full access to Ethernet I/O modules* and *Getting full access to Fibre Channel I/O modules* quick start guides, which are available at the following website:

http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.commontasks.doc/commontasks_chassis_config.html

3. Perform an inventory of the I/O module:
   a. In the Details section at the bottom of the Chassis Manager, click **Actions** > **Inventory** > **Collect Inventory**
   b. Make sure that **Run Now** is selected; then click **OK**.

   Tip: Collecting inventory is referred to as a job task. If you are not familiar with job tasks in the IBM FSM, see A.1, "Starting a job task," on page 155.
4. You must copy the updates to the IBM FSM and import them into the updates library. If you did not do so earlier, see 3.4, "Obtaining all updates," on page 79
5. Apply the update. From the Details section at the bottom of the panel, click **Actions** > **Release Management** > **Show and install updates** to continue.
6. Select the updates to apply to the I/O module and click **Install**.
7. Proceed to summary screen which summarizes the updates that will be installed. Click **Finish** to start the process of updating the I/O module.

   Tip: The update task is referred to as a job task. If you are not familiar with job tasks in the IBM FSM, see A.1, "Starting a job task," on page 155.

What to do next

You can verify the update completed successfully by looking in the Task Log Steps and verifying that each step completed with status Complete. For information about validating that the job completed successfully, see A.4, "Verifying an update completed successfully," on page 161.

After you have updated all I/O modules, you can then update the following components if they are part of your configuration:

- IBM Storwize V7000. See Chapter 5, "Updating the IBM Storwize V7000," on page 133.
- Top-of-rack switches. See Chapter 6, "Updating Top-of-Rack (TOR) switches," on page 135.

Chapter 4. Updating all components in a chassis when an IBM FSM is not present

Updates for an IBM Flex System offering are tested and released together. Therefore, you **must** update all components in a chassis to the same software level, as defined at the IBM PureSystems Center website.

Therefore, it is important to update all components in a chassis together. For more information about obtaining the updates that you will need, see 3.4, "Obtaining all updates," on page 79.

Tip: If you are updating components in a chassis when an IBM FSM is not present, you do not need to download the IBM FSM update.

If you are updating the components in a chassis that is not currently being managed by an IBM FSM management node, you can use the tools that are available with IBM ToolsCenter, such as the UpdateXpress System Pack Installer (UXSPI) to update the CMM and X-Architecture compute nodes.

Important considerations:

- Make sure that you verify the part number of the fan logic modules in your chassis and replace them if necessary.

  ECA083 (Engineering Change Announcement) provides for proactive replacement of the fan logic module in a limited number of IBM PureFlex systems. Details of this announcement and instructions for determining the part number of installed fan logic modules are available at the following location:

  http://www.ibm.com/support/entry/portal/docdisplay?lndocid=MIGR-5093506
- The Emulex firmware update requires either the Corekit or the OneCommand Manager (OCM) application to be installed on Microsoft Windows or Linux operation systems before updating compute nodes running those operating systems.
- Additional limitations for the UpdateXpress System Pack Installer can be found at the following website:

  http://publib.boulder.ibm.com/infocenter/toolsctr/v1r0/index.jsp?topic=%2Fuxspi%2Fuspi_r_limitations.html

For details about ToolsCenter tools, see the Deployment and Updates sections of ToolsCenter at this website:

https://www.ibm.com/support/entry/portal/docdisplay?brand=5000016&Indocid=TOOL-center

For information about using the UpdateXpress System Pack Installer, see the following website:

http://publib.boulder.ibm.com/infocenter/toolsctr/v1r0/topic/uxspi/uspi_main.html

Updates must be applied in the following order:

1. CMM
2. X-Architecture compute nodes.

   For information about updating firmware for X-architecture compute nodes directly, see the following website:

   http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8737.doc/updating_firmware.html

   Note: The process for updating all X-architecture compute nodes is similar.
3. IBM Flex System V7000 Storage Node

For information about updating the firmware on the IBM Flex System V7000 Storage Node with you do not have an IBM FSM managing a chassis, see the following website:

http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.4939.doc/svc_upgradingintro.html

4. I/O modules

   For information about updating I/O module firmware, see the documentation that was provided with the I/O module that you have installed in the chassis.

   The documentation for all I/O modules is available at the following website:

   http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.networkdevices.doc/network_iomodule.html

After you have updated the components in the chassis, update the following components:

1. IBM Storwize V7000
2. Top-of-rack switches

4.1 Updating the CMM

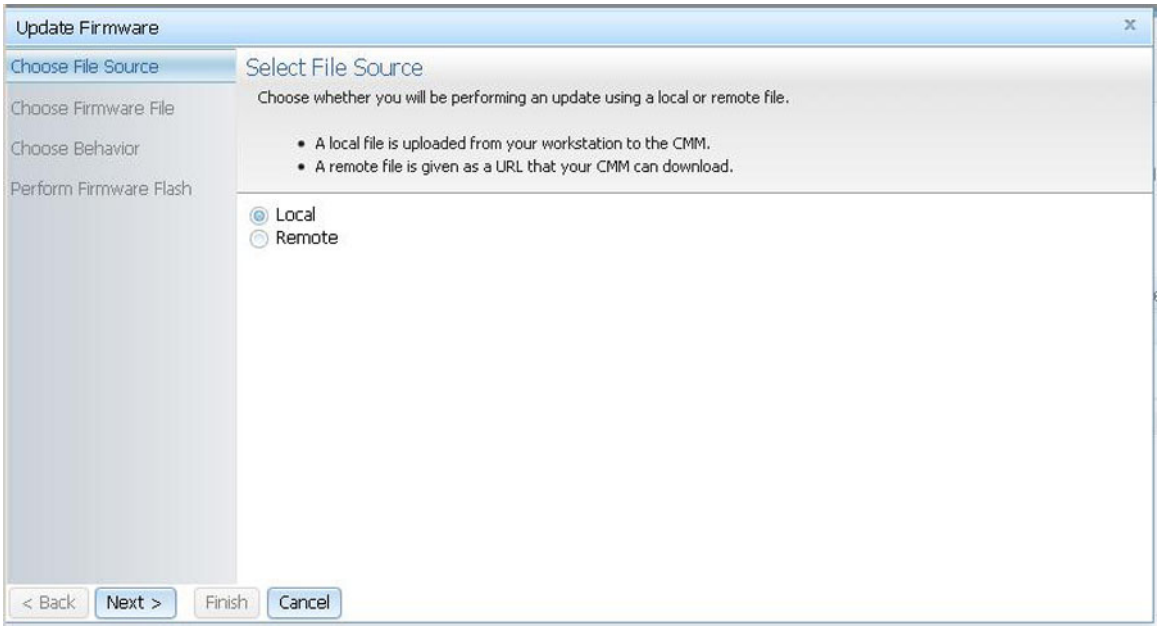
Use this procedure to update the firmware for the CMM through the CMM Web interface.

Before you begin

Make sure that you have downloaded the update for the CMM, which is described in 3.4, "Obtaining all updates," on page 79.

Procedure

1. Log in to the CMM Web interface
2. Select **Mgt.Module Management** > **Firmware**.
3. Choose the CMM to be updated from the table and click **Update**.
4. On the Select File Source page, choose to the source for the file. The update can be done from either a local file that you upload from your workstation to the CMM or a remote file that is given as a URL that your CMM can download



5. Choose the correct instruction based on what you selected for the file source.

- If you chose Local as the source, click **Browse**, navigate to the where you saved the firmware, and select **cmefs.uxp**. Click **Next**.
- If you chose Remote as the source, type the URL to the cmefs.uxp file for the web server that will serve the file. Click **Next**.

6. On the Choose Post Update Behavior page, select whether you want to automatically restart the Chassis Management Module after the update is complete. Click **Next**.
7. After the firmware has been updated to the CMM click **Finish**.

What to do next

Make sure that you restart the CMM to apply the firmware updates.

4.2 Updating Power Systems compute nodes

Complete the following steps to update firmware for power systems compute nodes when an IBM FSM is not present.

Procedure

1. Download the update based on the instructions listed in 3.4.4, "Downloading Power System compute node updates," on page 87.

   Note: Make sure that you download all files in the firmware update, including .rpm .xml, dd.xml, and pd.sdd files as well as the readme.txt file.
2. Use FTP to copy the update to a directory on the Power Systems compute node (such as `/tmp/fwrpms`).
3. Log on to the AIX or Linux system as root, or log on to the Virtual I/O Server (VIOS) as padmin.
4. If you are logging on to VIOS, run the following command to obtain root access:

   ```
   run oem_setup_env
   ```
5. Unpack the .rpm file.

   For example, if you are installing the FW773 service pack 01AF773_051_033:

   ```
   rpm -Uvh -ignoreos 01AF773_051_033.rpm
   ```

   The output from the command should be similar to:

   ```
   Preparing...                ########################################### [100%]
      1:01AF773_051_033        ########################################### [100%]
   ```

   The resulting .img file is now in the `/tmp/fwupdate` subdirectory.
6. Install the firmware update with one of the following methods:
   - Install the firmware with the AIX **update_flash** command:

     ```
     cd /tmp/fwupdate
     /usr/lpp/diagnostics/bin/update_flash -f 01AFxxx_yyy_zzz.img
     ```
   - Install the firmware with the Linux **update_flash** command:

     ```
     cd /tmp/fwupdate
     /usr/sbin/update_flash -f 01AFxxx_yyy_zzz.img
     ```
   - Return to VIOS and install the firmware with the **ldfware** command on Virtual I/O Server:

     ```
     #exit
     cd /tmp/fwupdate
     ldfware -file 01AFxxx_yyy_zzz.img
     ```

   Where 01AF*xxx_yyy_zzz*.img is the name of the firmware image.

   Note: You can also use the firmware update function of AIX diagnostics or the firmware update function of the stand-alone diagnostics boot image. More information about AIX diagnostics is available at the following location:

http://pic.dhe.ibm.com/infocenter/powersys/v3r1m5/index.jsp?topic=/p7ha5/fix_aix_diags.htm

7. Restart the compute node to apply the firmware update.
8. Verify that the update was successful.
   - In AIX or Linux, run the following command to verify if the firmware update was successful:
     `lsmcode -A`
   - In VIOS, run the following command to verify if the firmware update was successful:
     `lsfware -all`

What to do next

After testing the updated server, you might decide to install the firmware update permanently. For information about installing the firmware update permanently, see 2.6.2.1, "Activating the Power FSP update on the Permanent boot side," on page 39.

In addition if you need to update firmware for the IBM Flex System EN4054 4-port 10Gb Ethernet adapter, see 2.6.2.3, "Updating the IBM Flex System EN4054 4-port 10Gb Ethernet Adapter," on page 41.

Note: Before updating firmware on Ethernet adapters, make sure that all ports are inactive.

4.3 Updating X-Architecture compute nodes

Typically, use either Bootable Media Creator (BoMC) or UpdateXpress System Pack Installers (UXSPIs) to apply firmware updates to X-Architecture compute nodes.

- IBM ToolsCenter Bootable Media Creator

  You can use IBM ToolsCenter Bootable Media Creator to create bootable media that is suitable for applying firmware updates and running preboot diagnostics. Using IBM ToolsCenter Bootable Media Creator, you can create a single bootable image on supported media (such as CD, DVD, ISO image, USB flash drive, or set of PXE files) that bundles multiple IBM Flex System tools and updates from UpdateXpress System Packs, which contain Windows and Linux firmware updates. Typically, use IBM ToolsCenter Bootable Media Creator for the initial setup of a compute node or to update firmware for a compute node on which no operating system is installed.

  Note: UpdateXpress System Packs can be installed using the IBM ToolsCenter Bootable Media Creator but this will update the firmware only.

  More information about Bootable Media Creator is available at the following website:

  http://www.ibm.com/support/entry/portal/docdisplay?lndocid=TOOL-BOMC

  Detailed instructions for using the Bootable Media Creator are available at the following website:

  http://publib.boulder.ibm.com/infocenter/toolsctr/v1r0/topic/bomc/bomc_main.html

- UpdateXpress System Pack Installers (UXSPIs) and UpdateXpress System Packs (UXSPs)

  Note: When you update x440 M5 (MT 7167, 2590) and x240 M5 (MT 9532, 2588), you must use UXSPI version 10.0 or later.

  Note: Lenovo UXSPi is applicable to Lenovo systems and IBM UXSPi is applicable to IBM systems. Ensure to use the correct UXSPI on the respective systems.

  UpdateXpress System Packs (UXSP) contain an integration-tested bundle of online, updatable firmware and device drivers for your compute node.

  Typically, use UpdateXpress System Packs to update firmware and devices drivers for a compute node that has previously been provisioned. More information about UpdateXpress System Packs is available at the following website:

  http://www.ibm.com/support/entry/portal/docdisplay?lndocid=SERV-XPRESS

UpdateXpress System Packs can be installed as part of the IBM ToolsCenter Bootable Media Creator to update the firmware, but they can also be installed using the UpdateXpress System Pack Installer (UXSPI) to update firmware and device drivers inband (while the operating system is running).

More information about UXSPIs is available at the following website:

http://www.ibm.com/support/entry/portal/docdisplay?lndocid=serv-xpress#uxspinstall

Detailed instructions for using the UXSP Installer (USXPI) are available at the following website:

http://publib.boulder.ibm.com/infocenter/toolsctr/v1r0/topic/uxspi/uspi_main.html

In addition, specific firmware updates can be applied directly through the IMM interface for the compute node. Complete the following steps to apply firmware updates:

1. Download the specific update from the IBM Fix Central site

   http://www.ibm.com/support/fixcentral/

   For example, to find specific updates for the Flex System x222 Compute Node, you would fill in the form on the site like this:

   - **Product Group:** PureSystems
   - **Select from PureSystems:** PureFlex System and Flex System
   - **Select from PureFlex System and Flex System:** Compute Node
   - **Select from Compute Node:** x222 Compute Node
   - **Select from x222 Compute Node:** 7916
   - **Operating System:** All

   Then click **Continue**.
2. Download the pDSA (under Diagnostics), IMM, and UEFI updates.

3. Log in to the IMM interface to apply the updates.

Note: After applying IMM, pDSA, and UEFI updates, you will need to reset the IMM. To reset the IMM, establish an SSH session to the IMM for the compute node and use the **resetsp** command.

For information about updating the compute node firmware through the IMM, see the "Integrated Management Module II User's Guide," which is available at this location:

http://www.ibm.com/support/entry/portal/docdisplay?lndocid=MIGR-5086346

4.3.1 Updating Linux firmware and drivers

If you are using UpdateExpress System Packs to update firmware and drivers for compute nodes that have Linux installed, make sure that you meet the prerequisites.

Firmware prerequisites

When updating firmware, the following prerequisites are required:

- If you are running a 64-bit version of Linux, make sure that the 32-bit compatibility libraries are installed (i.e. 32 bit libstdc++.so). For example, on RHEL 6, this is libstdc++-4.4.4.13.el6.i686.rpm.
- Updates require the Ncurses library (i.e. libncurses.so). For example, on RHEL 6, this is ncurses-libs-5.7-3.20090208.el6.i686.rpm.
- Make sure that the following commands are installed on each compute node that will receive the update (depending on the version of Linux that is installed):
  - zip
  - gunzip
  - rug (for SUSE Linux Enterprise Server 10 with the service pack)
  - zypper (for SUSE Linux Enterprise Server 11)
  - yum (for Red Hat Enterprise Linux versions 5.x and 6.x)

Driver prerequisites

Additionally, the following packages are required for installing Linux drivers from IBM update packages:

- /bin/sh
- /usr/bin/perl
- bash
- perl
- perl(Cwd)
- perl(Getopt::Long)
- perl(Getopt::Std)
- perl(strict)
- rpm-build
- rpm-libs
- rpmlib(CompressedFileNames) - must be version 3.0.4-1 or earlier
- rpmlib(PayloadFilesHavePrefix) - must be version 4.0-1 or earlier

4.3.2 VMWare ESXi update considerations

Read through the following considerations if you are running VMware ESXi on X-Architecture compute nodes, and you are updating the firmware using UpdateXpress System Packs (UXSPs).

- If you are updating an ESX or ESXi system that is configured for virtual switch (vswitch) and there is no physical network adapter associated with the virtual switch, inventory collection from the IBM FSM will fail. See 7.24, "Inventory collection on compute nodes running ESX or ESXi consistently fails, which means that firmware update will not be deployed," on page 150 to resolve this issue.
- When managing compute nodes that are running the standard VMware ESXi image, the IBM FSM is limited to updating UEFI, preboot DSA, and IMM firmware.

  If the compute nodes are running the VMware ESXi 5/vSphere IBM-customized image, the IBM FSM can also update firmware for network (I/O) adapters and LSI RAID controllers. The IBM customized image can be downloaded from the following website:

  http://www.ibm.com/systems/x/os/vmware/index.html

  Note: Hard drive updates from the IBM FSM are not supported.

  Note: BNX1 and BNX2 firmware updates are not supported on ESXi Customized Image with Patch 1.2

  You can also choose to install the CIM providers developed by IBM on the VMware ESXi image. For more information, see the following website:

  https://www.ibm.com/support/entry/myportal/docdisplay?lndocid=MIGR-5092718
- When updating a compute node running VMware ESXi, the host must be fully initialized before the update process starts. Make sure you wait for the full compute node initialization to complete, which takes approximately 20 minutes.

  If the host is not fully initialized, you might see an error stating that the system failed to restart, and that it must be restarted manually (even if you choose to have the compute node restarted automatically after the update). If you see this error, restart the compute node manually. If there are no other errors listed, the firmware update was successful.
- You should use the latest CIM providers and drivers available from each vendor. These patches are usually available either on the vendor web site or directly on VMware's web site as offline-bundles that can be imported directly into VMware Update Manager.

  For IBM information on VMware operating systems, see the following website:

  http://www.ibm.com/systems/info/x86servers/serverproven/compat/us/nos/vmwarefx.html
- At a minimum, you must apply VMware vSphere ESXi 5.x with IBM Customization Patch 1.2 or later for each compute node running the IBM customized image.

  Important considerations

  – Before updating the firmware for a compute node that is running ESXi, make sure that you enable maintenance mode. For information about enabling maintenance mode, see the documentation that is provided with ESXi.

  – If you are running VMware vSphere ESXi 5.5.x (update 1) or earlier, you must apply both the Lenovo and the Independent Hardware Vendor (IHV) customization patches (Patch 1.2) on every compute node. If you are running VMware vSphere ESXi 5.5.x (update 2), you need not apply Patch 1.2.In addition to the IBM Customization Patch 1.2, make sure that you install one of the following updates to the VMware vSphere ESXi operating system:

    - If you are running VMware vSphere ESXi 5.0, make sure that, at a minimum, you install update 5.0u2 (update 2)
    - If you are running VMware vSphere ESXi 5.1, make sure that, at a minimum, you install update 5.1u1 (update 1)

    When you install an update to the Integrated Management Module (IMM) on an X-Architecture compute node, the IMM is reset. In this case, if you have not installed (at a minimum) update 5.0u2 or 5.1u1, a VMware vSphere ESXi system failure (host purple diagnostic screen) might occur.

  VMware vSphere ESXi 5.x with IBM Customization Patch 1.2 can be found at this location:

Note: There is an IBM Customization patch 1.2 for each VMWare version 5.0.x, 5.1.x and 5.5.x.

http://www.ibm.com/support/fixcentral/systemx/quickorder?product=ibm/systemx/8737
&&platform=All&function=fixId&fixids=ibm_sw_hyper_patchbundlv7_vmwaresx5_32-64
&includeRequisites=0&includeSupersedes=0&downloadMethod=ddp&source=fc

Note: The patch contains many of the ESXi vendor drivers that you will need. However, to ensure that you obtain all drivers that might be needed to support the latest adapters installed in the compute node, go to:

http://www.ibm.com/support/fixcentral/

For more information about obtaining the IBM Customization Patch 1.2, see the following location:

http://www.ibm.com/support/entry/portal/docdisplay?lndocid=MIGR-5092679

Make sure that you review the information provided in the readme for the patch. It contains instructions for installing the patch on a compute node.

- To validate that you are running the IBM-customized version, check that the file `/etc/cim/ibm/imm_fw_schema` exists on the image. This file should contain lines indicating that the SCHEMA_STATE is "check" and showing a version number for the FW_VERSION field. To review the list of custom providers, use the command "**`esxcli software vib list`**" on your ESXi server.

  Tip: You can compare this list with the list provided in the readme for Patch 1.2.
- If storage paths are lost for any reason in a configuration with VMware, CN4022, and storage devices, the paths might recover. Paths also might recover and then fail again in about 5 to 45 minutes.

  You can recognize lost paths with the following command:

  ```
  esxcfg-mpath -L | grep dead
  ```

  The paths can be recovered by issuing the following command:

  ```
  esxcli storage filesystem rescan -a
  ```

  To reduce potential issues, update one SVC controller, making sure the paths have a chance to settle and recover with the rescan command. Then update the second SVC controller.

4.3.3 Updating firmware using UXSPs

If you are updating firmware and device drivers for an X-Architecture compute node that already has an operating system loaded on the compute node, use UpdateXpress System Packs (UXSPs) and the UpdateXpress System Pack Installer (UXSPI)

About this task

The following procedure explains how to use UXSP and UXSPI to update a compute node that is running Windows 2008. For more information about using UXSP and UXSPI, see the following Website:

http://publib.boulder.ibm.com/infocenter/toolsctr/v1r0/topic/uxspi/uspi_main.html

Procedure

1. Download the UXSP and the UXSPI (UXSP installer) that maps to the operating system being run on the Flex System x240 X-Architecture compute node to be updated. For example, if you are updating a compute node that has Windows 2008 installed, you would download the following UXSP and UXSPI.
   - Flex System x240 Compute Node UpdateXpress System Pack for Windows 2008 x64, Windows 2012 x64 (ibm_utl_uxsp_b2sp09p-1.40_windows_32-64)
   - UpdateXpress System Pack Installer (ibm_utl_uxspi_9.30_winsrvr_32-64)

   Tip: For information about obtaining these packages, see 3.4.3, "Downloading X-Architecture compute node updates," on page 82

Note: Lenovo UXSPI and ToolsCenter tools are needed to update the Lenovo components. Lenovo ToolsCenter can be downloaded from the following websites:

- http://www.ibm.com/support/entry/portal/docdisplay?lndocid=LNVO-CENTER
- http://www.ibm.com/support/entry/portal/docdisplay?lndocid=LNVO-XPRESS
- http://www.ibm.com/support/entry/myportal/docdisplay?lndocid=LNVO-BOMC

2. Use a tool like Remote Desktop to log in with Administrator privileges to copy the updates and run UXSPI.
   a. Create a directory on the compute node where the update will be stored (such as `c:\tmp\uxsp`).
   b. Use SCP to copy the UXSP and UXSPI packages to the directory that you just created.
   c. Using Remote Desktop, navigate to the directory where the files were copied and run the installation program.

      ```
      ibm_utl_uxspi_9.30_winsrvr_32-64.exe update -u
      ```

      This command will update the firmware and devices drivers in unattended mode. Information about the parameters that you can use with this command are available at the following Website:

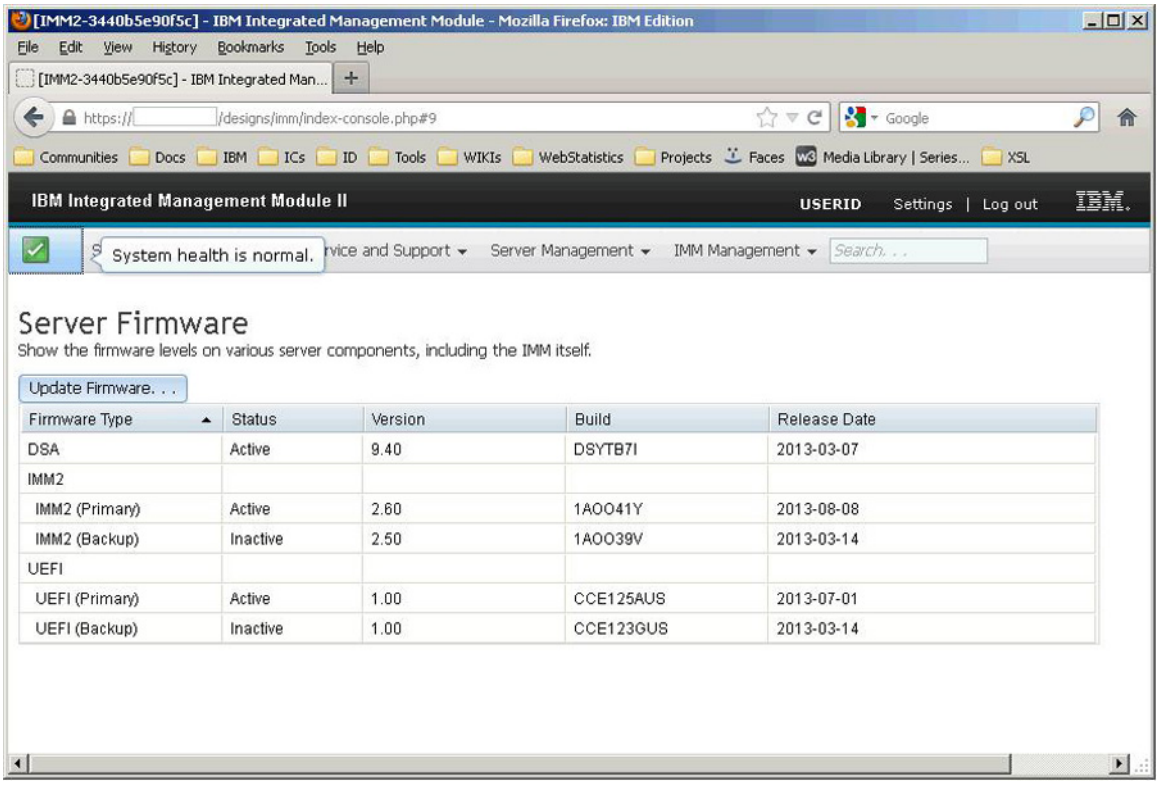
      http://publib.boulder.ibm.com/infocenter/toolsctr/v1r0/topic/uxspi/uspi_r_using_compare_update.html#uspi_r_using_compare_update

      Tip: Run `ibm_utl_uxspi_9.30_winsrvr_32-64.exe` with no parameters to start the graphical user interface.
3. Restart the X-Architecture compute node for the updates to take effect.

What to do next

Validate that the IMM, UEFI, and pDSA updates were installed successfully.

1. Log in to the IMM interface for the X-Architecture compute node.
2. Click **Server Management** > **Server Firmware** to valudate that the current versions are installed.



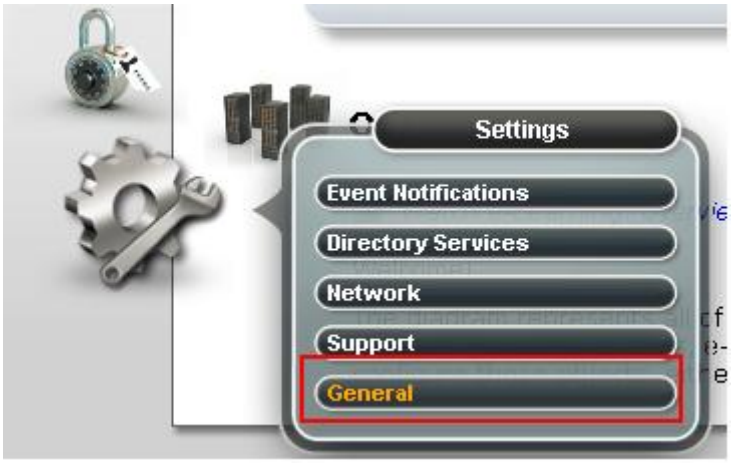
4.4 Updating Flex System V7000 Storage Nodes

Procedure

Complete the following steps to update the firmware on the Flex System V7000 Storage Node.

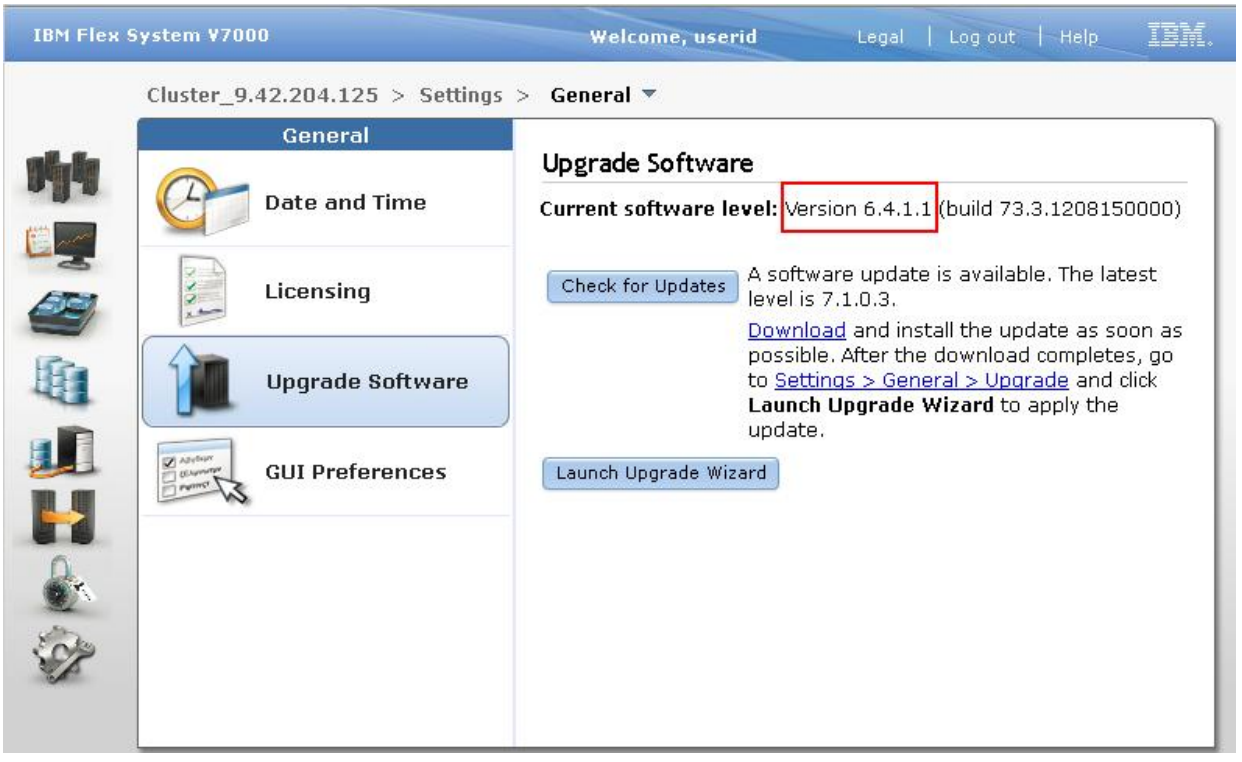
1. Log in to the CMM Web interface.
2. From the Chassis Graphical View, right–click the storage enclosure and then click **Launch Storage Node Console**.
3. From the Launch Node Console pop-up, make sure that you select **Cluster management interface** and click **Launch**.
4. Log in to the Flex System V7000 Web interface with a user account that has sufficient permissions to upgrade the software.

5. From the navigation menu, click **Settings** > **General**.



6. From the General page, click **Upgrade Software**.

   Note: The installed version is listed at the top of the page.



7. Click **Check for Updates** to see the latest version that is available.

   Note: If the Flex System V7000 storage node is not connected to the Internet, use the following procedure to update the firmware:

   http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.4939.doc/svc_upgradingintro.html

8. Click the **Download** link to download the update to your workstation.

   Note: Make sure that you download the StorageDisk-4939-SwUpgradeTestUtility package as well as the firmware update package.

9. Click **Launch Upgrade Wizard** to upgrade the Flex System V7000 storage node.

4.5 Updating I/O modules

To update I/O modules with an IBM FSM is not present, use the interface to the I/O module. You will typically need a TFTP server on which to load the updates for installation.

Typically, updating an I/O module software image consists of the following steps:

1. Obtain the software image for the I/O module. You can obtain the updates the IBM PureSystems Centre website, which is described 3.4, “Obtaining all updates,” on page 79.

   Note: The updates for the I/O modules are part of the Chassis updates.
2. Load the new software image and boot image onto an FTP or TFTP server on your network.
3. Specify the new software image as the one that will be loaded into switch memory the next time a switch reset occurs.
4. Reset the switch.

Important consideration:

Flex System FC3171 8 Gb SAN switches **must** be running CPLD version 0x22 or later. Switches with firmware levels of 9.1.0.26.00 and later will show the following error messages if the CPLD was not updated:

```
Installed CPLD version 0x20 older than available version 0x22. See 'help cpld install'
in the CLI for upgrade instructions.
```

Complete the following steps to update the CPLD, which will require a virtual switch restart.

1. Update the firmware level on the switch to 9.1.0.27.00 or later and restart the switch.
2. Log in to the CLI and run the following commands:

   ```
   admin start
   set advanced on
   cpld install
   ```
3. When CPLD install completes successfully, login to theCMM CLI and run these commands to perform a virtual reseat of the switch:

   ```
   env -T system:switch[x], where x is switch slot
   service -vr
   ```
4. Verify the CPLD version after the virtual reseat. Run the following commands from the switch CLI:

   ```
   set advanced on
    show setup mfg
   ```

   Look for the line CPLD Revision, which should end in 0x22.

Instructions for the specific I/O module that you are updating are available in the readme files that are provided for each update at that IBM PureSystems Centre website.

In addition, you can find product documentation for I/O modules available for IBM Flex and IBM PureFlex systems at the following website:

http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.lenovo.acc.networkdevices.doc/network_iomodule.html

Chapter 5. Updating the IBM Storwize V7000

To upgrade the IBM Storwize V7000, use the IBM Storwize V7000 interface.

Note: The IBM FSM does not support updating external storage, such as the IBM Storwize V7000 through the IBM FSM user interface.

More information about upgrading the IBM Storwize V7000 is available through the product documentation. For example, you can learn more about upgrading the system for the IBM Storwize V7000, Version 7.2, at the following website:

http://pic.dhe.ibm.com/infocenter/storwize/ic/topic/com.ibm.storwize.v7000.720.doc/svc_upgradecli_25eisl.html

Documentation related to other versions are available at that location as well.

Chapter 6. Updating Top-of-Rack (TOR) switches

To update the firmware for a top-of-rack (TOR) switch, you must download the update and apply the update the switch using the switch user interface (either using the Web Interface or using the command-line interface).

Note: The IBM FSM does not support updating the TOR updates through the IBM FSM user interface.

Typically, updating a top-of-rack switch software image consists of the following steps:

1. Obtain the software image for the top-of-rack switch. You can obtain the updates the IBM PureSystems Centre website, which is described 3.4, “Obtaining all updates,” on page 79.

   Note: After downloading the appropriate top-of-rack switch update, use the Release Notes provided with the update to install it on the switch.
2. Load the new software image and boot image onto an FTP or TFTP server on your network.
3. Specify the new software image as the one that will be loaded into switch memory the next time a switch reset occurs.
4. Reset the switch.

Use the following links to find product documentation related to the top-of-rack switches:

- RackSwitch G8264:
  http://www-01.ibm.com/support/docview.wss?uid=isg3T7000297
- RackSwitch G8052:
  http://www-01.ibm.com/support/docview.wss?uid=isg3T7000306

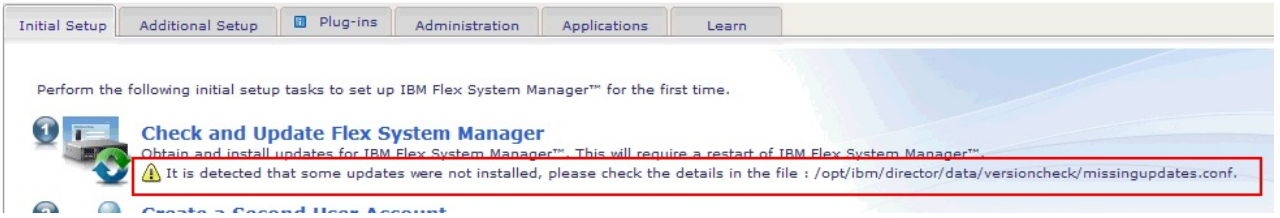
Chapter 7. Troubleshooting update issues

Use this section to resolve issues that might arise during the process of updating firmware.

Note: When an event received from the Chassis Management Module (CMM) is deleted from the IBM Flex System Manager management node, it remains on the CMM. The next time the IBM Flex System Manager management node synchronizes with the CMM, this event will appear in the Active Status view again. To permanently remove an event from the Event Log view, either ignore the event or delete it directly from the CMM.

7.1 IBM FSM software update causes warning on Initial Setup tab

After you havey applied an update to the IBM FSM software, you might see a warning on the Initial Setup tab from the Home page.



Attempt to update the IBM FSM software again from the IBM FSM command-line interface (CLI).

1. Log in to the IBM FSM CLI with a user account that has sufficient privileges to perform updates.
2. Attempt to update the IBM FSM software using the following command:
   ```
   smcli installneeded -v -F -I
   ```
3. If the problem persists, check the file that was generated during the update process to determine which updates were not applied. The generated file is opt/ibm/director/data/versioncheck/missingupdates.conf.
4. Attempt to update the IBM FSM software again using the following command:
   ```
   smcli installupdforce -f /opt/ibm/director/data/versioncheck/missingupdates.conf
   ```

7.2 Import of update fails due to SHA-1 mismatch error

Review this section to resolve the failure of the update import due to an SHA-1 mismatch error.

When attempting to import an update after copying it to the IBM FSM, you might see the following error:

```
ATKUPD285E The import updates task has completed with errors. Read the following
details and try again: ATKUPD260E The SHA-1 digest value
"aeb29c1e4d6ac6e7db2c2b2327cf2b81461442a1" from the SDD for file
"Flex_FC1764_2P8GbFC_050700_Readme.readme.txt" does not match the computed
SHA-1 value "da39a3ee5e6b4b0d3255bfef95601890afd80709". Ensure that the file
is completely downloaded and then retry the operation.
```

This error can result if the update was not copied in binary format to the IBM FSM. If you are using winscp, you must set transfer mode to binary, so that text files are not modified during transfer.

For instructions on copying files to the IBM FSM, see the following website:

http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/com.ibm.director.updates.helps.doc/fqm0_t_um_updates_director_manual_download.html

7.3 Import of an update fails due to missing files

Review this section to resolve the failure of the update import due to missing files.

When specifying to import updates from the file system through the IBM FSM interface, you should specify a directory where the updates are located, not a filename. If you do specify a filename, you might see an error similar to the following:

```
ATKUPD285E The import updates task has completed with errors. Read the following
details and try again: ATKUPD284E No updates were imported from
"/opt/ibm/director/data/updateslib/TEMP07295022882298868". Ensure the target
directory contains update descriptor files (.sdd), or files that can be generated
into .sdd files. Also, check that the updates do not already exist in the update
library.
```

If you see this error, attempt to import updates from the file system again but make sure that you specify a directory and not a filename.

7.4 Update process fails because files are missing

Review this section to resolve the failure of the update process because files are missing.

If you attempt to perform the updates from an IBM FSM and you receive error messages similar to the following:

```
Attempting to connect to Fix Service Provider
to obtain update files. Connection was not successful.
You may need to manually acquire and import update files
if you are not Internet-connected. If you have an available
proxy, use the updates settings page to configure the
connection settings and try again.
```

To resolve this issue, make sure that you acquire **all** files associated with an update (including readme files) and import all of those files.

For information about acquiring updates, see 3.4, "Obtaining all updates," on page 79.

For more information about importing files, see 3.6, "Copying and importing updates for chassis components to the IBM FSM," on page 92.

7.5 Update process fails because the updates library is full

Review this section to resolve the failure of the update process because the updates library is full.

If you attempt to perform the updates from an IBM FSM and you receive the following error messages:

```
ATKUPD783E An error occurred while updating
"com.ibm.dpsm.feature_1.0.0.201302061138" on system
"IBM 795501M 102073B 31F0D2D6-068B-4D1B-AB64-F6BFCC614536". Restart the
Common Agent on the managed system, verify connectivity to the system,
and try again.
```

```
Error: ATKUPD268E Updates cannot be installed on the system
"FSM-1-RTPEBC.raleigh.ibm.com". The install requires an estimated 4449 MB of free
space, and the disk volume containing the directory "/opt/ibm/director/lwi" has
4236 MB of free space remaining. Remove unused files from the disk volume or
increase the size of the volume and try again. Run the "cleanupd" command to
remove any update files that are no longer needed. For more information about
the "cleanupd" command, enter "smcli cleanupd --help" on the command line.
```

Complete the following steps to resolve the issue:

1. Log in to the IBM FSM command-line interface (CLI) using a remote-access utility such as Secure Shell (SSH).
2. From the command-line interface, run the following command to remove all updates related to the IBM FSM management node:

   ```
   smcli cleanupd -mFv -P "Platform='Director' OR Platform='DirectorAppliance'"
   ```
3. Attempt to perform the updates again.
4. If the problem persists, you can use the smcli cleanupd command to remove older individual updates that have already been installed.

   More information about the smcli cleanupd command is available at the following website:

   http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/com.ibm.director.cli.helps.doc/fqm0_r_cli_cleanupd.html

More information about the IBM FSM CLI is available at the following website:

http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/using_the_cli.html

7.6 IBM FSM software update continues to be applied

After you have successfully applied an update to the IBM FSM software, the update preparation (fsm_appliance_update_preparation_1.3.2) continues to show as needing to be applied.

When you update the IBM FSM successfully, the update preparation will continue to display as needing to be applied.

Note: This will not affect the function of the IBM FSM; it will continue to operate normally

If you rerun the IBM FSM update process using the command:

```
smcli installneeded -v -F -I
```

The preparation update will run again.

If you have set up compliance policies, the preparation update will always show as needed.

7.7 IBM FSM software update fails

Review this section to resolve the failure of the IBM FSM update process.

The IBM FSM update might fail and, if it does, you can see detailed error log messages using the following command:

```
cat /var/log/fsmprep.log
```

Situations that might cause the IBM FSM software update to fail include:

- You attempt to update the IBM FSM from a version that is earlier than that minumum supported version.
- Updates were copied to the /tmp directory

Update attempted from an Flex version earlier than the minimum supported version

Depending on the version of Flex System firmware that is installed, you might see the following error message:

```
ATKUPD767W The installation of update "fsm_appliance_update_preparation_@version"
was not successful for system
"IBM 8731AC1 23RBT07 623FC84F-5C0D-4E02-B402-56C8BE83DFDC".

DNZDVM122E An error occurred while installing "fsm_appliance_update_preparation_@version"
on system "IBM 8731AC1 23RBT07 623FC84F-5C0D-4E02-B402-56C8BE83DFDC" :
Failure to install rpm
fsm_appliance_update_preparation-@version-0.x86_64.rpm,.
Check the rpm file. Then, retry update operation.
```

If you view /var/log/fsmprep.log, you will see an error similar to the following:

```
"DNZFM4500: Installation of $ROOTAPPLFIXID requires a minimum Flex System Manager
release of $MINVERSION.  Installation of $ROOTAPPLFIXID will be skipped.
Install a minimum release of $MINVERSION before installing $ROOTAPPLFIXID."
```

Where:

- $MINVERSION is the minimum version of the IBM FSM to which you need to install.
- $ROOTAPPLFIXID = the IBM FSM target you are trying to install.

For more information about the minimum releases required for upgrading firmware, see 1.1, “Upgrading from an earlier version of Flex System firmware,” on page 3

Updates copied to the /tmp directory

For example, the IBM FSM update might fail if the updates were copied to the /tmp directory and you might see the following error messages:

```
ATKUPD767W The installation of update "fsm_appliance_update_preparation_1.3.2"
was not successful for system
"IBM 8731AC1 23RBT07 623FC84F-5C0D-4E02-B402-56C8BE83DFDC".
```

```
DNZDVM122E An error occurred while installing
"fsm_appliance_update_preparation_1.3.2" on system
"IBM 8731AC1 23RBT07 623FC84F-5C0D-4E02-B402-56C8BE83DFDC".
 Error: Failure to install rpm fsm_appliance_update_preparation-1.3.1-0.x86_64.rpm,.
Check the rpm file. Then, retry update operation.
```

Do not use /tmp for copying and importing updates to the IBM FSM.

If you copied updates to that directory, you can delete them using the following command:

```
rm –rf /tmp/*
```

This command deletes all files in the /tmp directory. However, you only have permissions to delete files that were created by your user ID, so you might see error messages related to files that cannot be deleted because you do not have permissions to do so. Therefore, you might need to log in with multiple user accounts to remove all files from the /tmp directory.

Restart the IBM FSM to clear the /tmp directory automatically.

7.8 An update was imported but does not show up as available to install

Review this section to resolve the issue of an imported update not showing up as being available to install through the IBM FSM.

If the firmware update for a component, such as a Power Systems compute node, was imported, but it does not show up in the list of available updates, complete the following steps:

1. From the Chassis Manager, make sure that the component is in an OK state and that there are no authentication issues with the IBM FSM.
2. Collect inventory on the component.
3. Attempt to perform the update again.

7.9 Power Systems compute node remains at a status pending state after an update

Review this section to resolve the issue of a Power Systems compute node remaining at a status pending state in the IBM FSM after an update.

If you updated the firmware for the CMM before updating the FSP on the Power Systems compute node and the FSP firmware is earlier than the December, 2012 release (AF763_043), and the Power Systems compute node remains at status pending, perform the following recovery steps:

Note: This procedure could be destructive to a production environment! You will delete all LPARs while performing these steps.

1. Prepare the Power Systems compute node for recovery. From the FSM ASMI:
   a. Ensure that no HMC or management connections are present: **System Configuration** > **Hardware Management Consoles**.
   b. If any management connections are present, remove them by placing a check beside the connection and clicking **Remove Connection**.
   c. Delete partition information: **System Service Aids** > **Factory Configuration** > **Reset all settings**.
2. Perform the inband update:
   a. Enable Serial over LAN (SOL). Connect to the CMM using SSH and enter the following commands:
      1) `env –T cmm [x]`
         where *x* is either 1 or 2, depending on which CMM is the primary CMM
      2) `sol –status enable`
      3) `env`
      4) `env -T blade[x]`
         where *x* is 1 – 14, depending on the compute node being updated
      5) `sol –status enable`
   b. Perform the update. For more information about performing an in-band update, see the following website:
      http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.7895.doc/updating_firmware.html
   c. Disable Serial Over LAN (SOL). Connect to the CMM using SSH and enter the following commands:
      1) `env –T cmm [x]`
         where *x* is either 1 or 2, depending on which CMM is the primary CMM
      2) `sol –status disable`
      3) `env`
      4) `env -T blade[x]`
         where *x* is 1 – 14, depending on the compute node being updated
      5) `sol –status disable`
3. From the IBM FSM, manage the Power Systems compute node again:
   a. From the Home page, select the Plugins tab.
   b. From the Plugins tab, click **Discovery Manager** > **System Discovery**. Then, enter the IP address of the FSP on the Power Systems compute node.
4. If the system reconnects with No Access or Partial Access state, click on that message and select Request Access to enter the user ID and password.

7.10 Power Systems compute node firmware update contains IP address errors

Review this section to resolve the issue if IP address errors are listed in the log when Power Systems compute node firmware update is applied..

When you update the firmware for a Power Systems compute node, you might see any of the following errors in the log:

```
Platform firmware (0x82) reported error
The IP xxx is not a service processor
The alternate IP is not available
```

Complete the following steps to resolve these errors:

1. Select the Power System compute node from the Chassis Manager.
2. Click **Manage Power System Resources**.
3. Click **Virtual Servers**.
4. Select the virtual server and click **Actions** > **System Configuration** > **Manage Profiles**.
5. Select the profile and click **Edit** to edit the profile to change the IP address.
6. Save the profile when complete.
7. Shutdown the partition profile (click **Operations** > **Shutdown**).
8. Activate the partition profile you modified (click **Operations** > **Activate** and select the modified profile).

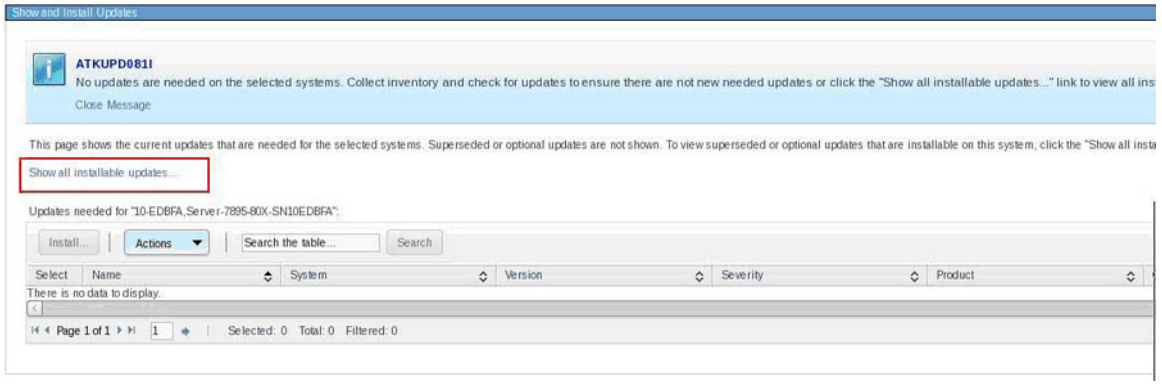
7.11 Power Systems firmware update does not display as needed

Review this section to resolve the issue where Power Systems updates do not display in the IBM FSM as being needed.

The Power System compute node firmware updates that show as needed are those that are newer than the currently installed level and in the same firmware release stream. For example, going from the AF743_100 update to the AF743_110 update will display as needing to be updated.

However, going from AF743 to AF763 or from AF763 to AF743 is considered to be updating across different streams and the IBM FSM Web interface will not indicate that these updates are needed.

On the Show and Install updates page, select **Show all installable updates** to apply updates across different update streams.



7.12 Power Systems network adapter or hard drive update still shows as needed after a firmware update

Review this section to resolve the issue where you updated the firmware for a Power Systems compute node, but the network adapter or hard drive update still shows as being needed.

For example, from the Chassis Manager, if you select the Power Systems compute node and then click **Actions** > **Release Management** > **Show and Install Updates**, the updates show as being needed after the update has been applied.

Complete the following steps to resolve the issue:

1. From the Chassis Manager, click **General Actions** > **Manage Power Systems Resources**.
2. From the Manage Power Systems Resources menu, click **Operating Systems**.
3. Select the required Power Systems operating systems.
4. Collect inventory. Click **Actions** > **Inventory** > **Collect Inventory**.

7.13 Microsoft Windows updates do not show as needed after an IBM FSM update

After the IBM FSM is updated, updates to managed compute nodes running Microsoft Windows might now show as needing to be updated (when they actually do need to be updated).

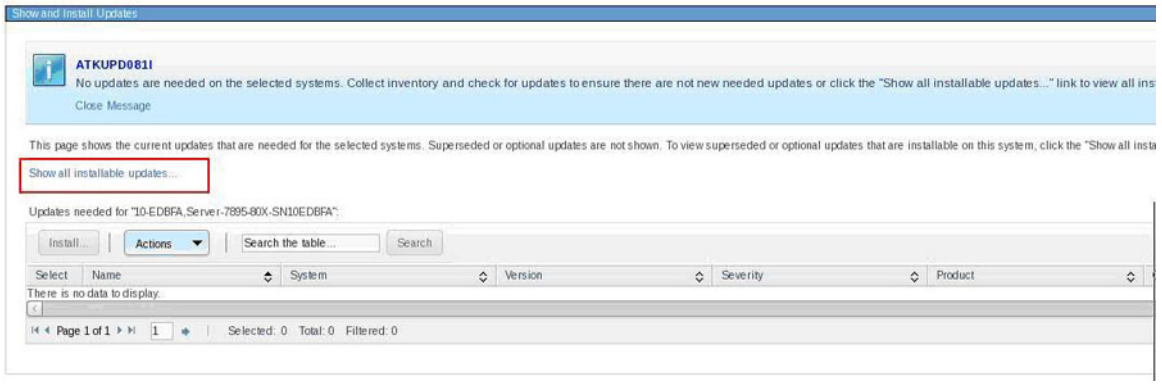
Updating the IBM FSM might cause the removal of the Distributed Component Object Model (DCOM) protocol access end point on managed compute nodes running Microsoft Windows, if a Platform Agent or Common Agent is installed on the compute node. The removal of the DCOM access point will result in firmware and updates never showing as needed on the compute node. To resolve this issue, rediscover the operating system on the managed compute node.

Note: You do not need to delete the compute node or the operating system from the IBM FSM inventory before you rediscover the operating system.

7.14 X-Architecture update does not display as needed

It is possible that some updates, such as driver updates will not display as being needed.

On the Show and Install updates page, select **Show all installable updates** to see a list of all available updates.



7.15 Error occurs when installing Linux driver updates

Review this section to resolve the issue when you experience errors when attempting to install Linux drivers on compute nodes.

The following error might occur in the task log when installing driver updates for compute nodes on which Linux is installed:

```
September 19, 2013 4:37:33 PM EDT-Level:50-MEID:8594--
MSG: DNZUPX104W The command
"/tmp/updatemanager/staging/systemxandbc/qlgc_dd_fc_qla2xxx-8.04.00.12.b_rhel6_32-64
/qlgc_dd_fc_qla2xxx-8.04.00.12.b_rhel6_32-64.tgz;
tar xzf qlgc_dd_fc_qla2xxx-8.04.00.12.b_rhel6_32-64.tgz;
export PATH=/usr/local/bin:$PATH; ./install.sh --update --force --add-initrd"
failed to install update "qlgc_dd_fc_qla2xxx-8.04.00.12.b_rhel6_32-64"
on system "gts-kvm2-p.rtp.raleigh.ibm.com".
The following log was collected from the installation command:


install.sh: ibm-driver-tools failed to install.
This installation requires the following:
/bin/sh
/bin/sh
/usr/bin/perl
bash
perl
perl(Cwd)
perl(Getopt::Long)
perl(Getopt::Std)
perl(strict)
rpm-build
rpm-libs
rpmlib(CompressedFileNames) <= 3.0.4-1
rpmlib(PayloadFilesHavePrefix) <= 4.0-1

sh: line 137: /tmp/updatemanager/staging/systemxandbc/qlgc_dd_fc_qla2xxx-8.04.00.12.b_rhel6_32-64
/qlgc_dd_fc_qla2xxx-8.04.00.12.b_rhel6_32-64.tgz: cannot execute binary file
```

Make sure that the listed packages have been installed for Linux and attempt to install the firmware update again.

7.16 X-Architecture compute node shows as locked on the IBM FSM when using Centralized Management

Review this section to resolve the issue where you have already enabled centralized user management on the IBM FSM, you have X-Architecture compute nodes at an IMM firmware level lower than December 2012 (v1.60 build 1AOO32P), and the compute node shows as being in a locked state in the IBM FSM Web interface.

You must first update the IMM firmware for the X-Architecture compute node to be at a later level. Then, continue with the update process.

Note: You will still need to follow the procedures for updating the X-Architecture compute nodes listed in yes.

Complete the following steps to update the IMM firmware for the X-Architecture compute node to a later level:

1. Disable centralized user management on the chassis where the affected X-Architecture compute nodes are installed.

   For more information about disabling centralized management, see the following website:

   http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/changing_a_chassis_user_management_mode.html
2. Download the UpdateXpress System Pack (UXSP) based on the operating system that is installed on the compute node. To obtain the UXSP, follow the procedures described in 3.4.3, "Downloading X-Architecture compute node updates," on page 82.

   Note: You will need only the IMM firmware update from the UXSP. When you download the UXSP, you will want to unzip the UXSP (if you downloaded it on a zipped format) into a directory, and search the directory for an update named ibm_fw_imm2*.UXZ. If there are multiple files with that name, make sure that you choose the latest version.
3. 3. Update the firmware for the X-Architecture compute node directly through the IMM Web interface for the compute node:
   a. Make sure that you have downloaded the UpdateXpress System Pack (UXSP). You do not need the UpdateXpress System Pack installer.
   b. Log in to the IMM Web Interface using a user ID that has administrator privileges.

      Note:
      - Centralized user management has been disabled, so you need to use a CMM user account.
      - From the Chassis Manager on the IBM FSM, select the X-Architecture compute node. In the Common Actions section, click **Launch Web Brower** to access the IMM Web interface.

   c. Click **Server Management** > **Server Firmware**.
   d. Click **Update Firmware**.
   e. Click **Select File** and navigate to the directory on your workstation where you downloaded the UXSP. Choose the latest file named ibm_fw_imm2*.UXZ. For example, the update might be named something similar to ibm_fw_im2_1aoo40a-1.88_anyos_noarch.uxz.
   f. After the update process is complete, you will need to restart the service processor for the X-Architecture compute node.
4. Re-enable Centralized Management from the FSM.

   You can use the command-line interface (CLI) to update a managed chassis from decentralized to centralized user management mode.

   Important consideration:

You cannot change a chassis from decentralized to centralized user management mode in the management software web interface; you must use the CLI. The web interface enables you to unmanage a chassis, and re-manage the chassis in centralized user management mode. However, unmanaging a chassis deletes all of the chassis settings, and is more complicated than using the manageChassis command and its options to change the chassis user management mode to centralized.

To update the chassis from decentralized to centralized user management mode in the management software CLI, run the following command:

```
manageChassis --Uc -c <userid:password@1.1.1.1>
              --Cu <centralized user ID>
              --Cp <centralized password>
              --Rp <RECOVERY_ID password>
```

where the variables in the command are:

- <*userid:password@1.1.1.1*> represents the administrator credentials and IP address for the target chassis.
- <*centralized user ID*> is an administrator user ID, with supervisor authority, on the management node. This account is use to request access to the CMM on behalf of the management node and managed nodes after the CMM is centrally managed.
- <*centralized password*> is the password for the centralized user ID.
- <*RECOVERY_ID password*> is the password for the CMM recovery account, which has the user ID RECOVERY_ID.

Next, proceed through the process for updating chassis components. Remember that you will still need to follow the procedures for updating the X-Architecture compute nodes:

- If you are updating X-Architecture compute nodes from an IBM FSM that is connected to the Internet, see 2.6.3, “Updating X-Architecture compute nodes,” on page 46.
- If you are updating X-Architecture compute nodes from an IBM FSM that is not connected to the Internet, see 3.8.3, “Updating X-Architecture compute nodes,” on page 104

7.17 X-Architecture compute node in "no access" state

Either before or after you install a firmware update, an X-Architecture compute node might be shown in a "no access" state.

Complete the following steps to resolve the access issue:

1. From the IBM FSM Chassis Manager, click the compute node that is showing no access.
2. From the list of Common Actions, click **Request Access**.
3. Specify the user ID and password. Then click **Request Access**.

7.18 Compute node update completes with errors

When you update a compute node, you might see that the job completed with errors.

You might see error messages similar to the following:

```
MSG: ATKUPD756W The updates installed successfully, but a restart is required
for one or more updates. The option to automatically restart resources after
installing updates was not selected, so manually restart the appropriate resources
on system "xpet23-143.xpet-rsl.rtp.stglabs.ibm.com" and then collect inventory.

MSG: ATKUPD705E The update installation request was not successful for system
"xpet23-143.xpet-rsl.rtp.stglabs.ibm.com". Search above for previous related
errors, fix each error, and then retry the operation.
```

These errors are displayed if you update the firmware but do not select the option **Automatically restart during installation as needed**. They are a reminder that you need to restart the compute node to apply the firmware updates.

7.19 X-Architecture compute node firmware updates fail

Review this section to resolve the issue where all X-Architecture compute node firmware updates fail.

If all X-Architecture compute node firmware updates fail, you might see an error that shows up as “Error 59” in the update task log. If so, make sure that the LAN-over-USB setting is enabled before applying firmware updates. The IBM FSM and X-Architecture compute nodes require that the LAN-over-USB setting is enabled before applying the firmware updates.

For information about enabling the LAN-over-USB interface, see 2.2, “Prerequisites,” on page 21.

7.20 X-Architecture compute node is in "No Access" state after an update

Review this section to resolve the issue when an X-Architecture compute node is in a "No Access" state after a firmware update.

Complete the following steps to resolve this issue:

1. From the Chassis Manager, right-click the X-Architecture compute node.
2. Click **Security** > **Request Access**.
3. Enter the User ID and password for the X-Architecture compute node.

7.21 ESXi updates fail due to SSL timeout errors

Firmware updates on X-Architecture compute nodes might fail if the system is under a heavy work load or the maximum number of Secure Socket Layer (SSL) connections has been reached.

To resolve this issue, attempt to perform the updates again or increase the number of SSL connections that are allowed for this compute node.

Complete the following steps to increase the number of SSL connections:

1. Establish an SSH session to ESXi.
2. Edit the file `/etc/sfcb/sfcb.cfg` in a plain text editor.
3. Change the httpsProcs property:
   ```
   httpsProcs: 8
   ```
4. Save the file.
5. Run the following command to restart the sfcbd-watchdog:
   ```
   /etc/init.d/sfcbd-watchdog restart
   ```

More information about this issue is available at the following website:

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1020806

7.22 X-Architecture compute node running ESXi requires a manual restart after an update

Review this section to resolve the issue that can occur when you attempt to update the firmware for a compute node running ESXi that has not been fully initialized.

If you are updating a compute node running ESXi and the host is not fully initialized, you might see the following error:

```
DNZUPX063W A failure occurred when trying to restart system "xxxx". Manually
restart the system, verify the connection and collect inventory.
```

The problem can occur when updating an X-Architecture compute node running VMware ESXi in the following cases:

- When updating a compute node running VMware ESXi, the host must be fully initialized before the update process starts. If you are restarting a compute node before applying an update, this process will take approximately 20 minutes to complete.
- Intermittently after the compute node is fully initialized (when the IMM is reset).

If you see this error, restart the compute node. Unless you see other errors, the firmware update was successful.

7.23 Operating systems not discovered on compute nodes running ESXi 5.5

Review this section to resolve the issue when operating systems on compute nodes running ESXi 5.5 are not discovered through the IBM FSM interface.

The IBM FSM discovery process can fail if the compute node is configured with VMware vSphere Hypervisor 5.5 with IBM Customization Installable, any model, any update and there are multiple VMK interfaces. To resolve the issue, see the following website:

http://www-947.ibm.com/support/entry/portal/docdisplay?brandind=5000008&indocid=MIGR-5095635

7.24 Inventory collection on compute nodes running ESX or ESXi consistently fails, which means that firmware update will not be deployed

Review this section to resolve the issue of firmware updates not being deployed on X-Architecture compute nodes running ESX or ESXi because of issues with inventory collection.

There are times with inventory collection on compute nodes running ESX or ESXi can fail, which means that firmware updates will not be deployed:

- The IBM FSM produces inventory task report errors, and no firmware updates succeed.

  The error messages are similar to the following:

  ```
  March 24, 2014 3:20:40 AM EDT-Level:200-MEID:0--MSG: Subtask activation status
  changed to "Complete with errors".

  March 24, 2014 3:20:40 AM EDT-Level:1-MEID:0--MSG: Job activation status
  changed to "Complete with errors".
  ```

  This can occur if the compute node has the following operating systems installed:

  – VMware vSphere Hypervisor 5.1 with IBM Customization Installable, update 2

  – VMware vSphere Hypervisor 5.5 with IBM Customization Installable, any model, any update

  To resolve this issue see the following website:

  http://www-947.ibm.com/support/entry/portal/docdisplay?brandind=5000008&indocid=MIGR-5095627

- IBM FSM inventory collection on ESX or ESXi systems will fail if the ESX or ESXi system is configured for an internal virtual switch (vswitch) but the virtual switch has no associated physical network adapter. This error can occur when you directly run an inventory collection on the node or when you run a task that indirectly triggers inventory collection.

  The error message is similar to the following:

  ```
  MSG: ATKSRV642E The "sdnm.virtual.discovery.VirtualExtendedDiscoveryModule"
  inventory extension failed for "flexComputeNode", which has a type of
  "Operating System".
  ```

  If you have this type of configuration and inventory collection fails, you will not be able to update the firmware on the compute node through the IBM FSM. Instead, you can update the firmware directly through the IMM interface for the compute node.

  For information about updating the compute node firmware through the IMM, see the *Integrated Management Module II User's Guide*, which is available at this location:

  http://www.ibm.com/support/entry/portal/docdisplay?lndocid=MIGR-5086346

  Make sure that you update firmware for UEFI, pDSA, IMM, and any network adapters that are installed.

  Tools are available to assist you in the update process through the IMM interface:

– IBM Fast Setup
  http://www.ibm.com/support/entry/portal/docdisplay?lndocid=TOOL-FASTSET
– IBM Bootable Media Creator
  http://www.ibm.com/support/entry/portal/docdisplay?lndocid=TOOL-BOMC

7.25 Performing inventory collection on a compute node produces an error when using the common agent

Review this section to resolve issues when performing an inventory collection on compute nodes on which the common agent is installed.

When performing an inventory collection on compute nodes on which the common agent is installed, you might see the following error messages:

```
April 16, 2013 8:41:39 AM CDT-Level:150-MEID:28294--MSG: ATKSRV635E The CAS
connection with "lbspureflex173" was not initialized.

April 16, 2013 8:41:39 AM CDT-Level:150-MEID:28294--MSG: ATKSRV642E The
"systems.discovery.extended.AgentExtendedDiscoveryModule" inventory extension
failed for "lbspureflex173", which has a type of "Operating System".
```

Complete the following steps to resolve the issue:

1. Remove the operating system from the IBM FSM Resource Explorer. More information about removing an operating system is available at this location:
   http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/unmanaging_removing_os_instances.html
2. Discover the operating system for the compute node from the IBM FSM again.
3. Specify the credentials to gain full access to the compute node from the IBM FSM.
4. Perform a full inventory of the operating system.

For more information about discovering systems and performing an inventory, see the following location:

http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/com.ibm.director.discovery.helps.doc/fqm0_t_discovering_and_inventorying_resources.html

7.26 Preboot DSA (pDSA) update fails to update on an X-Architecture compute node

Review this section if you attempt to update the firmware for an X-Architecture compute and the update fails to perform the update for pDSA.

If you attempt to update the firmware for an X-Architecture compute, the update might fail to perform the update for pDSA, and you might see errors similar to the following messages:

```
April 28, 2013 5:56:14 PM EDT-Level:50-MEID:20965--MSG: DNZUPX105E Failed to install
update "ibm_fw_dsa_dsytab5-9.29_anyos_32-64" on system
"xpet23-148.xpet-rsl.rtp.stglabs.ibm.com". The UXSPi return code is "59" and error
message is "?". For more information, refer to
http://publib.boulder.ibm.com/infocenter/toolsctr/v1r0/topic/uxspi/
uspi_r_returncodes.html. Resolve the issue and then retry the operation.

April 28, 2013 5:56:15 PM EDT-Level:75-MEID:20965--MSG: DNZUPX067I Return code "44"
for the installation of update "ibm_fw_dsa_dsytab5-9.29_anyos_32-64" on system
"xpet-c1s8".
```

If you see these errors, attempt to update the firmware again.

7.27 The ServeRAID M5115 PSoC3 update package cannot be installed from IBM FSM or UXSPI

Review this section if you are installing the ServeRAID M5115 PSoC3 update package to version 68 from version 63.

The ServeRAID M5115 PSoC3 update to version 68 must be done in a controlled manner.

1. Before performing this update, shutdown the system and wait ten minutes.
2. Perform a virtual reset using one of the following methods:
   - From the CMM Web User Interface:
     a. Log into the CMM web interface.
     b. Navigate to **Service and Support** > **Advanced**from the main menu.
     c. Select the **Service Reset** tab.
     d. Select the desired compute node by clicking on its radio button.
     e. Under the Reset pull down, click **Virtual Reseat**.
   - From the CMM CLI:
     a. Log into the CMM SSH interface.
     b. Enter the following command:

        ```
        'service -vr -T blade[x]'
        ```

        where *x* is the compute node bay number for the Flex compute node to be virtually reseated.
3. Once the system is powered back up, boot to the operating system and update the ServeRAID M5115 PSoC3 on this boot by using the extracted embedded update package:
   - Windows operating systems.

     Open update package and select the "Extract to Hard Drive" option and select path where the embedded package will be extracted to.
   - Linux operating systems.

     Run the following command:

     ```
     ibm_fw_psoc3_m5115-68_linux_32-64.bin -x <path>
     ```

     where <*path*> is the location the embedded package will be extracted to.

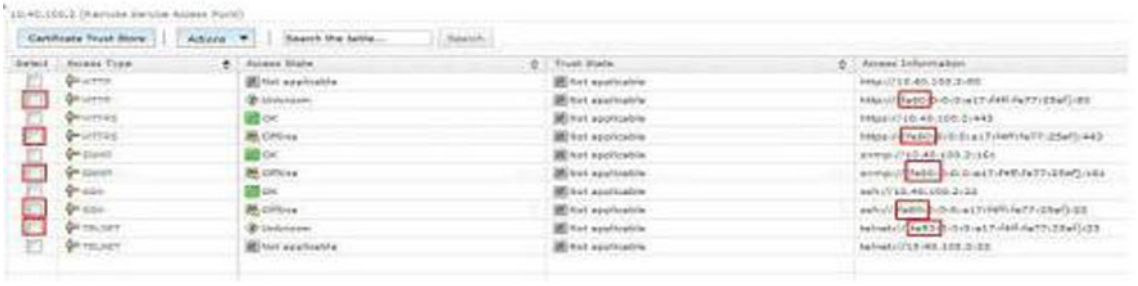
4. Run the embedded package to update the ServeRAID M5115 PSoC3 to version 68.

7.28 I/O Modules in partial access state after IBM FSM update

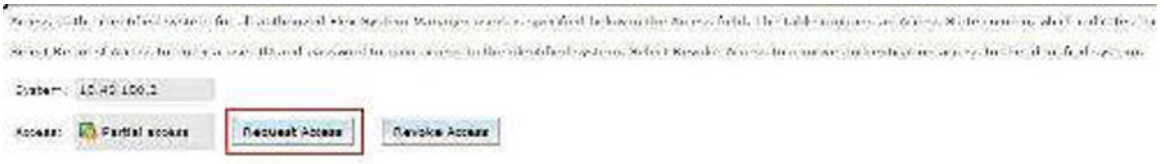
Review this section to resolve the issue that might occur when you update the chassis from IBM FSM version 1.1.1 or earlier, and I/O modules show partial access state after performing full inventory.

If this occurs, update all components in the chassis as described in this document. Then, set the I/O module to full access by deleting the unused IPv6 Link Local Addresses (LLA). Complete the following steps to remove the unused link local addresses and request access:

1. From the Chassis Manager, right-click on the I/O module.
2. Click **Security** > **Configure Access**.
3. Select the LLA access points. The will all have IPv6 addresses starting with "FF80:" and duplicate Access Types as shown in the following example:



4. Click **Actions** > **Remove** to delete selected access points.
5. Click **Request Access** and enter the log in credentials for the I/O module to request access.



7.29 IBM FSM fails to update IB6131 and EN6131 switches

Review this section to resolve the issue that might occur when you update the IB6131 and EN6131 switches with the Flex 1.3.2 firmware.

The 3.3.5064 switch firmware update package released for these switches and importing the update package to the IBM FSM will not result in an automatic detection from the IBM FSM to end users for starting a switch firmware update. Therefore, you should update the firmware for these switches using one of the following methods:

- The switch CLI or web interface.
- Tthe CMM CLI or web interface.

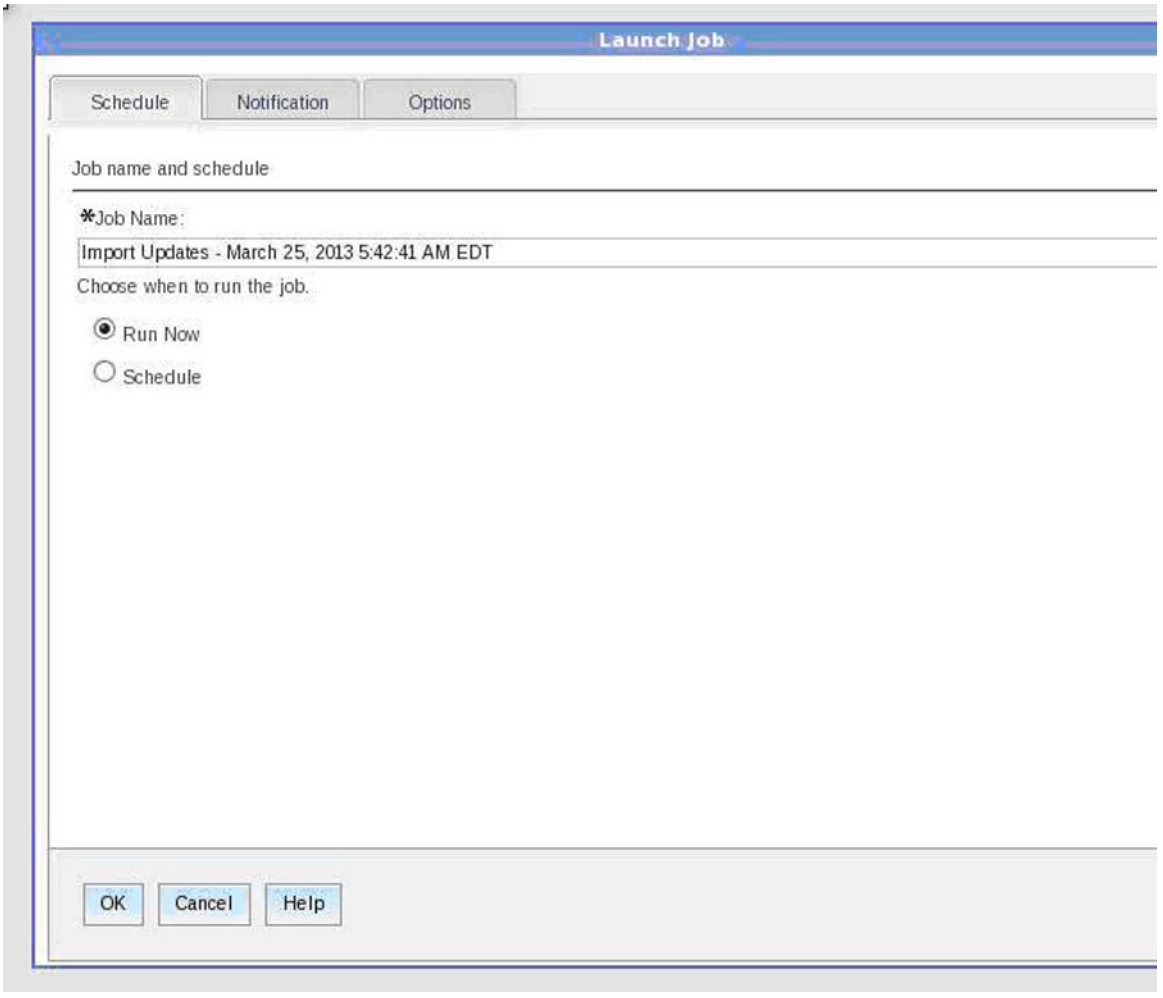
Appendix A. IBM FSM hints and tips

This section provides an overview of common functions in the IBM FSM Web interface.

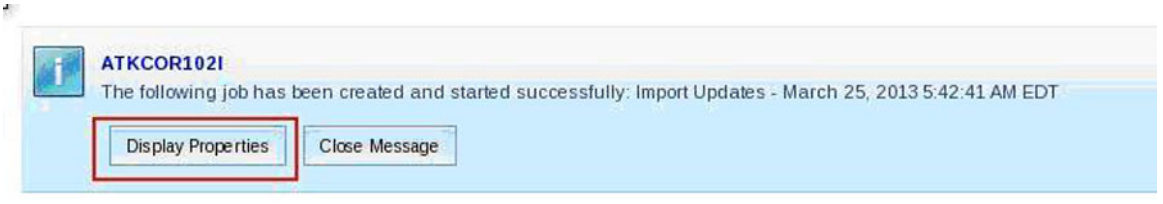
A.1 Starting a job task

Procedures such as acquiring updates and applying updates on the FSM user interface are performed using job tasks.

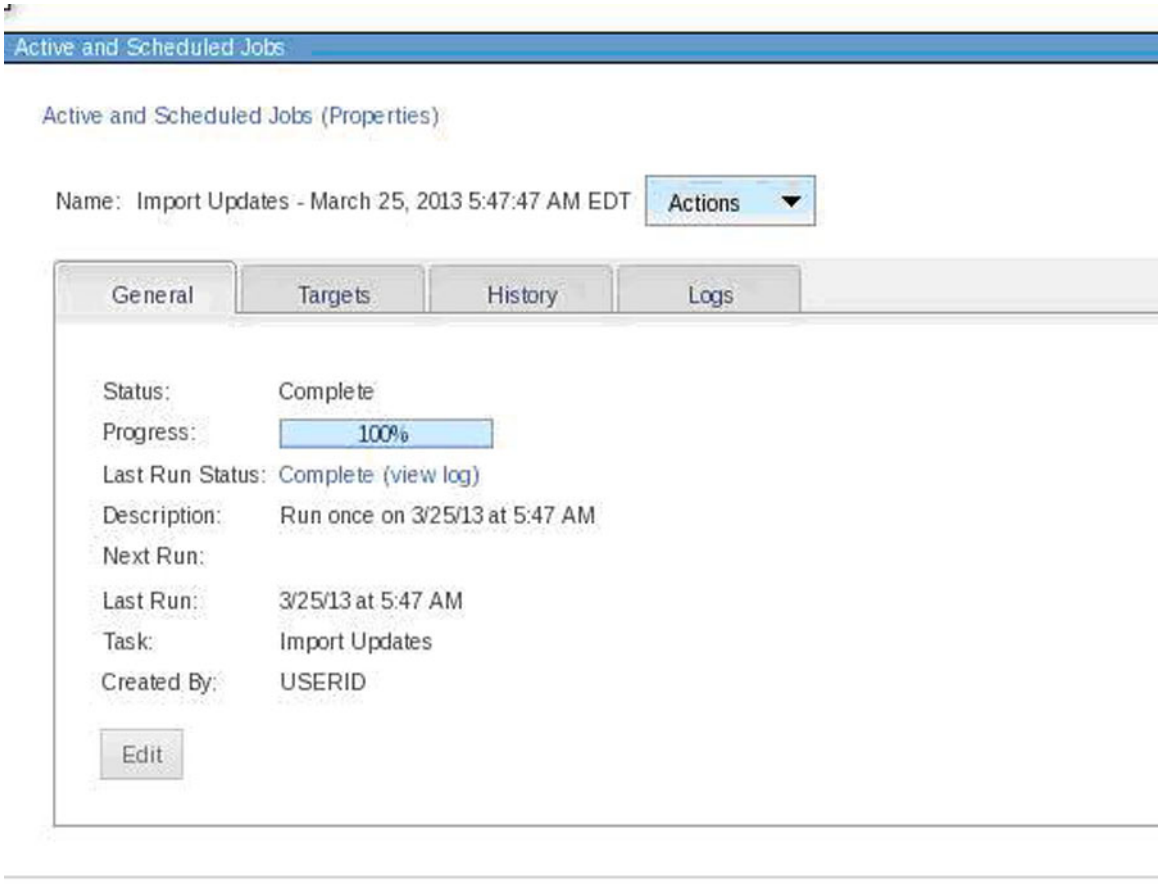
The simplest way to start a job is to select **Run Now**, as shown in the following example:



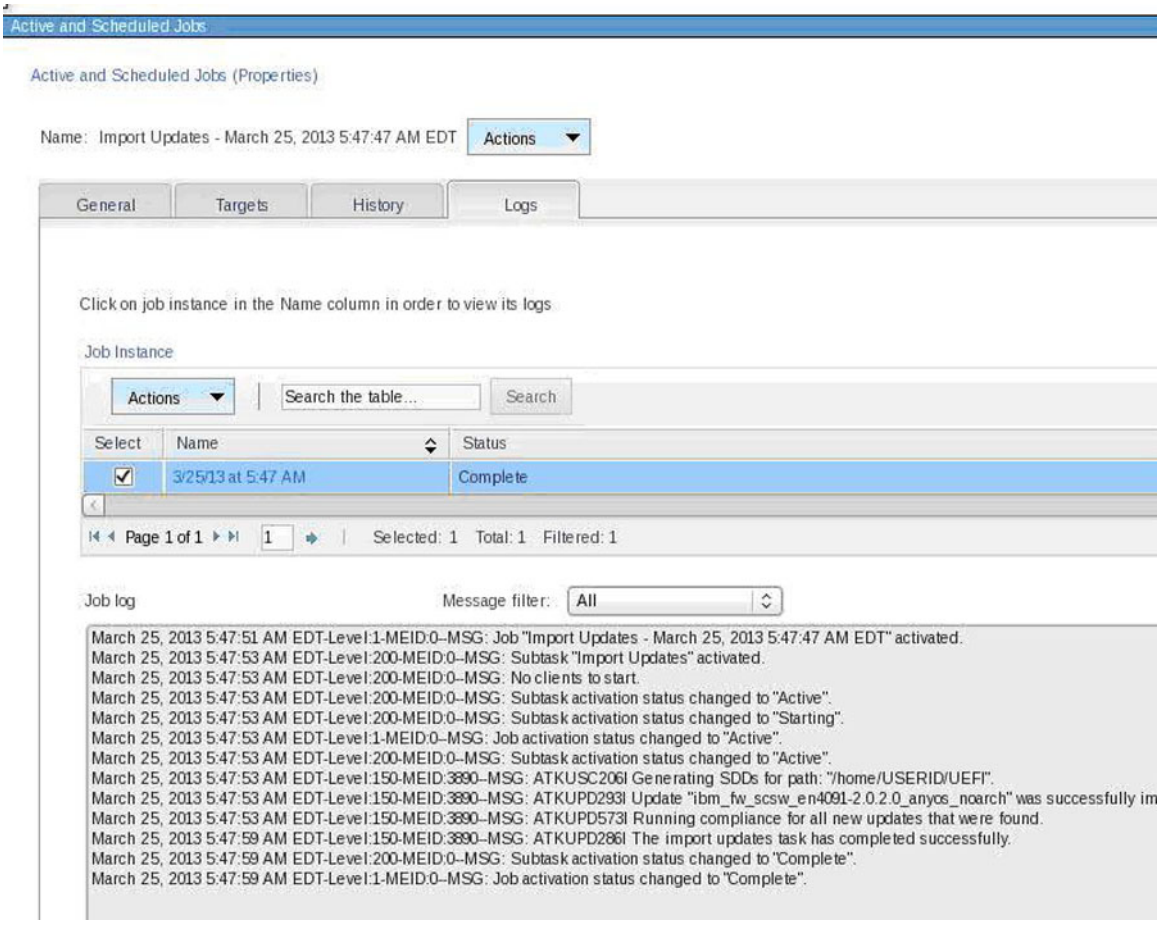
You can monitor and wait for the job to complete by selecting **Display Properties** as shown in the following example:



From the Job Properties dialog, use the **General** tab for an overview of your job status. The status can be running, complete or complete with errors.



Use the **Logs** tab to see job details, including any errors that might have occurred.



A.2 Displaying firmware inventory

You can determine the specific firmware levels that are installed for each of the components in the chassis through the IBM FSM.

Procedure

Note: You must have already collected inventory for a component to see the list firmware levels installed on a component.

Tip: The following procedure explains how to view firmware levels for a specific component. To view all firmware levels for all components, complete the following steps:

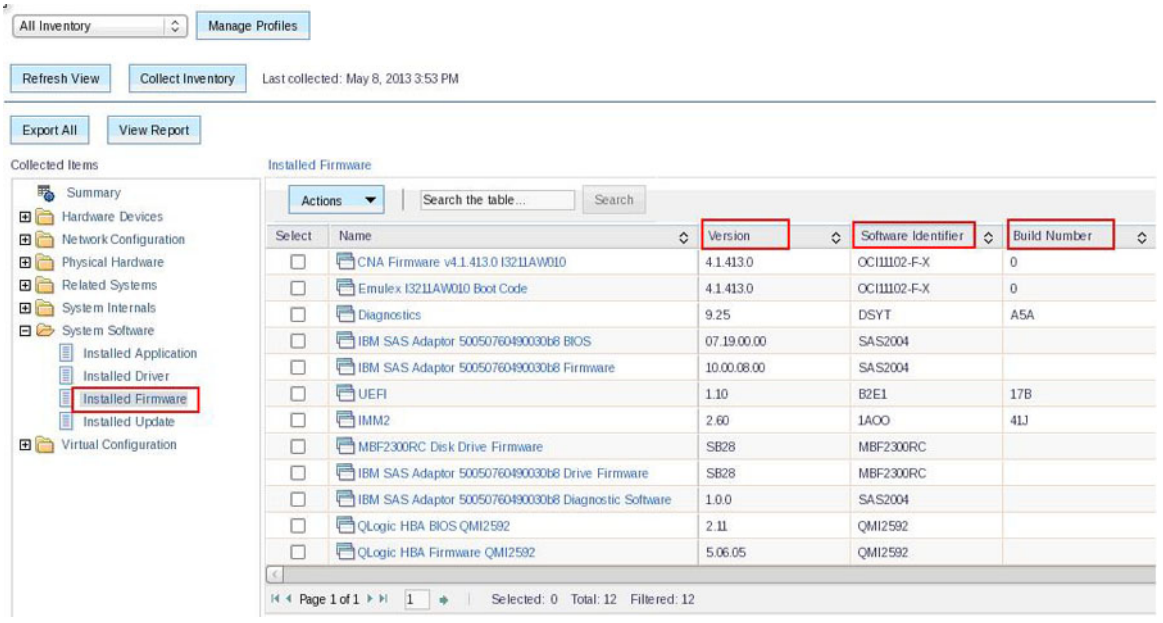
1. From the Initial Setup tab on the Home page, click **Update Chassis Components**.
2. Under List all Firmware Levels and Compliances, click **View All Firmware Levels**.
3. Make sure that Chassis and Members is listed for Target Systems. The firmware levels for all chassis components is listed.

Complete the following steps to display firmware inventory for a specific component:

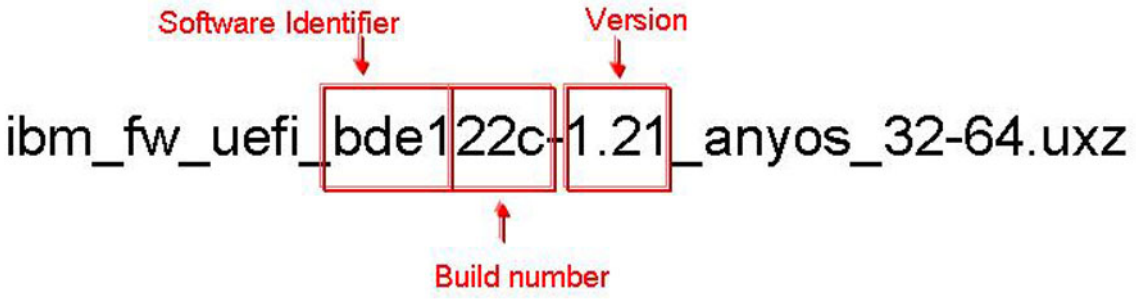
1. From the Chassis Manager, select the component (such as an X-Architecture compute node).
2. Right-click the component; then click **Inventory** > **View and Collect Inventory** to display the View and Collect Inventory panel.
3. Click **System Software** > **Installed Firmware** to see a list of the firmware installed for the component.

Results

The following example shows a list of the firmware installed on an X-Architecture compute node:

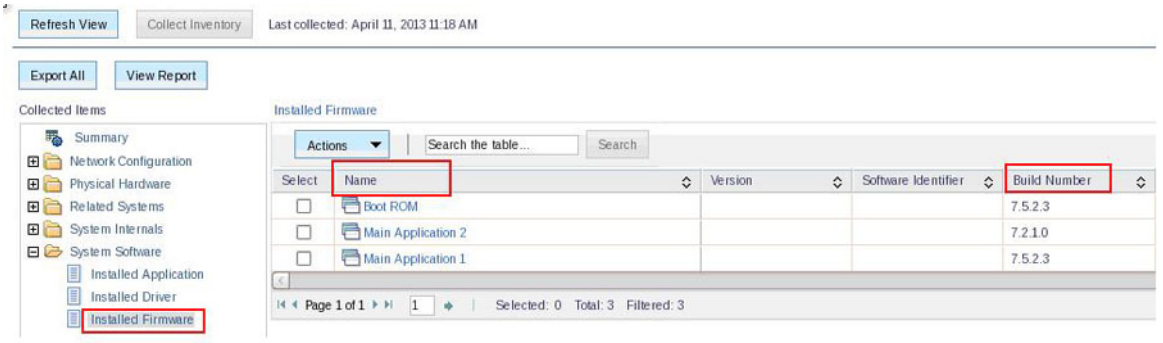


The installed version of IMM, UEFI, or pDSA firmware is determined by the Version and Build Number fields. For example, consider a firmware update for UEFI that you might see for the Flex System x240 Compute Node:



The installed version of non-IBM firmware is determined by the Version and Software Identifier fields.

The following example shows the firmware listed for an I/O module:



Typically, the installed firmware version is determined by the Build Number and Name fields.

A.3 Acquire updates wizard

The Acquire Updates wizard enables you to obtain the firmware updates that you need to update components in a chassis through an IBM FSM.

About this task

The Acquire Updates wizard enables you to obtain the firmware updates that you need to update components in a chassis through an IBM FSM.

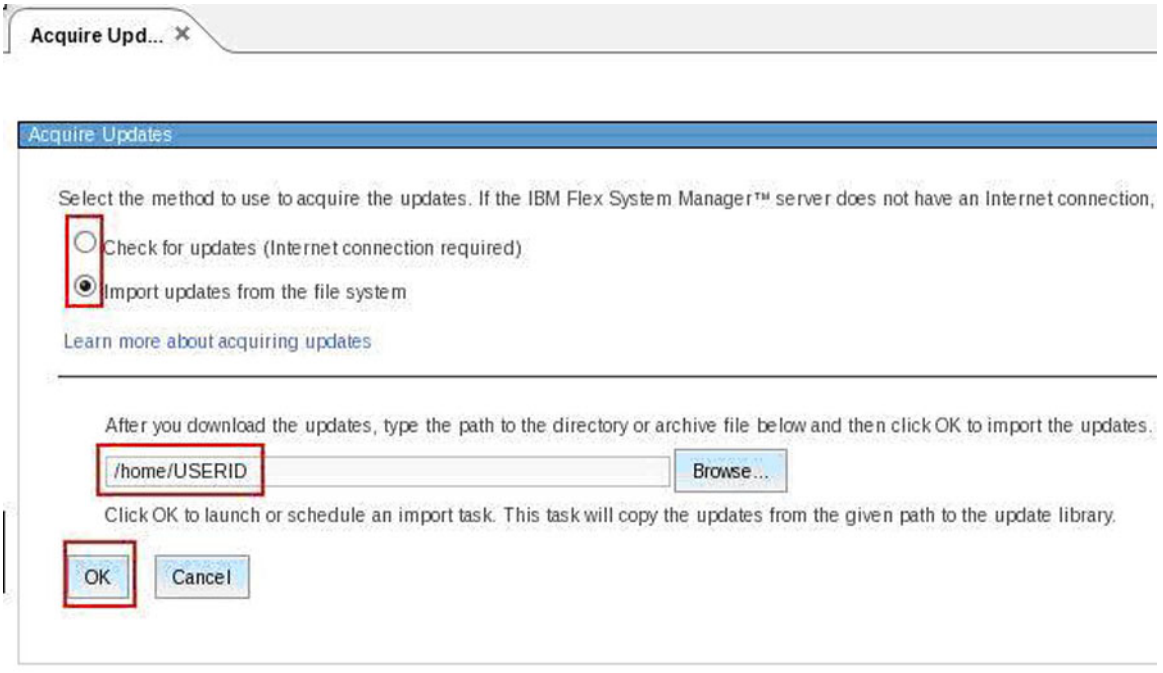
- If you are updating components through an IBM FSM that is connected directly to the Internet, the Acquire Updates wizard allows you to download updates directly from IBM when the FSM is connected to the internet. Therefore, you would click **Check for updates (Internet connection required)** from the Acquire Updates wizard.
- If you are updating components through an IBM FSM that is not connected to the Internet, you can download the updates from the IBM website, copy those updates to a directory on the IBM FSM, and then specify the location on the file system where those updates are located. Therefore, you would click **Import updates from the file system** from the Acquire Updates wizard. Enter any valid path. Remember to enter a path, **not** a filename here.

Important considerations:

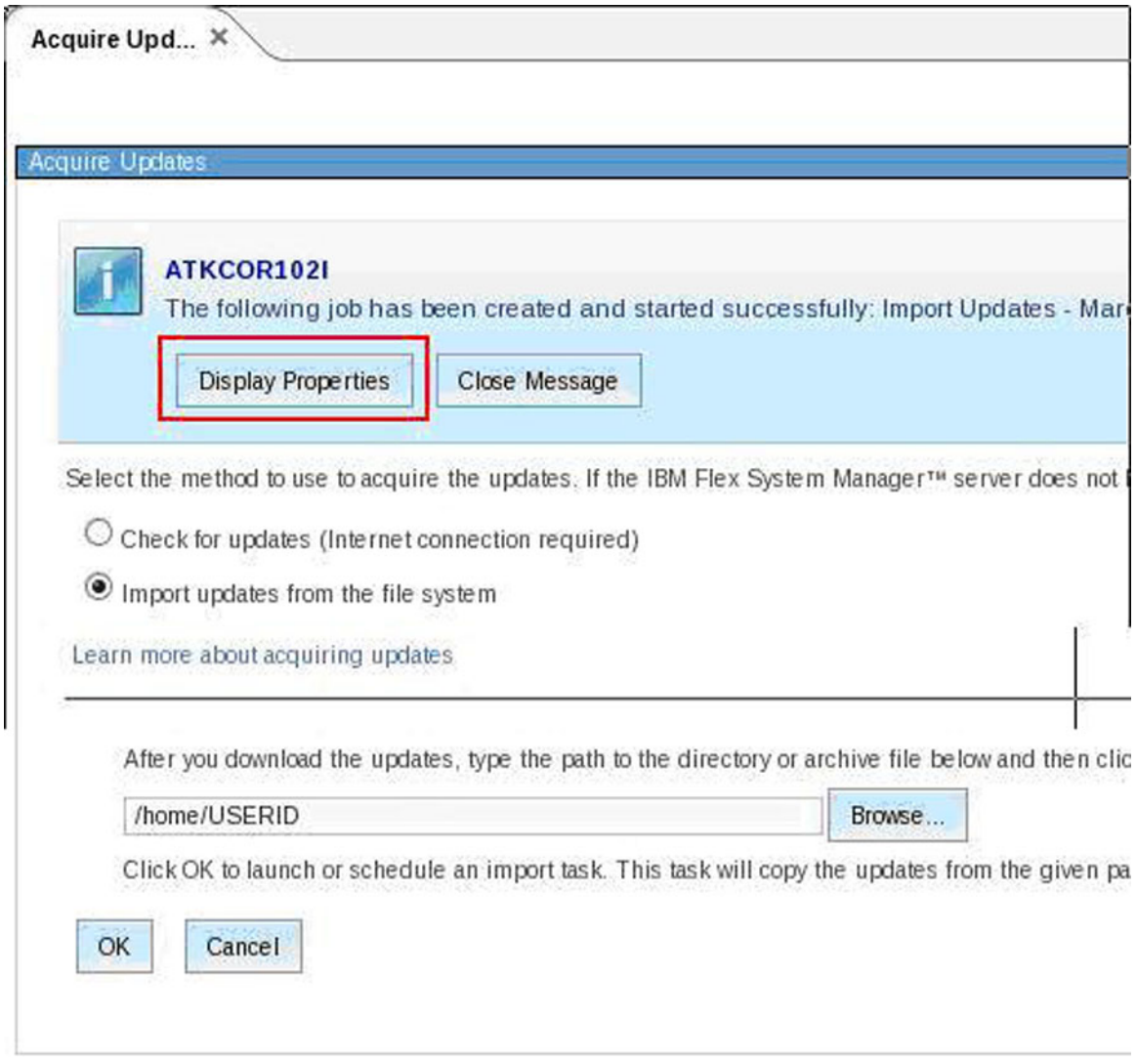
In Chapter 3, "Updating firmware from an FSM that is not connected to the Internet," on page 63, you copied updates over to the IBM FSM and then imported those updates to the IBM FSM updates library (and deleted the updates from the directory where you copied them). However, you will still enter a valid path, such as `/home/USERID` in the Acquire Updates wizard. You might receive an error stating that no updates were found, but you can ignore that error and proceed with the next step to show all updates for a component.

Procedure

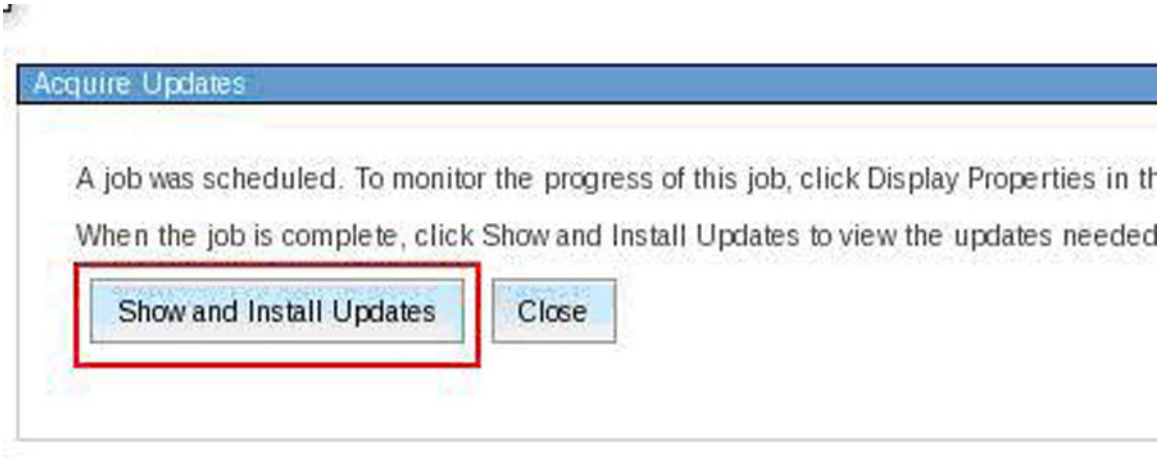
The following example shows the first step in the Acquire Updates wizard.



1. Make the appropriate selections on the panel and click **OK** to display the Launch Job window.
2. Go the to the Schedule tab and select **Run Now**. A message stating that the job was created and started successfully is displayed.
3. Click **Display Properties** to monitor the job status.



4. Close the **Active and Scheduled Jobs** tab once the update has successfully imported.
5. Click the **Show and Install Updates** button in the Acquire Updates tab.



Note: If you are updating components through an IBM FSM that is not connected to the Internet, you should have already imported updates into the IBM FSM updates library, so you might receive an error stating that no updates were found. You can ignore that error and proceed with showing and installing the update.

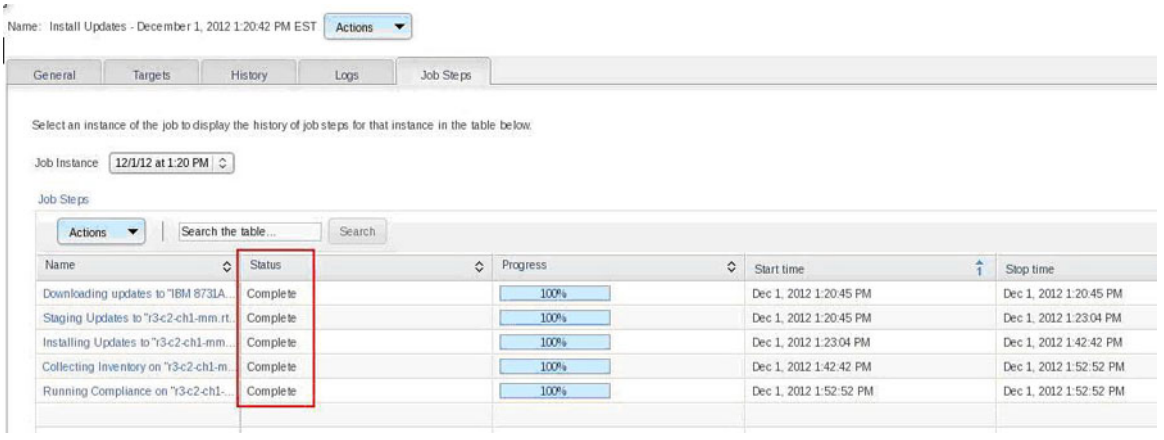
6. Select the updates that apply and click **Install**.
7. At the Summary page, click **Finish** to start the job.

A.4 Verifying an update completed successfully

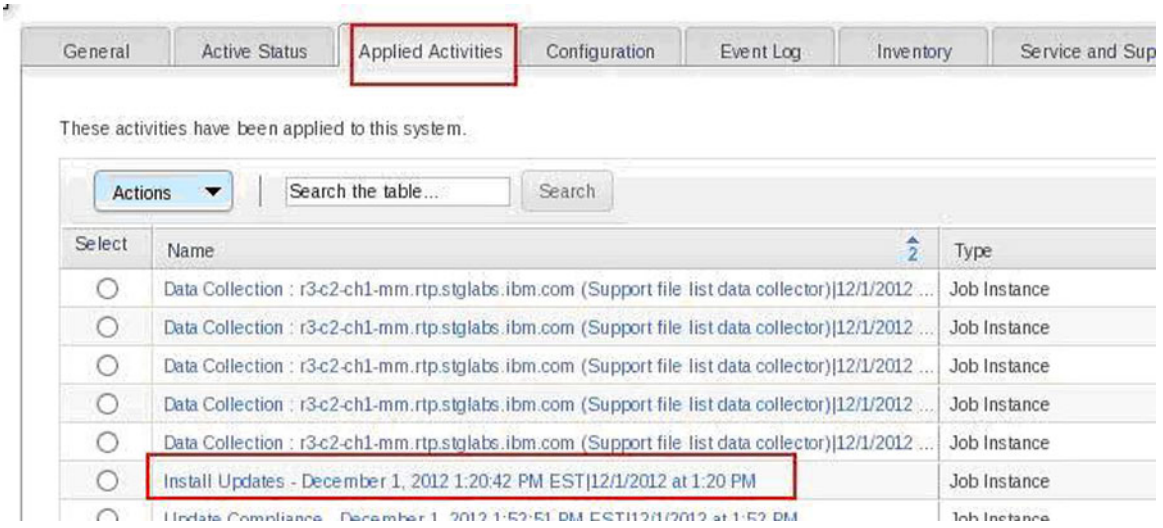
You can verify that an update task succeeded.

Procedure

1. If the update task display is still open, select the **Jobs Steps** tab and verify all steps have completed with Status Complete:



2. You can display previous tasks including tasks started from the FSM command-line interface (CLI) by going to the Chassis Manager.
   a. Right-click on a component, such as a compute node, and click **Advanced Properties**.
   b. In the Applied Activities tab, select the installation task for the update that you performed:


General
Active Status
Applied Activities
Configuration
Event Log
Inventory
Service and Sup
These activities have been applied to this system.
Actions
Search the table...
Search
Select
Name
Type
Data Collection : r3-c2-ch1-mm.rtp.stglabs.ibm.com (Support file list data collector)|12/1/2012 ...
Job Instance
Data Collection : r3-c2-ch1-mm.rtp.stglabs.ibm.com (Support file list data collector)|12/1/2012 ...
Job Instance
Data Collection : r3-c2-ch1-mm.rtp.stglabs.ibm.com (Support file list data collector)|12/1/2012 ...
Job Instance
Data Collection : r3-c2-ch1-mm.rtp.stglabs.ibm.com (Support file list data collector)|12/1/2012 ...
Job Instance
Data Collection : r3-c2-ch1-mm.rtp.stglabs.ibm.com (Support file list data collector)|12/1/2012 ...
Job Instance
Install Updates - December 1, 2012 1:20:42 PM EST|12/1/2012 at 1:20 PM
Job Instance

Appendix B. Where to find more information

There are several locations where you can find more information related to IBM Flex System products and IBM PureFlex offerings.

- IBM PureSystems Centre website:
  http://www.ibm.com/software/brandcatalog/puresystems/centre/
- Initial Setup:
  http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/getting_started.html
- IBM FSM backup information:
  http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/backing_up_frm.html
- Instructions for transferring files to the IBM FSM:
  http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/com.ibm.director.updates.helps.doc/fqm0_t_um_updates_director_manual_download.html
- Update Considerations for specific Operating Systems:
  http://pic.dhe.ibm.com/infocenter/flexsys/information/index.jsp?topic=%2Fcom.ibm.acc.8731.doc%2Fcom.ibm.director.updates.helps.doc%2Ffqm0_c_um_platform_extensions.html
- IBM FSM task support for VMware ESXi /vSphere:
  http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/com.ibm.director.plan.helps.doc/fqm0_r_task_support_for_vmware_esxi_systems.html
- Considerations for VMware ESXi /vSphere Updates:
  http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/com.ibm.director.updates.helps.doc/fqm0_c_um_considerations_for_updating_vmware-esxi.html
- IBM FSM security settings:
  http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/frm_security_policies.html
- Preparations for Windows managed systems:
  http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/com.ibm.director.install.helps.doc/fqm0_t_preparing_windows_managed_systems.html
- Performing a system discovery through the IBM FSM:
  http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/com.ibm.director.discovery.helps.doc/fqm0_t_performing_system_discovery.html
- Collecting inventory on components in a chassis through the IBM FSM:
  http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/com.ibm.director.discovery.helps.doc/fqm0_t_collecting_inventory.html
- Configuring Update Manager:
  http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/com.ibm.director.updates.helps.doc/fqm0_t_um_configuring_update_manager.html
- Integrated Management Module II User's Guide:
  http://www.ibm.com/support/entry/portal/docdisplay?lndocid=MIGR-5086346
- IBM Fast Setup:
  http://www.ibm.com/support/entry/portal/docdisplay?lndocid=TOOL-FASTSET
- IBM Bootable Media Creator:
  http://www.ibm.com/support/entry/portal/docdisplay?lndocid=TOOL-BOMC

Part Number: 00FH377

Printed in USA

(1P) P/N: 00FH377