IBM Flex System and IBM PureFlex Backup and Restore Best Practices

Flex Version 1.3.2

IBM Flex System and IBM PureFlex Backup and Restore Best Practices

Flex Version 1.3.2

First Edition (August 2013)

Chapter 1. Introduction

This document describes the best practices for backing up and recovering IBM Flex System® and IBM® PureFlex™ components.

A backup of the management software includes the following data:

- The management software image
- The local IBM Flex System Manager user registry
- IBM Flex System Manager configuration settings (including network settings)
- The list of discovered endpoints and inventory
- Configuration pattern data

1.1 Getting started

This section provides an overview of the order of operations for performing backup and recovery of your IBM Flex Systems environment. Use this section as a guideline for your backup and recovery process, or follow the links for more information on how to backup and restore systems in your Flex environment.

1. Plan your backup and create a backup policy:
   a. Determine the criteria for creating backups in your environment. For help, see 1.2, "When to perform backups," on page 2.
   b. Allocate sufficient time for creating backups. See 1.3, "How much time to set aside for backup," on page 2 for guidance.
   c. Specify and document your file naming conventions. See 1.4.1, "Determine file naming conventions for archives and backups," on page 5 for suggestions.
   d. Ensure that the chassis to be backed up are being managed by an IBM Flex System Manager. For instructions, see 1.4.2, "Making sure that the IBM FSM is managing the chassis," on page 5.
2. Back up the components in your Flex Systems environment:
   a. Print the 2.1, "Backup checklist," on page 7.
   b. Perform an inventory for all managed devices using the Flex System Manager. This is described in 1.4.2, "Making sure that the IBM FSM is managing the chassis," on page 5.
   c. Backup the IBM Flex System Manager and management software, as described in 2.3, "Backing up the IBM FSM," on page 8.
   d. Backup up the x-Architecture compute nodes as described in 2.4.2, "Backing up x86 Compute Nodes," on page 16.
   e. Backup Power systems compute nodes as described in 2.4.3, "Backing up Power Systems compute nodes," on page 19.
   f. Backup the Chassis Management Module (CMM) as described in 2.4.1, "Backing up the Chassis Management Module (CMM)," on page 15.
   g. Backup Top-of-Rack (ToR) SAN switches as described in 2.5, "Backing up top-of-rack switches," on page 22.
   h. Backup Flex System Chassis Network switches as described in 2.4.5, "Backing up I/O modules," on page 22.
   i. Backup ITE operating systems and customer data according to your current process.
   j. Archive the setup and configuration documentation for your Flex environment. This usually includes, but is not limited to:
      - Setup build sheets.
      - Network configuration diagrams.

- PureFlex eConfig files, when applicable.

3. Restore your Flex environment from backups:
   a. Determine whether your current environment is compatible with your backups. See 3.1, “Restoring and version compatibility,” on page 23 for information on version compatibility.
   b. Restore the management software image. See 3.2, “Restoring the management software image,” on page 24 for more information.
   c. Perform inventory using the restored management software image. If the existing environment does not match the information in the backup, reconcile the environments by manually removing missing systems or adding systems not included in the backup.
   d. Restore the Chassis Management Module as described in 3.3.1, “Restoring the Chassis Management Module (CMM),” on page 25.
   e. Restore x-architecture compute nodes as described in 3.3.2, “Restoring X-Architecture compute nodes,” on page 26.
   f. Restore Power systems compute nodes as described in 3.3.3, “Restoring Power Systems compute nodes,” on page 29.
   g. Restore IBM V7000 storage nodes as described in 3.3.4, “Restoring the IBM Flex System V7000 storage node,” on page 30.
   h. Restore I/O modules as described in 3.3.5, “Restoring I/O modules,” on page 34.
   i. Restore ToR switches as described in 3.4, “Restoring up top-of-rack switches,” on page 36.
4. When you have restored all components, validate your system restoration as described in the Firmware Update Guides.

1.2 When to perform backups

In general, backups of IBM Flex System and IBM PureFlex System components should occur whenever significant changes have been made to the configuration of those components.

1.3 How much time to set aside for backup

The amount of time required to back up all IBM Flex System and IBM PureFlex System components depends on the number of devices for which a backup needs to be performed.

Backup does not affect the workload that is running in the chassis, including the FSM. Unless I/O module intensive activities are running, the backup is generally not disruptive. The examples in this section assume one unit of each type of hardware and are intended to provide guidance on approximate times for planning purposes.

Note: Configuration backup is straightforward. Backing up data volumes, such as FSM or VIOS backups, may significantly impact the performance of the module. For optimal performance, these types of backups should be run at off-peak hours.

1.3.1 Example times for single-chassis backup

The table in this topic breaks down estimated backup times for single items.

Table 1. Estimated backup times for single-chassis components

Single item	**Estimated backup time (in minutes)**
CMM settings	2
IMM settings	2
FSM appliance disks content (excluding IMM settings)	32
FSM inventory data for visual reference (chassis Map screen shot and html, full inventory csv, logical networks csv, virtual servers csv, VLAN csv)	7
Power ITE partition profile data	2
VIOS settings and data volume (**viosbr** / **backupios**)	1/17
KVM virtual servers list and virtual resources settings	5
ESXi virtual servers list and virtual resources settings	3
vCenter inventory and virtual resources settings	2
Ethernet chassis switch settings (EN4093)	2
Converged chassis switch settings (CN4093)	2
FC3171 SAN switch settings (QLogic)	2
FC5022 SAN switch settings (Brocade)	2
DVS 5000V virtual switch settings	2
Switch Center settings and data volume	3
Storwize & Flex V7000 settings (exclude IMM settings)	3
Total (mins)	**89**

1.3.2 Example times for two-chassis backup

The table in this topic breaks down estimated backup times for items for two chassis.

Table 2. Estimated backup times for components in two chassis

Backup items	Two chassis (time in minutes)		Comments
CMM settings	2	32	One could write a script to invoke all of these backup tasks in parallel from the FSM. The total duration would be the longest task's time. The FSM does not provide either a script or a job schedule to perform this function.
IMM settings	2		
FSM appliance disks content (exclude IMM settings)	32		
VIOS settings and data volume (**viosbr** / **backupios**)	1/17		
Storwize & Flex V7000 settings (exclude IMM settings)	3		
KVM virtual servers list and virtual resources settings	5		
FSM inventory data for visual reference (Chassis Map screen shot & html, full inventory csv, logical networks csv, virtual servers csv, VLAN csv)	7		FSM GUI
vCenter inventory and virtual resources settings	2		vCenter
ESXi virtual servers list and virtual resources settings	3		vCLI
Ethernet chassis switch settings (EN4093)	2	2	The Switch Center has a GUI button you can click to back up all of the switches' configurations at once. The more switches that it is managing, the greater the time-saving potential.
Converged chassis switch settings (CN4093)	2		
DVS 5000V virtual switch settings	2		
Switch Center settings and data volume	3		SC
FC3171 SAN switch settings (QLogic)	4		Native UI 2*n
FC5022 SAN switch settings (Brocade)	4		Native UI 2*n
Total (mins)	89	57	Non disruptive backup of entire chassis

1.4 Before you begin

If you are using an IBM Flex System Manager management node (IBM FSM) to manage IBM Flex System and IBM PureFlex System, make sure that the IBM FSM has discovered all managed devices and that you perform a full inventory of all managed devices before you begin the backup process.

1.4.1 Determine file naming conventions for archives and backups

You should determine naming conventions for all files that you will generate during the backup process. This will enable you to more quickly recover data during the restoration process.

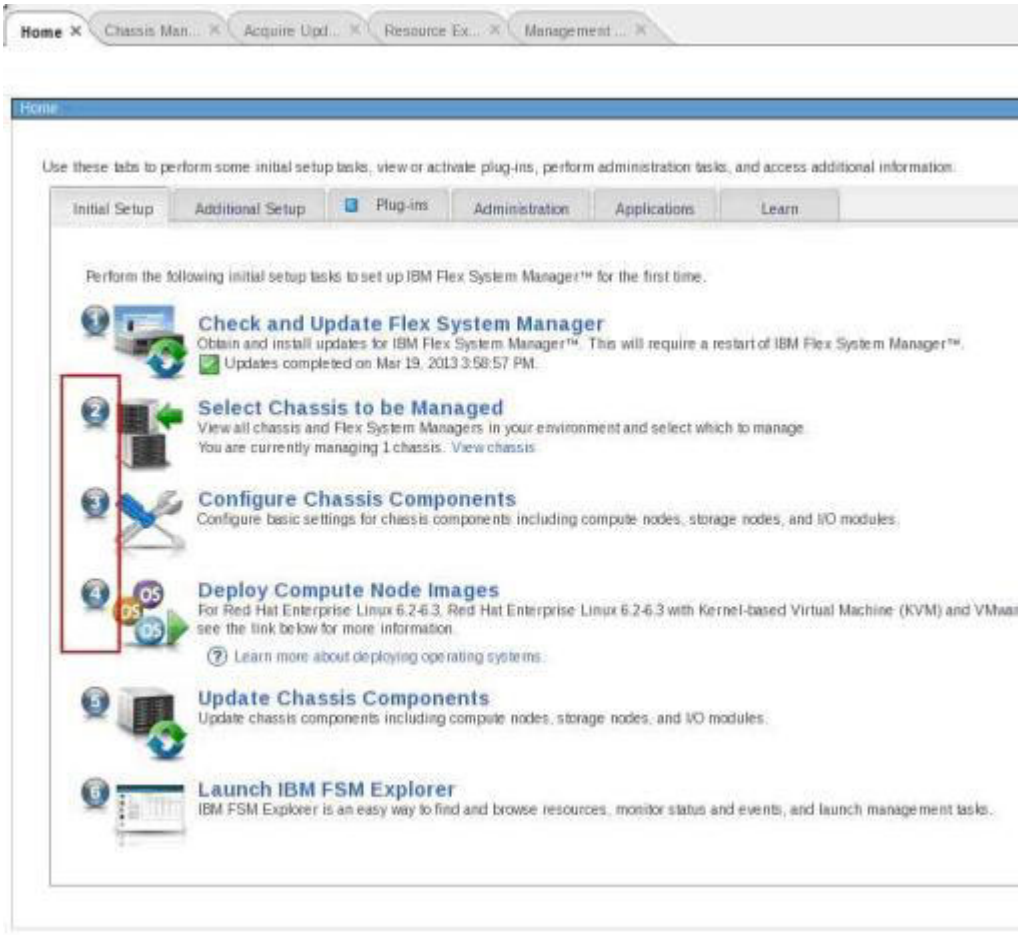
Note: The backup file is time-stamped, and renaming it is not recommended. Some files, such as the FSM backup file that is stored on the HDD, cannot be renamed.

1.4.2 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).

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 on the **Chassis Manager** and selecting the common action **Remote Access** > **Remote Control** to start a remote login session to the operating system and determine the IP address.

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



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**.

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

   http://publib.boulder.ibm.com/infocenter/flexsys/information/topic/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://publib.boulder.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/fqm0_t_requesting_access_to_a_secured_system.html

   Note: You can only perform this step if an operating system is not already installed or if you are running VMware or Red Hat Enterprise Linux.
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:
   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**.

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

   http://publib.boulder.ibm.com/infocenter/flexsys/information/topic/com.ibm.director.discovery.helps.doc/fqm0_t_collecting_inventory.html

Chapter 2. Backing up the system

When you back up the system, make sure that you back up the IBM FSM, all chassis components, all top-of-rack switches, and all external storage devices.

2.1 Backup checklist

Use this checklist to ensure that you have backed up your entire system in the correct order.

Important: It is recommended that all backed-up data be encrypted.

Table 3. Backup checklist

Step	Task name	Description
1	Inventory	Perform full system inventory on all managed devices via the FSM.
2	IMM backup	Capture, export, and archive for all IMMs.
3	System p – backup data profile	Backup the Profile Configuration via the FSM.
4	System p – backup VIOS	Backup the VIOS configuration via the FSM.
5	CMM backup	Capture, export, and archive all primary CMMs.
6	FSM Chassis Map – Graphical	Capture, and archive a screenshot picture via the FSM for each chassis managed.
7	FSM Chassis Map – Table View	Capture, export and archive the chassis map table view csv files via the FSM for each chassis managed.
8	FSM Resource Explorer – Full Inventory	Capture, export (as html) and archive full inventory using Resource Explorer.
9	FSM Resource Explorer – Logical Networks & Members	Capture, export and archive Logical Network view using FSM Resource Explorer.
10	FSM Resource Explorer – Virtual Servers and Hosts	Capture, export and archive Virtual Servers and Hosts view using FSM Resource Explorer.
11	FSM Resource Explorer – Systems by VLAN and Subnet	Capture, export and archive Systems by VLAN and Subnet view using FSM Resource Explorer.
12	FSM Full Backup	Capture, export and archive the FSM Backup using the FSM Administration functions.
13	Backup Top-of-Rack (ToR) SAN Switches	Capture, export, and archive configuration data.
14	Backup Flex System Chassis Integrated SAN Switches	Capture, export, and archive configuration data.
15	Backup IBM Storwize V7000	Capture, export, and archive configuration data.
16	Backup Top-of-Rack (ToR) Network Switches	Capture, export and archive all Top-of-Rack Network switches.
17	Backup Flex System Chassis Network Switches	Capture, export, and archive all PureFlex Chassis integrated Network switches.
18	Backup ITE OS and Customer Data	Use current backup procedures to validate regular backups are being performed and current for all systems.
19	LBS/ITS Setup Buildsheets	Archive any Lab Services or ITS Buildsheets that were provided during initial setup.
20	Network Configuration if not on Buildsheet	Archive any Network Configuration data that is not included in the LBS/ITS Buildsheets.

Table 3. Backup checklist (continued)

Step	Task name	Description
21	PureFlex eConfig files	Archive any eConfig files that were used in the ordering of the PureFlex HW. Human readable output is preferable.

2.2 Saving the IBM PureFlex configuration files

If you purchased an IBM PureFlex system, save the eConfig files used to generate the order and the setup buildsheets that were provided to you during initial installation.

Note: An IBM PureFlex System can be ordered without IBM LBS. The buildsheets or network diagrams are provided only if LBS services were included.

2.2.1 Saving setup buildsheets

An IBMPureFlex installation should be accompanied by build/configuration sheets and network diagrams prepared by those who performed initial setup and configuration.

Note: It is important to maintain these configuration and network diagrams on an ongoing basis. Archive buildsheets that were provided during the initial setup.

2.3 Backing up the IBM FSM

When you back up the IBM FSM, make sure that you complete all procedures in this section so that you can recreate the IBM FSM if you need to fully recover the IBM FSM in the event of a disaster.

These procedures combined with the Backup/Recovery DVDs should enable you to recreate your IBM FSM if required.

2.3.1 Capture the Chassis Manager view (optional)

For **each** chassis being managed by the IBM FSM, use a screen capture program to capture the graphical view of the Chassis Manager. Make sure to select the Hardware Status view. This screen capture will enable you to know the exact bay locations for all devices in the chassis.

Note: This procedure is optional. It is useful in disaster recovery scenarios when it is necessary to replace all hardware and set it up to look like the original.

Complete the following steps to capture the graphical view of the chassis manager.

1. Log in to the IBM FSM Web interface from a Web browser.
2. From the home page, select the **Chassis Manager** tab.
3. From the list of managed chassis, select a chassis by double-clicking on a chassis name to display the graphical view.

4. Make a screen capture of the Chassis Manager and save it to your backup archive. Make sure that you name the file according to the previously established file naming conventions.

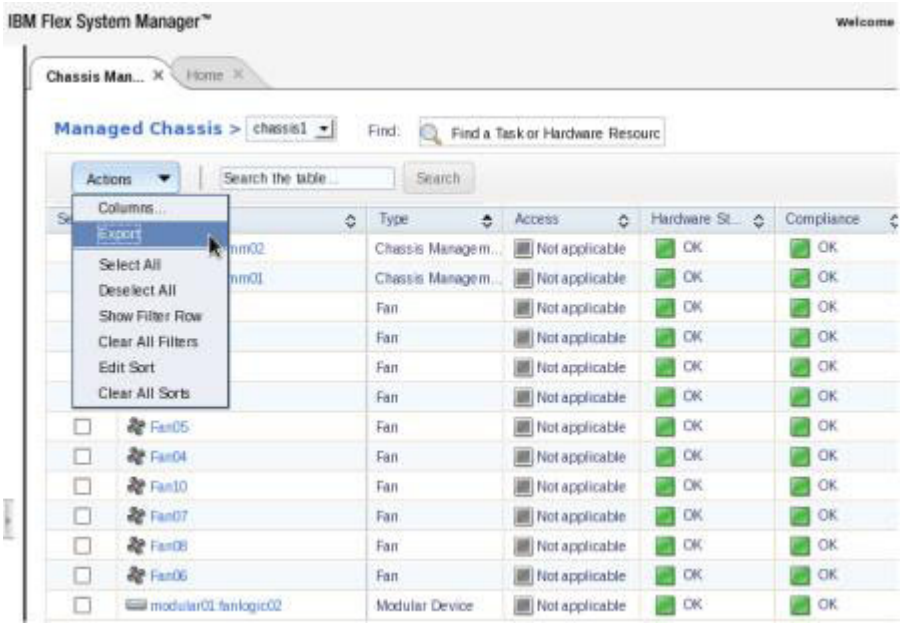
2.3.2 Export the Chassis Manager table view (optional)

For each chassis being managed by the IBM FSM, export the table view and save the file as part of your backup archive.

Note: This procedure is optional. It is useful in disaster recovery scenarios when it is necessary to replace all hardware and set it up to look like the original.

Complete the following steps to export the table view.

1. From the Chassis Manager graphical view, click **Table view**.
2. Click **Actions** > **Export**.



The file is saved as Chassis_Map.csv

3. Copy the file to the location where you are storing your archives. Make sure that you name the file according to previously established file naming conventions.

2.3.3 Capture inventory data for the chassis (optional)

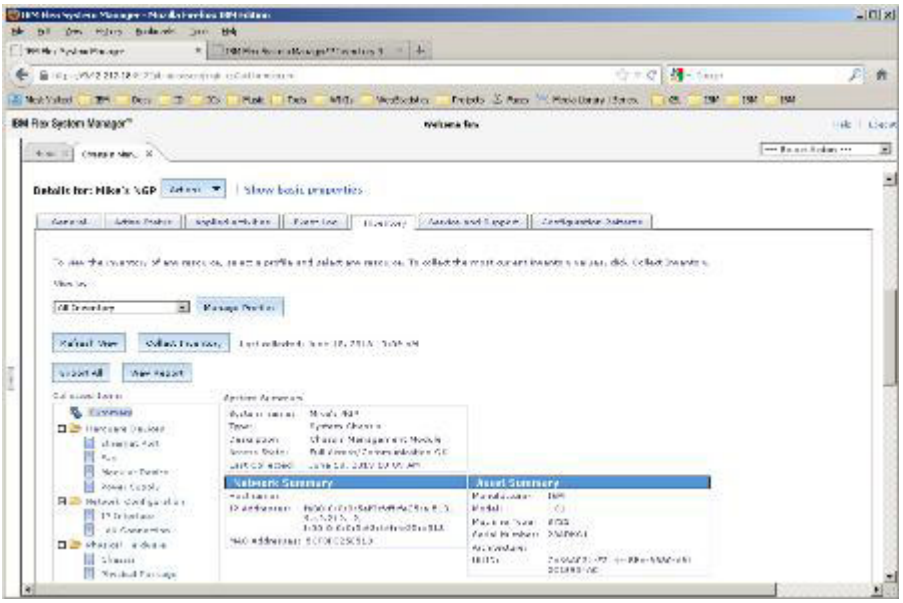
For each chassis being managed by the IBM FSM, capture the inventory data for all devices in the chassis.

Note: This procedure is optional. It is useful in disaster recovery scenarios when it is necessary to replace all hardware and set it up to look like the original.

Tip: Make sure that you have performed a full inventory on the chassis before capturing the inventory data. See 1.4.2, "Making sure that the IBM FSM is managing the chassis," on page 5 for details about performing a full inventory.

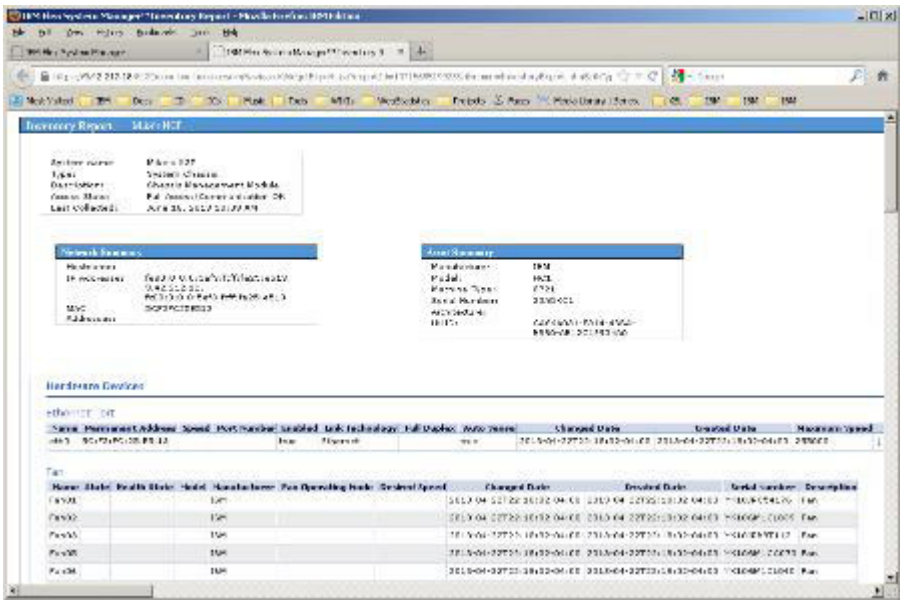
Complete the following steps to export the table view.

1. From the Chassis Manager graphical view, click the chassis itself.
2. In the Details section at the bottom of the page, click **Show Advanced Properties**.
3. Click the **Inventory** tab to display the inventory for the chassis.



4. Click **Export All** to display the Export Inventory page:

5. Click **OK** to display the results in your Web browser:



6. Save the HTML page. The default name is InventoryExport.html.
7. Copy the file to the location where you are storing your archives.

2.3.4 Export logical networks and members

For each chassis being managed by the IBM FSM, capture the logical networks configuration.

Complete the following steps to export logical networks and members:

1. From the Chassis Manager, enter **Logical Networks and Members** in the find field.
2. Select the Task tab and click **Logical Networks and Members**

3. From the Logical Networks and Members page, click the **Actions** > **Export** :

The file is saved as Logical_Networks_and_Members__View_Members_.csv

4. Copy the file to the location where you are storing your archives. Make sure that you name the file according to previously established file naming conventions.

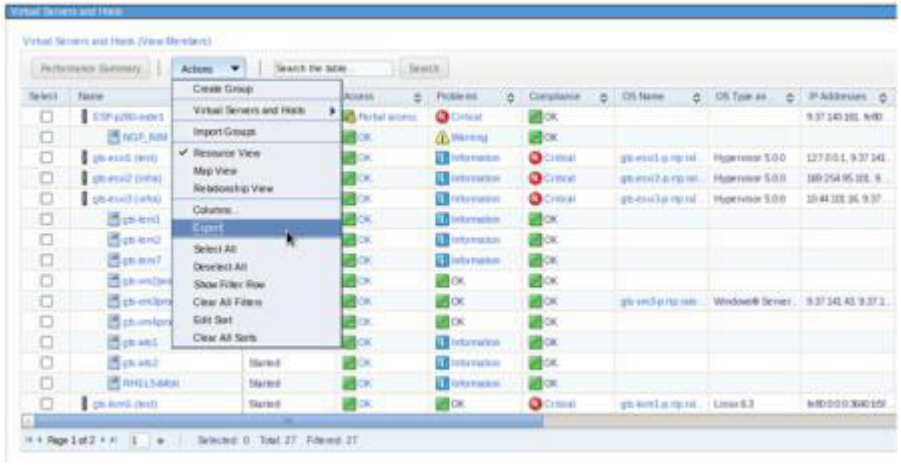
2.3.5 Export virtual servers and hosts

For each chassis being managed by the IBM FSM, capture the virtual server and host configuration.

Complete the following steps to export virtual servers and hosts:

1. From the Chassis Manager, enter **Virtual Servers and Hosts** in the find field.
2. Select the Task tab and click **Virtual Servers and Hosts**

3. From the Virtual Servers and Hosts page, click the **Actions** > **Export** :



The file is saved as Virtual_Servers_and_Hosts.csv

4. Copy the file to the location where you are storing your archives. Make sure that you name the file according to previously established file naming conventions.

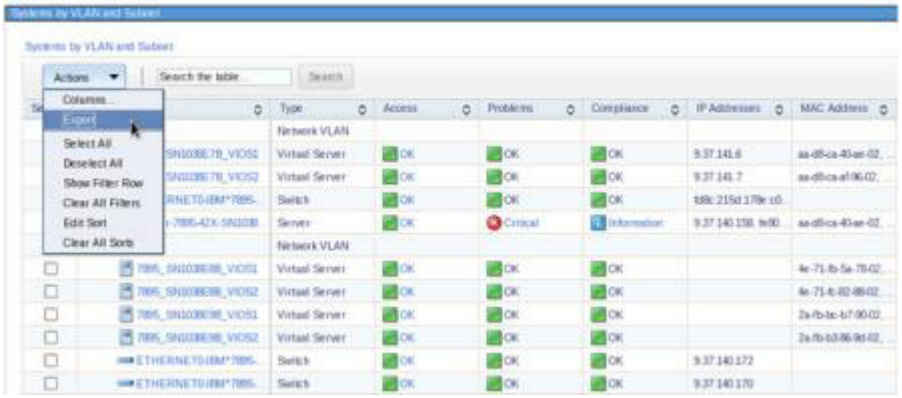
2.3.6 Export VLAN and Subnet configuration

For each chassis being managed by the IBM FSM, capture the VLAN and subnet configuration.

Complete the following steps to export the VLAN and subnet configuration:

1. From the Chassis Manager, enter **Systems by VLAN and Subnet** in the find field.
2. Select the Task tab and click **Systems by VLAN and Subnet**

3. From the Systems by VLAN and Subnet page, click the **Actions** > **Export** :



The file is saved as Systems_by_VLAN_and_Subnet.csv

4. Copy the file to the location where you are storing your archives. Make sure that you name the file according to previously established file naming conventions.

2.3.7 Back up the IBM FSM configuration

Create a backup of the IBM FSM configuration.

Note: This procedure applies to backing up the FSM configuration to secure FTP (SFTP) server. IBM also support backup of the FSM configuration to a local hard disk drive or USB drive. For more information, see Restoring the management software image.

Make sure that the IBM FSM has network access to a secure FTP (SFTP) server. Then complete the following steps to back up the IBM FSM image to the SFTP server:

Run the **smcli lsjob -m** command to determine whether there are active jobs. Either terminate background jobs or wait for the jobs to terminate. The FSM backup may not start or complete if other jobs are running.

Log on to the FSM via the CLI with an smadmin group user and run the **backup -e** command to check uncompressed backup size. Then, prepare enough free space for an sftp backup. The actual backup file size is less than the uncompressed backup size.

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

1. From the Home page, click the **Administration** tab.
2. On the Administration tab under Serviceability tasks, click **Backup and Restore**. The Backup and Restore page opens.
3. From the Backup and Restore page, click **Backup Now**. The Backup Now window opens.
4. 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).

   Important: To back up the management software to an SFTP server, the destination server must have Linux with Secure Shell (SSH) enabled. Otherwise, the backup operation might fail.
6. Enter the User ID and password for the SFTP server (must have sufficient permissions to write to the server).
7. Click **OK**.

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

http://publib.boulder.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/backing_up_frm.html

2.4 Backing up chassis components

Make sure that you back up all component in the chassis.

2.4.1 Backing up the Chassis Management Module (CMM)

The CMM can be backed up through the CMM web interface.

2.4.1.1 Backing up the CMM through the GUI

Use the native CMM GUI to back up the CMM using the GUI method.

Note: It is important that you remember the FSM password in use at the time of the backup, as it is required to restore that backup.

See Saving a CMM configuration for the steps in the procedure.

2.4.1.2 Back up the CMM through the CLI

The CMM can be backed up using the command-line interface of the CMM.

Note: By default, the CMM operates in secure mode. When the CMM is set to secure, only the secure file transfer methods HTTPS and SFTP can be used for firmware updates and other tasks involving file transfers, such as transferring a backup configuration file to restore a configuration. The unsecure file transfer protocols HTTP, FTP, and TFTP are disabled.

Note: It is important that you remember your FSM password, as it is required to restore a backup.

Assume that you have set up an SFTP server as follows:

- IP address: 191.168.1.101
- User ID: userid
- Password: xxxxxxxx
- Encryption Passphrase: b@ckupN0w (zero, not an uppercase o)
- Backup directory: /home/userid/backup

You are creating a backup of the primary CMM.

Complete the following steps to back up the CMM configuration.

1. Using a secure protocol, such as SSH, log in to the CMM CLI interface using a user ID that has Supervisor or Chassis Configuration authority.
2. At the `system>` prompt, enter the following command:

   ```
   write -u sftp://userid:xxxxxxxx@192.168.1.101/home/userid/backup/cmmp.bkp
   -p "b@ckupN0w" -T system:mm[p]
   ```

   where:

   - -u specifies the remote location to which the file will be written.

     Note: You must enter the full destination path for the SFTP server in the URL that you provide.
   - -p specifies a double-quote delimited passphrase that will be needed to restore the configuration file. Minimum passphrase length is 6 characters. Maximum passphrase length is 31 characters.
   - in mm[*x*], *x* is the primary CMM bay number.

   If successful, the system responds with `OK`.

Additional information about the CMM backup process and the CLI command used to perform a backup is available:

- Saving a CMM Configuration

http://publib.boulder.ibm.com/infocenter/flexsys/information/index.jsp?topic=%2Fcom.ibm.acc.cmm.doc%2Fsave_config_cmm.html

- **write** command

  http://publib.boulder.ibm.com/infocenter/flexsys/information/index.jsp?topic=%2Fcom.ibm.acc.cmm.doc%2Fcli_command_write.html

2.4.2 Backing up x86 Compute Nodes

To create a backup of the service processor (Integrated Management Module) on x86 Compute Nodes, use either the IMM graphical user interface or the IMM command-line interface. For operating system and user data, use standard backup procedures.

You need to back up the IMM for every x86 Compute Node in your system.

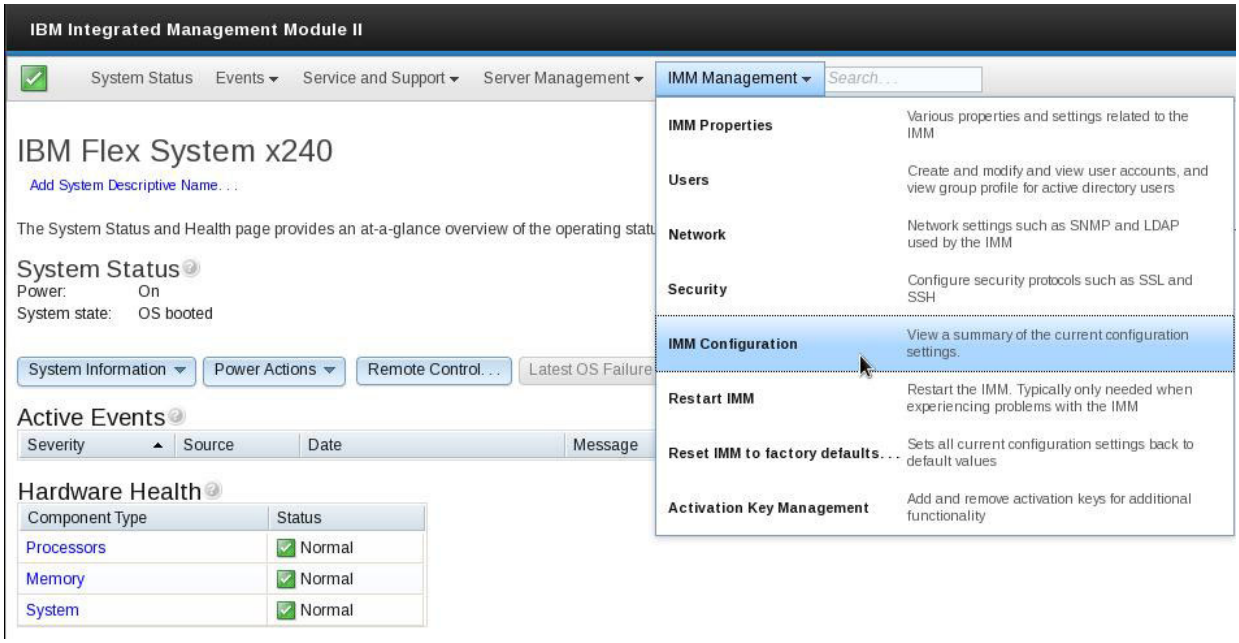
2.4.2.1 Backing up the IMM through the graphical user interface

Follow this procedure to back up the IMM through the graphical user interface.

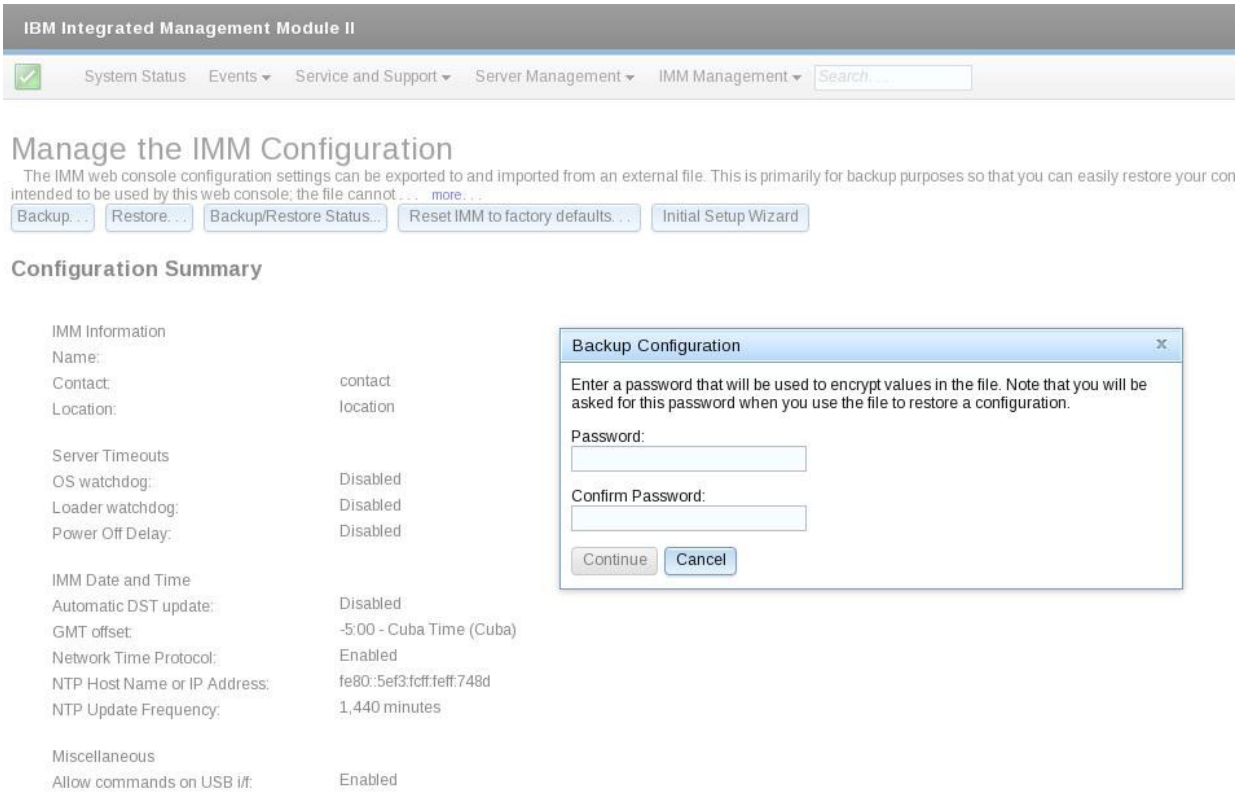
Note: It is important that you remember your FSM password, as it is required to restore a backup.

Complete the following steps to back up the IMM for an X-Architecture compute node:

1. From a Web browser, log in to the IMM graphical user interface for the X-Architecture compute node.
2. From the user interface, click **IMM Management** > **IMM Configuration**.

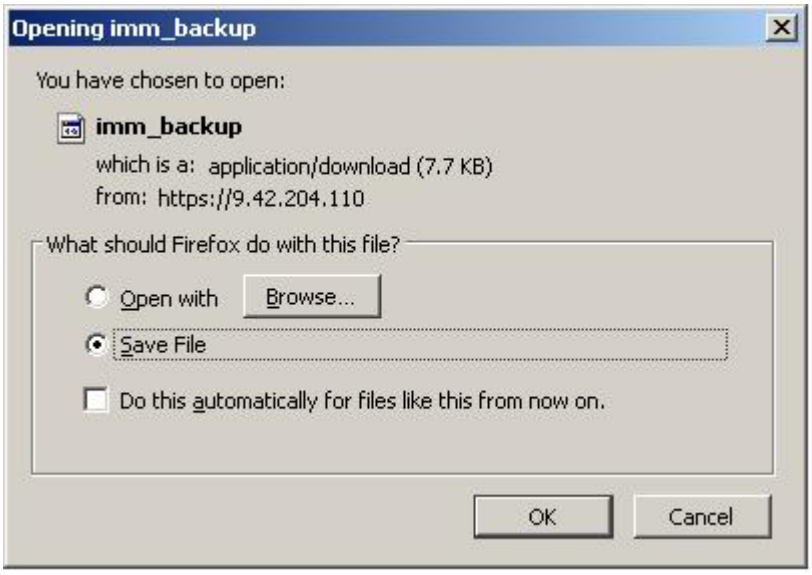


3. From the Manage the IMM Configuration panel, click **Backup**.
4. Enter a password that is used to encrypt the backup on the Backup Configuration panel.



After filling in (and confirming) the password, click **Continue**.

5. Press and hold the **Ctrl** key to display the Save dialog



6. Save the file on your system until you can add it to the archive.
7. Close the confirmation dialog in the IMM graphical user interface.
8. Save the IMM configuration Web page from your Web browser.
   a. If you are using Firefox, click **File** > **Save Page As**
      Save the file as type **Web Page, complete**.
   b. Compress the file (using zip or tar) the file index-console.php, **and** the folder index-console.php_files. Protect the archive through encryption using a strong passphrase.

Repeat this process for all X-Architecture compute nodes. Then, you can copy the files to your archive location.

2.4.2.2 Backing up the IMM through the CLI

The command-line interface can be used to back up the IMM.

Note: It is important that you remember your FSM password, as it is required to restore a backup.

Assume that you have set up an SFTP server as follows:

- IP address: 191.168.1.101
- User ID: backupid
- Password: entR3v0Us
- Encryption Passphrase: b@ckupN0w (zero, not an uppercase o)
- Backup directory: /home/userid/backup

Complete the following steps to back up the IMM configuration.

1. Using a secure protocol, such as SSH, log in to the IMM CLI interface.
2. At the system prompt, enter the following command:

   ```
   backup -f imm_backup -pp "b@ckupN0w" -ip 192.168.1.101 -u backupid -pw entR3v0Us -fd commands
   ```

   where:
   - -f specifies the file name to be used for the backup..
   - -pp specifies a quote-delimited passphrase
   - -u specifies a valid user ID for the SFTP server
   - -pw specifies the password corresponding to the user ID
   - -fd specifies the file name for the XML description of backup CLI commands

Additional information about the IMM backup process and the CLI command used to perform a backup is available in the *Integrated Management Module II User's Guide*:

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

2.4.2.3 Backing up operating system and user data

Use your own operating-system and user-data backup methods to back up the operating system and user data for the X-Architecture compute node.

Consider using a solution, such as IBM Tivoli® Storage Manager to back up operating system and user data for X-Architecture compute nodes. Most information about Tivoli Storage Manager is available at the following website:

www.ibm.com/software/products/us/en/tivostormana/

2.4.3 Backing up Power Systems compute nodes

When you back up the Power Systems™ compute nodes, create backups in phases.

2.4.3.1 Back up the Power Systems profile configuration

Create a backup of the profile data for all virtual servers using the IBM FSM Web interface. Profile data include all the virtual server profiles and virtual server definitions within the system.

When you perform a back up, it is written to the IBM FSM and then backed up as part of the FSM backup process.

1. From the Home page, click the **Chassis Manager** tab.
2. On the Chassis Manager tab, right-click the Power Systems compute node to be backed up and click **System Configuration**.
3. Click **Manage Virtual Server Data** and then click **Backup**
4. Choose a file name based on your backup file name guidelines and click **OK**.

2.4.3.2 Backing up VIOS

Backup up VIOS is essential to later recover defined virtual devices, such as disks and networks.

VIOS can be backed up using either the **backupios** or **viosbr** command.

2.4.3.2.1 Backing up Power Systems compute nodes using backupios:

The backupios command will backup all the information required to completely rebuild a VIOS server.

Make sure that you also back up the following components (these will be needed for the successful recovery of VIOS.

- External device configuration, such as SAN devices (V7000) and network switches.
- Resources defined on the IBM Flex System Manager® management software, such as processor and memory allocations.
- The operating systems and applications running in the client virtual servers.

These backups should be done via script in cron and the image should be backed up to an external device via TSM client on VIOS. Other backup options include backing up to DVDs or to a NIM server.

Additional information

For more information, see backupios command and Backing up the VIOS.

2.4.3.2.2 Backing up Power Systems compute nodes using viosbr:

The viosbr command backs up user defined virtual devices, which is useful for restoring information on the same VIOS from which is it is backed up

The backup will include the following:

- Logical devices, such as storage pools, clusters (VIOS Version 2.2.0.11, Fix Pack 24, Service Pack 1, or later), file-backed storage pools, the virtual media repository, and paging space devices.
- Virtual devices, such as Etherchannel, shared Ethernet adapter, virtual server adapters, and virtual Fibre Channel adapters.
- Device attributes for devices like disks, optical devices, tape devices, fscsi controllers, Ethernet adapters, Ethernet interfaces, and logical Host Ethernet Adapters.

Before you begin

Before you start, run the **isolevel** command to verify that the VIOS is at version 2.1.2.0, or later.

You can use following command from cron to create a backup of the configuration:

```
viosbr -backup -file /home/padmin/backup
```

The created backup file should be stored on external device using TSM, or DVD or NIM Sever.

Additional information

For more information, see viosbr command.

2.4.3.3 Backing up user data

Use your own operating-system and user-data backup methods to back up the operating system and user data for the Power Systems compute node.

Consider using a solution, such as IBM Tivoli Storage Manager to back up operating system and user data for Power Systems compute nodes. Most information about Tivoli Storage Manager is available at the following website:

www.ibm.com/software/products/us/en/tivostormana/

2.4.4 Backing up the IBM Flex System V7000 storage node

The same procedures apply for backing up the Storwize® V7000 and the V7000 storage node.

It is recommended that a backup be performed after any significant changes in configuration have been made to the system.

Note: The system automatically creates a backup of the configuration data each day at 1 a.m. This is known as a cron backup and is written to `/dumps/svc.config.cron.xml_serial#` on the configuration node.

A manual backup can be generated at any time using the instructions in this procedure. If a severe failure occurs, both the configuration of the system and application data may be lost. The backup of the configuration data can be used to restore the system configuration to the exact state it was in before the failure.

In some cases, it may be possible to automatically recover the application data. This can be attempted via the <Recover System Procedure>, also known as a Tier 3 (T3) procedure. Restoring the system configuration without attempting to recover the application data is performed via the <Restoring the System Configuration> procedure, also known as a Tier 4 (T4) recovery. Both of these procedures require a recent backup of the configuration data.

Backup of the V7000 is similar to the switch backups—one command is used to back up and another to restore.

It is recommended that you keep the automatic backup that runs each day in order to provide an extra measure of protection.

This file has a separate (but similar) naming format as the user or automation triggered backups, so there should be little confusion around this.

Follow these steps to perform the backup procedure.

1. **`svcconfig backup`**
2. Review backups in `/dumps` on your V7000 configuration node canister. There should have been three files created by the previous command. They all start with `svc.config.backup` and end with `.sh_serial#`, `.xml_serial#`, and "`.log_serial#`. The XML file is the configration backup. The log file includes any warnings and messages and the .sh file contains the commands issued to generate the backup. You may notice another configuration backup file with the name `cron` in it. That is the nightly backup that is taken automatically.
3. Transfer the backup data to backup location described at the start of this document using scp, as follows from the V7000 CLI: **`pscp superuser@cluster_ip :/dumps/svc.config.backup.* /FSM_IP/MyBackupUserDirectory`**

2.4.5 Backing up I/O modules

The topics in this section provide information on how to back up I/O modules.

2.4.5.1 Backing up SAN switches

Each supplier has a different procedure used to back up SAN switches.

To back up a SAN switch, use the direct switch interface to copy the configuration file from the switch to another location.

2.4.5.2 Backing up Ethernet switches

Each supplier has a different procedure used to back up Ethernet switches.

To back up an Ethernet switch, use the direct switch interface to copy the configuration file from the switch to another location.

2.5 Backing up top-of-rack switches

The network switches in the IBM PureFlex are BNT® (BladeNetwork Technologies, an IBM Company) brand switches.

Models 8052 and G8264 both use the same operating system, so they can be backed up the same way.

Before you begin, decide whether you plan to hardcode the switch user and password in a very simple script or to set up SSH Authentication Keys for use with your simple script.

SSH Keys are the recommended method, but you may also script using the password and username. The examples below assume that you are using the SSH key with Default Name for Authentication. The following steps assume that you have created a short shell script to redirect the data into a flat file (plain text.) The contents of the file should look something like this:

```
#!/usr/bin/ksh
ssh admin@hostname.or.ip.address  terminal 0;enable;copy running-config backup-config;show backup-config >  admin@h
ssh admin@hostname.or.ip.address terminal 0;show version > hostname.or.ip.address.ver
```

1. Create a Script to redirect the data and place it in the OS (sample above) as text files.
   a. SSH into the switch
   b. Set the terminal length to unlimited (0)
   c. Enable EXEC/Privileged Mode
   d. Copy the Running Configuration to the Backup Configuration
   e. Show the Backup Configuration; the redirection shown in the sample script above will save the output of the show Backup Configuration.
   f. SSH into the switch
   g. Set your terminal length to unlimited (0)
   h. Show the version; the redirection shown in the sample script above will save the output of the show version.

As shown in the sample script, it is recommended that you save the version information, as it is useful in the event of failure.

Chapter 3. Restoring the IBM FSM

This section contains procedures for restoring numerous parts of the IBM Flex and IBM PureFlex systems.

3.1 Restoring and version compatibility

Make sure that you understand the version restrictions for backup images before you restore a backup image.

In most situations that require you to restore a backup of the IBM® Flex System Manager management software, make sure that the management software version in the backup file matches the management software version that you use to restore the backup. The following guidelines show the compatible backups for each management software version.

- With version 1.3.0, you can restore only a backup of version 1.3.0 or version 1.2.1
- With version 1.2.1, you can restore only a backup of version 1.2.1
- With version 1.2.0, you can restore only a backup of version 1.2.0
- With version 1.1.1, you can restore only a backup of version 1.1.1
- With version 1.1.0, you can restore only a backup of version 1.1.0

You cannot restore a backup image from management software version 1.1.1 or earlier on an IBM Flex System Manager management node with management software version 1.2.0 installed. If you must restore an image from version 1.1.1 or earlier, use the IBM Flex System Manager management software Recovery DVDs for the management software version that you want to restore. For more information about using the Recovery DVDs, see the information in Management software recovery and reinstallation.

If you want to restore from a backup image that is stored locally on the management node hard disk drive, make sure that you use the Recovery DVDs for version 1.1.1 and not version 1.1.0. A problem with version 1.1.0 requires that you noted the local backup image name before performing the recovery. With version 1.1.1, you can use the command-line interface (CLI) to list the local backups; then, you can restore the local backup from the CLI. For more information about restoring an earlier version of the management software, see Restoring an earlier version of the management software image.

3.2 Restoring the management software image

You can restore an IBM® Flex System Manager management software image from a backup that is stored on the management node hard disk drive, USB drive, or a secure FTP server (SFTP).

Important: Recovery from the DVDs is a last resort, to be used only if the service partition does not hold the original image. In normal scenarios, the service partition contains the factory image. The only exception is if you have consciously ordered the recovery DVDs and manually updated the service partition. This is not normally recommended.

Preparing to restore a backup image

You cannot restore a backup image from management software version 1.1.1 or earlier on an IBM Flex System Manager management node with management software version 1.2.0 installed. If you must restore an image from version 1.1.1 or earlier, use the IBM Flex System Manager management software Recovery DVDs for the management software version that you want to restore.

Before you restore a backup image, make sure that you understand the following conditions.

Configuring the management software after you restore a backup image

After a restore operation is complete, collect inventory for all of the managed resources in your IBM Flex System environment.

If you restored a backup that was taken from an earlier version of the management software, update the management software to the same version as before the restore operation.

Important: If you do not update the management software in this situation, the management software version might be older than other components in your environment, which might cause compatibility problems.

If any managed resources were removed from management after a backup was created, and you restore that backup image, the endpoints for the deleted resources will reappear in the management software. You must delete the endpoints manually to remove them.

Similarly, any managed resources that were discovered after a backup image was created must be re-discovered after that backup is restored.

If a chassis was managed in centralized user management mode, and you restore a backup image that was created before centralized user management mode was enabled, you might have to use the RECOVERY_ID account to re-manage the chassis. For more information, see Recovering chassis management with a CMM after a management node failure.

Further information

For detailed instructions on how to restore backups from supported sources, see the information center. The information center provides procedures for:

- Restoring a management software image from the hard disk drive
- Restoring a management software image from a USB drive
- Restoring the management software image from a secure FTP server
- Restoring an earlier version of the management software image

3.3 Restoring chassis components

The topics in this section provide procedures for restoring chassis components.

3.3.1 Restoring the Chassis Management Module (CMM)

The CMM can be restored through the CMM web interface, or it can be restored using the command-line interface (CLI) of the CMM.

3.3.1.1 Restoring the CMM through the GUI

Use the CMM's native interface to restore the CMM through the GUI.

See Restoring a CMM configuration for the steps in the procedure.

3.3.1.2 Restoring the CMM through the CLI

Use the CMM CLI read command to restore a CMM configuration through the CMM CLI.

Note: By default, the CMM operates in secure mode. When the CMM is set to secure, only the secure file transfer methods HTTPS and SFTP can be used for firmware updates and other tasks involving file transfers, such as transferring a backup configuration file to restore a configuration. The unsecure file transfer protocols HTTP, FTP, and TFTP are disabled.

Assume that you have set up an SFTP server as follows:

- IP adress: 191.168.1.101
- User ID: userid
- Password: xxxxxxxx
- Encryption Passphrase: b@ckupN0w (zero, not an uppercase o)
- Backup file: /home/userid/backup/cmmp.bkp

Also assume that you previously created a backup using the procedure in 2.4.1.2, “Back up the CMM through the CLI,” on page 15

You are restoring the backup to the primary CMM.

Complete the following steps to restore the CMM configuration.

1. Using a secure protocol, such as SSH, log in to the CMM CLI interface using a user ID that has Supervisor or Chassis Configuration authority.
2. At the system> prompt, enter the following command:

   ```
   read -u sftp://userid:xxxxxxxx@192.168.1.101/home/userid/backup/cmmp.bkp -p "b@ckupN0w" -v
   ```

   where:

   - -u specifies the remote location to which the file will be written.

     Note: You must enter the full destination path for the SFTP server in the URL that you provide.
   - -p specifies a quote-delimited passphrase (between 6 and 31 characters)

   If successful, the system responds with:

   ```
   OK

   Configuration restore was successful

   Restart the MM for the new settings to take effect
   ```

Restart the CMM to apply the settings.

To restart the CMM from the CLI, enter the following command:

```
reset -o
```

You will lose connectivity through the SSH while the CMM is being restarted.

Additional information about the CMM restoration process and the CLI command used to restore a CMM configuration from a backup:

- Restoring a CMM Configuration

  http://publib.boulder.ibm.com/infocenter/flexsys/information/index.jsp?topic=%2Fcom.ibm.acc.cmm.doc%2Frestore_saved_config_cmm.html
- **read** command

  http://publib.boulder.ibm.com/infocenter/flexsys/information/index.jsp?topic=%2Fcom.ibm.acc.cmm.doc%2Fcli_command_read.html

3.3.2 Restoring X-Architecture compute nodes

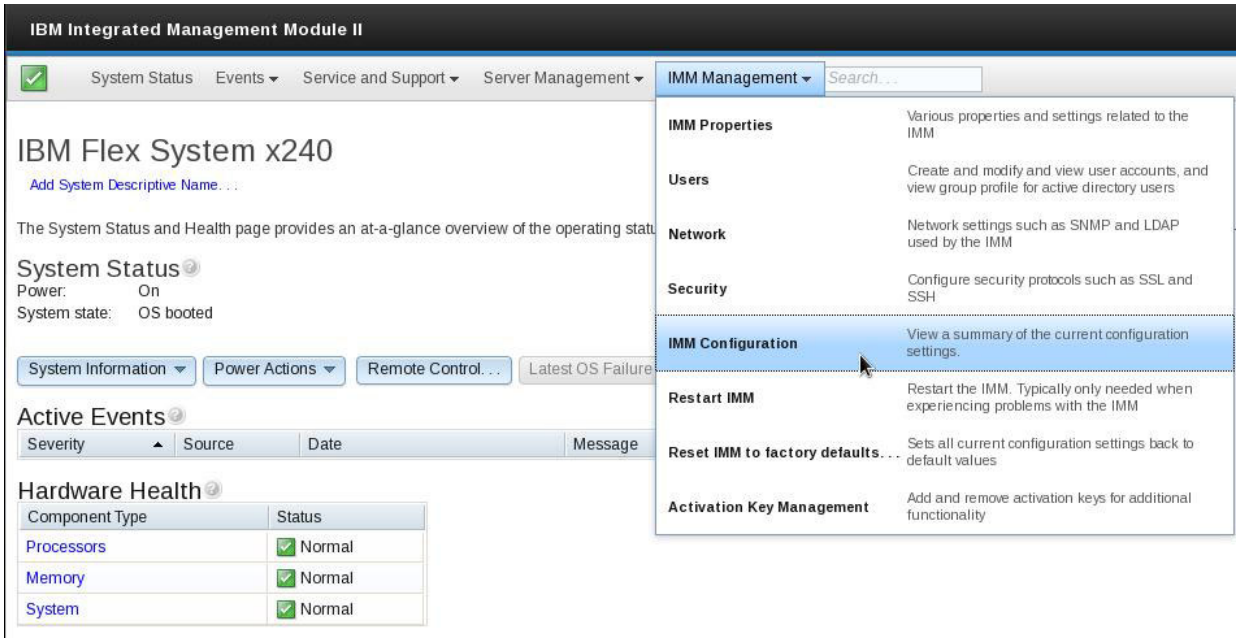
To restore the service processor (IMM) for X-Architecture compute nodes, use either the IMM graphical user interface or the command-line interface. To restore operating system and user data, use standard restore procedures.

3.3.2.1 Restoring the IMM through the graphical user interface

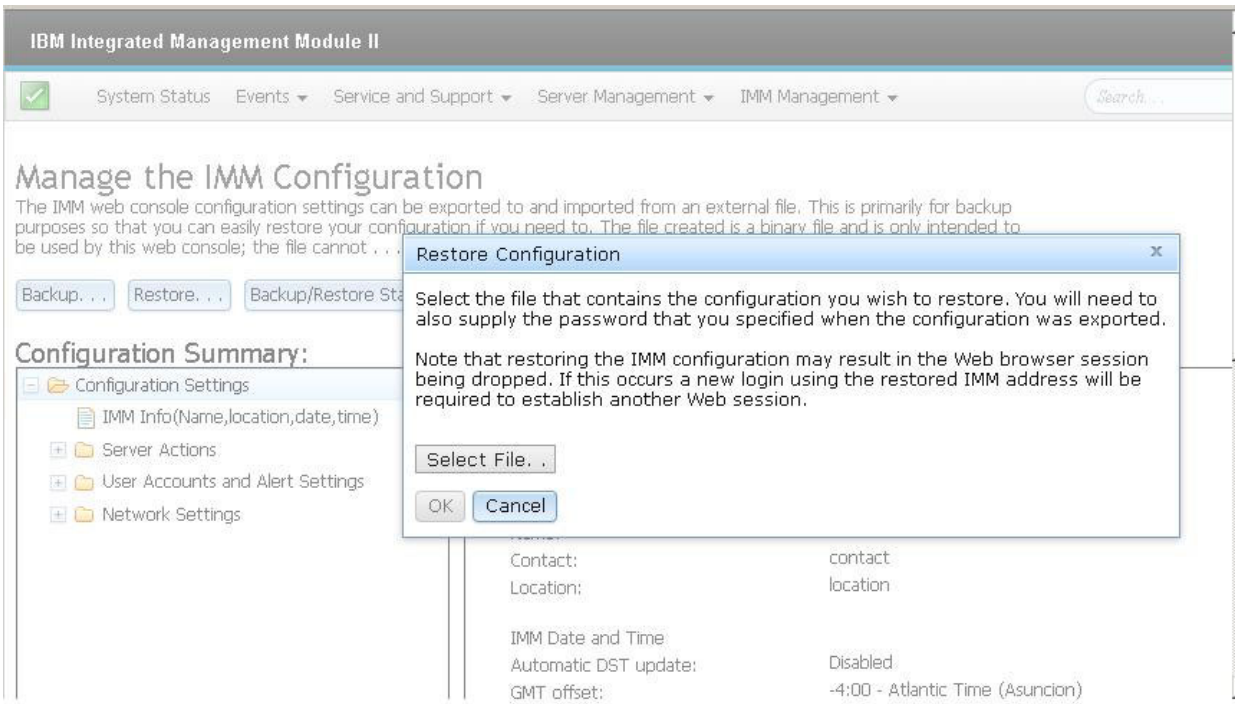
Follow this procedure to restore the IMM through the graphical user interface.

Complete the following steps to restore the IMM for an X-Architecture compute node:

1. From a Web browser, log in to the IMM graphical user interface for the X-Architecture compute node.
2. From the user interface, click **IMM Management** > **IMM Configuration**.

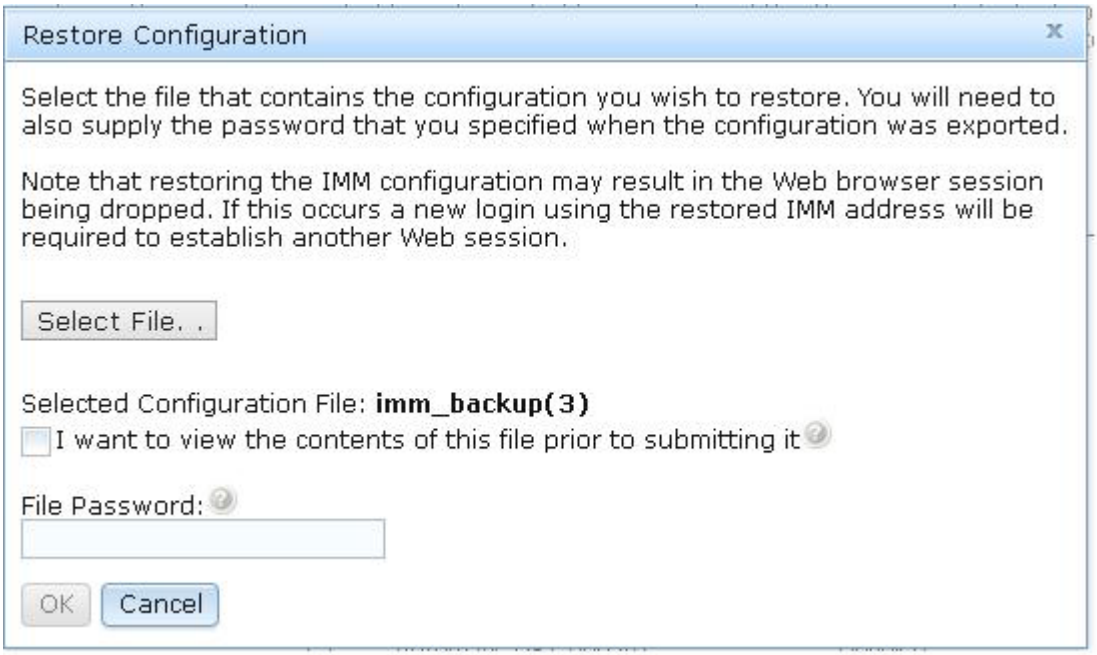


3. From the Manage the IMM Configuration panel, click **Restore**.
4. Click **Select File** to choose the location where the backup file resides.



After selecting the file, click **OK**.

5. Enter the Passphrase that you used when creating the backup in the File Password field (b@ckupN0w).



After entering the passphrase, click **OK** and the Restoring IMM Configuration window shows you the progress being made during the restore process.

When the restore process has completed, the status is displayed. After viewing the status to ensure the restore process was successful, click **Close**.

Repeat this process to restore the IMM configuration for any other X-Architecture compute nodes.

3.3.2.2 Restoring the IMM through the CLI

Follow this procedure to restore the IMM through the command line interface.

Assume that you have set up an SFTP server as follows:

- IP address: 191.168.1.101
- User ID: backupid
- Password: entR3v0Us
- Encryption Passphrase: b@ckupN0w (zero, not an uppercase o)
- Backup directory: /home/userid/backup

Complete the following steps to restore the IMM configuration.

1. Using a secure protocol, such as SSH, log in to the IMM CLI interface.
2. At the system prompt, enter the following command:

   ```
   restore -f imm_backup -pp "b@ckupN0w" -ip 192.168.1.101 -u backupid -pw entR3v0Us
   ```

   where:

   - -f specifies the file name used for the backup.
   - -pp specifies a quote-delimited passphrase
   - -ip is the IP address for the SFTP server where the backup file is located.
   - -u specifies a valid user ID for the SFTP server
   - -pw specifies the password corresponding to the user ID

Additional information about the IMM restore process and the CLI command used to perform a restore is available in the *Integrated Management Module II User's Guide*:

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

3.3.2.3 Restoring operating system and user data

Use your own operating-system and user-data restore methods to restore the operating system and user data for the X-Architecture compute node.

3.3.3 Restoring Power Systems compute nodes

A number of checks must be performed before restoring Power Systems compute nodes.

Before you begin

Make sure that you have recovered the following components before you recover Power Systems compute nodes:

- FSM
- Switches
- CMM
- V7000

In order to recover a Power ITE in case of disaster, backups must be performed at multiple layers. Before recovering the compute node, the FSM must be recovered and fully functional. Recovery of switches, CIMM, V7000, and FSM are prerequisites for compute node recovery. To ensure you have a capability to recover a POWER ITE, all backups must be performed on a regular basis.

3.3.3.1 Restoring the Power Systems profile configuration

The Chassis Manager tab is used to restore the Power Systems profile configuration.

1. From the Home page, click the **Chassis Manager** tab.
2. On the Chassis Manager tab, right-click the Power Systems compute node to be restored and click **System Configuration**.
3. Click **Manage Virtual Server Data** and then click **Restore**
4. Choose a file name to be restored and choose the appropriate restore option.

   There are 3 options to choose from:

   - **Full restore**.

     The full restore option restores all profile data using your backup file only. Profile modifications performed after the selected backup file was created will be lost.
   - **Backup priority**.

     The backup priority option merges the stored backup file with recent profile activity, but the backup information takes precedence. If information conflicts, the stored backup data is restored over the recent profile activity.
   - **Host priority**.

     The host priority option merges recent profile activity with the stored backup file, but the recent profile activity takes preference. If information conflicts, the recent profile activity is restored over the stored backup data.
5. Click **OK** to start the restore process.

3.3.3.2 Restoring VIOS

Depending on the backup taken using backupios, the restore procedure varies.

- If the backup was creating using the NIM server nimresources.tar, the restore can be completed using the following command:

  ```
  installios
  ```

  Note: Run the **smcli lsbundle** command to obtain a list of valid commands.
- If backup is done via mksysb image to NIM defined NIM resource and restore the mksysb image.

  Note: Before restoring VIOS, ensure that the data from external devices are restore and available. Ex: SAN, Network

3.3.3.3 Restoring operating system and user data

Use your own operating-system and user-data restore methods to restore the operating system and user data for the X-Architecture compute node.

3.3.4 Restoring the IBM Flex System V7000 storage node

The same procedures apply for restoring the Storwize V7000 and the V7000 storage node.

Before you restore the IBM Flex System V7000 storage node, ensure that you read the topics in this section thoroughly.

Before you start, be aware of the following:

- The default object names for controllers, I/O groups, and managed disks (MDisks) do not restore correctly if the ID of the object is different from what is recorded in the current configuration data file.
- All other objects with default names are renamed during the restore process. The new names appear in the format *name*_r, where *name* is the name of the object in your system.

Before you restore your configuration data, the following prerequisites must be met:

- The Security Administrator role is associated with your user name and password.
- A copy of your backup configuration files are available on a server that is accessible to the system.
- A backup copy of your application data is accessible and ready to load on your system after the restore configuration operation is complete.
- You must know the current license settings for your system.
- No hardware can have been removed since the last backup of your configuration.
- No zoning changes were made on the Fibre Channel fabric that would prevent communication between the Storwize V7000 and any storage controllers that are present in the configuration.
- For configurations with more than one I/O group, if a new system is created on which the configuration data is to be restored, the I/O groups for the other control enclosures must be added.

3.3.4.1 Determining how to achieve an ideal T4 recovery

Before you attempt to restore the IBM Flex System V7000 storage node, determine the ideal method for the restoration.

1. Open the appropriate `svc.config.backup.xml` (or `svc.config.cron.xml`) file with a suitable text editor or browser.
2. Navigate to the node section of the file.
3. For each node entry, make a note of the value of following properties; IO_group_id, canister_id, enclosure_serial_number.
4. Use the CLI **`sainfo lsservicenodes`** command and the data to determine which node canisters previously belonged in each IO group.

Restoring the system configuration must be performed via one of the nodes previously in IO group zero. For example, property name="IO_group_id" value="0" . The remaining enclosures must be added, as required, in the appropriate order based on the previous IO_group_id of the node canisters.

Note: It is not possible to determine which canister within the identified enclosure was previously used for cluster creation. Typically, the restoration should be performed via canister 1.

The Storwize V7000 analyzes the backup configuration data file and the system to verify that the required disk controller system nodes are available. Use this procedure only in the following situations:

- If the recover procedure has failed
- If the data that is stored on the volumes is not required

This configuration restore procedure is designed to restore information about your configuration, such as volumes, local Metro Mirror information, local Global Mirror information, storage pools, and nodes. All data that you have written to the volumes is not restored. To restore the data on the volumes, you must restore application data from any application that uses the volumes on the clustered system as storage separately. Therefore, you must have a backup of this data before you follow the configuration recovery process.

You must reinstate the system to the exact state it was in before the failure, and then recover the application data.

Important: There are two phases during the restore process: prepare and execute. You must not change the fabric or system between these two phases. If you do not understand the instructions to run the CLI commands, see the command-line interface reference information.

3.3.4.2 Restoring configuration data

After you have read the prerequisites, perform these steps to restore configuration data.

Important: Ensure that you have read the prerequisite information in 3.3.4, "Restoring the IBM Flex System V7000 storage node," on page 30 and 3.3.4.1, "Determining how to achieve an ideal T4 recovery," on page 31 before you perform this procedure.

1. Verify that all nodes are available as candidate nodes before you run this recovery procedure. You must remove errors 550 or 578 to put the node in candidate state. For all nodes that display these errors, perform the following steps:
   a. Point your browser to the service IP address of one of the nodes, for example, `https://node_service_ip_address/service/`.
   b. Log on to the service assistant.
   c. From the Home page, put the node into service state if it is not already in that state.
   d. Select **Manage System**.
   e. Click **Remove System Data**.
   f. Confirm that you want to remove the system data when prompted.
   g. Exit service state from the Home page. The 550 or 578 errors are removed, and the node appears as a candidate node.
   h. Remove the system data for the other nodes that display a 550 or a 578 error. All nodes previously in this system must have a node status of Candidate and have no errors listed against them.

      Note: A node that is powered off might not show up in this list of nodes for the system. Diagnose hardware problems directly on the node using the service assistant IP address and by physically verifying the LEDs for the hardware components.
2. Verify that all nodes are available as candidate nodes with blank system fields. Perform the following steps on one node in each control enclosure:
   a. Connect to the service assistant on either of the nodes in the control enclosure.
   b. Select **Configure Enclosure**.
   c. Select the **Reset the system ID** option. Do not make any other changes on the panel.
   d. Click **Modify** to make the changes.
3. Use the initialization tool that is available on the USB flash drive to a create a new Storwize® V7000 system. Select the **Initialize a new Storwize V7000 (block system only)** option from the Welcome panel of the initialization tool.
4. In a supported browser, enter the IP address that you used to initialize the system and the default superuser password (`passw0rd`).
5. At this point the setup wizard is shown. Complete these steps:
   a. Accept the license agreements.
   b. Set the values for the system name, date and time settings, and the system licensing. The original settings are restored during the configuration restore process.
   c. Verify the hardware. Only the control enclosure on which the clustered system was created and directly attached expansion enclosures are displayed. Any other control enclosures and expansion enclosures in other I/O groups will be added to the system.
   d. On the Configure Storage panel, clear the **Yes automatically configure internal storage now** option. Any internal storage configuration is recovered after the system is restored.
6. Optional: From the management GUI, click **Access** > **Users** and configure an SSH key for the superuser.
7. By default, the newly initialized system is created in the storage layer. The layer of the system is not restored automatically from the configuration backup XML file, so if the system you are restoring

was previously configured in the replication layer, you must change the layer manually now. For more information, refer to Metro Mirror and Global Mirror partnerships.

8. For configurations with more than one I/O group add the rest of the control enclosures into the clustered system.
   a. From the management GUI, select **Monitoring** > **System Details**.
   b. Select the system name in the tree.
   c. Go to **Actions** > **Add Enclosures** > **Control and Expansions**.
   d. Continue to follow the on-screen instructions to add the control enclosures. Decline the offer to configure storage for the new enclosures when asked if you want to do so.
9. Identify the configuration backup file from which you want to restore. The file can be either a local copy of the configuration backup XML file that you saved when backing up the configuration or an up-to-date file on one of the nodes. Configuration data is automatically backed up daily at 01:00 system time on the configuration node. Download and check the configuration backup files on all nodes that were previously in the system to identify the one containing the most recent complete backup. For each node in the system:
   a. From the management GUI, click **Settings** > **Support**.
   b. Click **Show full log listing**.
   c. Select the node to operate on from the selection box at the top of the table.
   d. Find the file name that begins with `svc.config.cron.xml`.
   e. Double-click the file to download the file to your computer. The XML files contain a date and time that can be used to identify the most recent backup. After you identify the backup XML file that is to be used when you restore the system, rename the file to `svc.config.backup.xml`.
10. Issue the following CLI command to remove all of the existing backup and restore configuration files that are located on your configuration node in the `/tmp` directory: **svcconfig clear -all**
11. Copy the XML backup file that you wish to restore from back onto the system. **pscp full_path_to_identified_svc.config.backup.xml superuser@cluster_ip:/tmp/**
12. Issue the following CLI command to compare the current configuration with the backup configuration data file: **svcconfig restore -prepare** This CLI command creates a log file in the `/tmp` directory of the configuration node. The name of the log file is `svc.config.restore.prepare.log`

    Note: It can take up to a minute for each 256-MDisk batch to be discovered. If you receive error message `CMMVC6200W` for an MDisk after you enter this command, all of the managed disks (MDisks) might not have been discovered yet. Allow a suitable time to elapse and try the **svcconfig restore -prepare** command again.
13. Issue the following command to copy the log file to another server that is accessible to the system: **pscp superuser@cluster_ip:/tmp/svc.config.restore.prepare.log full_path_for_where_to_copy_log_files**
14. Open the log file from the server where the copy is now stored.
15. Check the log file for errors.
    - If there are errors, correct the condition that caused the errors and reissue the command. You must correct all errors before you can proceed to the next step.
    - If an error indicates that the system layer will not be restored, then return to step 7, configure the layer setting correctly, and then continue the restore process from step 10.
    - If you need assistance, contact the IBM® Support Center.
16. Issue the following CLI command to restore the configuration: **svcconfig restore -execute** This CLI command creates a log file in the `/tmp` directory of the configuration node. The name of the log file is `svc.config.restore.execute.log`.
17. Issue the following command to copy the log file to another server that is accessible to the system: **pscp superuser@cluster_ip:/tmp/svc.config.restore.execute.log full_path_for_where_to_copy_log_files**

18. Open the log file from the server where the copy is now stored.
19. Check the log file to ensure that no errors or warnings have occurred.

    Note: You might receive a warning stating that a licensed feature is not enabled. This message means that after the recovery process, the current license settings do not match the previous license settings. The recovery process continues normally and you can enter the correct license settings in the management GUI at a later time. When you log into the CLI again over SSH, you see this output: `IBM_2076:your_cluster_name:superuser`
20. After the configuration is restored, verify that the quorum disks are restored to the MDisks that you want by using the **lsquorum** command. To restore the quorum disks to the correct MDisks, issue the appropriate **chquorum** CLI commands.

You can remove any unwanted configuration backup and restore files from the `/tmp` directory on your configuration by issuing the following CLI command: **svcconfig clear -all**.

3.3.5 Restoring I/O modules

The topics in this section provide information on how to restore I/O modules.

3.3.5.1 Restoring SAN switches

Each supplier has a different procedure used to restore SAN switches.

To restore a SAN switch, use the direct switch interface to copy the configuration file from its backup location to the switch.

Restore FC3171 SAN switch (QLogic)

User credentials are not stored in the backup file. Users must reconfigure it after restore.

Restore FC5022 SAN switch (Brocade)

Restore configuration is as follows:

```
User Name [user]: root
Path/Filename [<home dir>/config.txt]: /home/brocade_35_new.txt
Section (all|chassis|switch [all]): all

                        *** CAUTION ***

  This command is used to download a backed-up configuration
  for a specific switch.  If using a file  from a  different
  switch, this file's configuration  settings will  override
  any current switch settings.   Downloading a configuration
  file, which was uploaded  from a different type of switch,
  may cause this switch to fail.  A switch reboot might be
  required for some parameter changes to take effect.

  configDownload operation may take several minutes
  to complete for large files.

  Do you want to continue [y/n]: y
root@9.27.18.173's password:
duplicate license-key "XXJAmWLM4YtZKCWAE7Fr3gFNmP7RmXaWB7ZJJ"
duplicate license-key "ZaFJG3ZYYT94CZf73MY4EKKtaDLN4aABB7PFK"

Doing configDownload on switch ...

Activating configDownload: Switch is disabled


configDownload complete: All selected config parameters are downloaded
FC5022:USERID> switchenable
```

3.3.5.2 Restoring Ethernet switches

Each supplier has a different procedure used to restore Ethernet switches.

To restore an Ethernet switch, use the direct switch interface to copy the configuration file from its backup location to the switch.

Restoring Ethernet chassis switch (EN4093)

The switch must be in the same CLI mode (IBMNOS/ISCLI/prompted) for backup and restore. Otherwise, the restore will fail.

Note: If EN4093 is configured in ISCLI mode, the deployment of EVB profile via FSM will fail. The deployment only works with IBMNOS or prompted mode.

```
Router(config)#copy tftp running-config mgt-port
Address or name of remote host: 9.27.18.173
Source file name: config_9.27.20.32_14Aug2013_175459.txt
Start transfer ......................
Loading to current configuration.
.
Apply to current configuration.
Successfully downloaded config_9.27.20.32_14Aug2013_175459.txt from 9.27.18.173.

Router(config)#copy running-config startup-config
Confirm saving to FLASH (y/n) ? y
Copy running configuration to startup configuration
Switch is currently set to use factory default config block on next boot.
Do you want to change that to the active config block (y/n) ?
Aug 14 15:23:34 9.27.20.32 INFO    mgmt: new configuration saved from ISCLI
y
Next boot will use active config block.

Aug 14 15:23:38 9.27.20.32 NOTICE  mgmt: boot config block changed
```

3.4 Restoring up top-of-rack switches

To restore simply copy and paste the configuration commands.

Important: In order for the commands to paste accurately, you must default the switch to factory settings and perform the copy and paste action from there.

The copy and paste of the configuration commands will work in all environments.

Chapter 4. Performing manual failover

It is possible to use the backup and restore feature of the IBM Flex System Manager management node to perform a manual failover process in the event that a Flex System Manager is damaged or lost. This document outlines the process for performing a manual failover using a new Flex System Manager node to replace the lost or damaged one.

4.1 Create backups of the primary node

In order to manually fail over an IBM Flex System Manager management node, you will need backup images of the primary Flex System Manager. This section describes how to create these backups on a working Flex System Manager.

For maximum utility, backup images that might be used for failover recovery should be stored externally on a USB drive or SFTP server, rather than on the hard disk drive of the primary Flex System Manager.

4.1.1 Backing up and restoring the management software

Use the IBM Flex System Manager management software to back up or restore your software image.

On the Backup and Restore page in the management software web interface, you can initiate a backup of the management software image, schedule future backups of the management software image, and restore a management software image.

Important: The backup file that is created through the management software backup task is unencrypted, and contains unsecured data that is otherwise restricted in an IBM Flex System and IBM PureFlex System environment. Use your own method to protect the backup file.

A backup of the management software includes the following data:

- The management software image
- The local IBM Flex System Manager user registry
- IBM Flex System Manager configuration settings (including network settings)
- Discovered endpoints and inventory
- Configuration pattern data

Note: When you initiate a backup, the management software checks for jobs that are active and in process. If one or more jobs are running when you initiate the backup, the backup will not proceed.

4.1.1.1 Backing up the management software image

You can back up the IBM Flex System Manager management software image to the management node hard disk drive, a USB drive, or a secure FTP server. The backup image is a full backup, and includes all applied fixes, data on managed chassis, and any custom settings.

A backup of the management software includes the following data:

- The management software image
- The local IBM Flex System Manager user registry
- IBM Flex System Manager configuration settings (including network settings)
- Discovered endpoints and inventory
- Configuration pattern data

Important: The backup file that is created through the management software backup task is unencrypted, and contains unsecured data that is otherwise restricted in an IBM Flex System and IBM PureFlex System environment. Use your own method to protect the backup file.

Choosing a location for management software backups

Attention: The option to back up the management software to the local hard disk drive is selected by default in the web interface. However, a backup that is stored on the local drive is useless if that drive fails. To protect your backup from a disk failure, make sure that you back up to a secure FTP (SFTP) server or USB drive.

Important: 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.

To create a backup that is available in a disaster recovery situation, backup the management software to an SFTP server in a remote location or to a USB drive that will be stored in a remote location. It is recommended that you schedule your backups to an SFTP server on a regular basis for use in a manual failover scenario.

The local hard disk drive in the IBM Flex System Manager management node has a limited amount of available space for storing backups. Typically, the local hard drive has space for only three backups. USB drives have similar space constraints. An SFTP server, which potentially has more backup storage space, might be the best backup location for your management software backup images.

Choosing when to back up the management software

Back up the management software often. For a typical IBM Flex System and IBM PureFlex System environment, you might want to backup the management software once or twice weekly. You can schedule backups so that the backup image is created and saved automatically; see 4.1.1.1.3, “Scheduling management software image backups,” on page 40 for more information.

Note: You can schedule only one backup at a time.

In addition to regular and scheduled backups, back up the management software in the following situations:

- After multiple new managed resources are discovered or removed.
- After multiple new virtual machines are deployed or removed.
- After a management software policy change (for example, the security policy or password rules policy).
- Before and after every management software update or upgrade.
- After an IP configuration change or other network configuration change.
- After user accounts are created, deleted, or modified (for example, after user passwords expire or reset).
- After user credentials or permissions are modified.
- After you have created, modified, or deployed configuration patterns.
- After obtaining new updates for managed resources, even it the updates are not yet deployed.

See 4.3.2, “Restoring the management software image,” on page 44 for information about how to restore the management software image.

4.1.1.1.1 Backing up the management software image to a USB drive:

Use this information to back up the IBM Flex System Manager management software image to a USB drive. The backup image includes all applied fixes, data on managed chassis, and any custom settings.

You can back up the management software image to a USB drive by using either the Backup and Restore page in the web interface or the command-line interface (CLI). For more information about backing up the software to a secure FTP server or the management node hard disk drive, see 4.1.1.1.2, “Backing up the management software image to a secure FTP server” or Backing up the management software image to the hard disk drive.

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

Before you initiate a management software backup to a USB drive, be aware of the following conditions:

- The only supported USB file system formats are FAT32, ext3, and ext4.
- If you use the management software web interface to back up the management software image, the USB drive is mounted automatically as part of the backup process.

  See 4.1.1.1.3, “Scheduling management software image backups,” on page 40 for more information about scheduling a management software backup.
- Some USB drives might not be recognized when they are first mounted. If you remove and reinsert the USB drive, it should then be recognized.
- If you back up to a USB device that does not support a minimum write speed of 5 MBps, the management software pauses for several minutes, and the management node is inoperable.

To back up the management software image to a USB drive with the management software web interface, complete the following steps:

1. From the Home page, click the **Administration** tab.
2. On the Administration tab under Serviceability tasks, click **Backup and Restore**. The Backup and Restore page opens.
3. From the Backup and Restore page, click **Backup Now**. The Backup Now window opens.
4. Select **USB device**; then, click **OK**.

To back up the management software image to a USB drive with the **backup** command in the management software CLI, complete the following steps.

Important: A backup that is created with the **backup** command (whether on an SFTP server or a USB device) does not appear in the list that is generated when you run the **listBackups** command, or in the Recent Backups table on the Backup and Restore page in the management software web interface.

1. Insert a USB device into the USB port on the management node. The USB device is mounted automatically.
2. Open a CLI prompt.
3. Use the **backup -l usb** command to back up the software image to the USB drive. A file named *yyyymmddhhmmss*.tar.gz (where *yyyymmddhhmmss* is the year, month, day, hour, minute, and second the file was created) is saved on the USB drive.

See 4.3.2.2, “Restoring a management software image from a USB drive,” on page 45 for information about how to restore the management software image from a USB drive.

4.1.1.1.2 Backing up the management software image to a secure FTP server:

Use this information to back up the IBM Flex System Manager management software image to a secure FTP (SFTP) server that has Secure Shell (SSH). The backup image includes all applied fixes, data on managed chassis, and any custom settings.

You can back up the management software image to an SFTP server by using either the Backup and Restore page in the web interface or the command-line interface (CLI).

Important: 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.
For more information about backing up the software to a USB drive or the management node hard disk drive, see 4.1.1.1.1, “Backing up the management software image to a USB drive,” on page 38 or Backing up the management software image to the hard disk drive.

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

To back up the management software image to an SFTP server with the management software web interface, complete the following steps:

1. From the Home page, click the **Administration** tab.
2. On the Administration tab under Serviceability tasks, click **Backup and Restore**. The Backup and Restore page opens.
3. From the Backup and Restore page, click **Backup Now**. The Backup Now window opens.
4. Select **SFTP Server**.
5. Type the SFTP filepath, user name, and password; then, click **OK**.

   Note: Please note that the following characters cannot be used in the directory paths for SFTP backups created using the web interface: '_', '#', '$', and '*'.

To back up the management software image with the **backup** command in the management software CLI, complete the following steps.

Important: A backup that is created with the **backup** command does not appear in the Recent Backups table on the Backup and Restore page in the management software web interface.

1. Open a CLI prompt.
2. Use the **backup** command with the SFTP server name, path, user name, and password (see the following example) to back up the software image to SFTP:

   ```
   backup -l sftp -s [sftp server name] -d [path on sftp server]
    -u [sftp user name] -p [sftp_password]
   ```

   A file named *yyyymmddhhmmss*.tar.gz(where *yyyymmddhhmmss* is the year, month, day, hour, minute, and second the file was created) is saved on the SFTP server.

See 4.3.2.3, “Restoring the management software image from a secure FTP server,” on page 46 for information about how to restore the management software image from an SFTP server.

4.1.1.1.3 Scheduling management software image backups:

Schedule regular backups of your IBM Flex System Manager management software image to ensure that you have a working software image in the event of system failure.

Note:

1. You can schedule only one backup at a time.
2. If you are planning for a manual failover scenario, it is recommended that you schedule your backups to a secure FTP server.

To schedule backups of the management software image to the management node hard disk drive, a USB device, or a secure FTP server with the management software web interface, complete the following steps:

1. On the Home page, click the **Administration** tab.
2. Under Serviceability Tasks, click **Backup and Restore**. The Backup and Restore page opens.

3. Click **Schedule backups**. The Backup Scheduler wizard opens.
4. Complete the steps in the Backup Scheduler wizard.

The Backup Scheduler wizard offers the following backup options:

- Scheduled backups:
  - Disable scheduled backups
  - Enable scheduled backups to a USB device
  - Enable scheduled backups to a secure FTP server
- Frequency:
  - Start date
  - Time of day
  - Repeat options: weekly, monthly, or yearly
  - Duration: for a particular period, until a particular date, or for an unlimited amount of time

4.2 Perform initial setup on the secondary node

In order to restore an existing backup image to a new, or secondary, IBM Flex System Manager node, you must perform initial setup on the secondary node. To do this, complete the Management server setup wizard, as described here.

When you have completed the setup wizard, ensure that the secondary Flex System Manager is using the same release and fix levels as the original node. You can find instructions for updating the code and fix levels in the Flex System Firmware Update Guide.

4.2.1 Setting up the IBM Flex System Manager management node

The Management Server Setup wizard enables you to configure the IBM Flex System Manager management software for your network.

Before you use the Management Server Setup wizard to configure network settings, consider whether you want to assign static IP addresses to system-management elements or use a DHCP server to assign IP addresses to these elements dynamically. System-management elements include Chassis Management Modules (CMMs), Integrated Management Modules (IMMs), System-management processors, and network switches. To assign IP addresses to system-management elements dynamically, you must attach an external DHCP server to the management network (Eth0).

During the initial setup of the management software, the Management Server Setup wizard opens automatically.

Within the Management Server Setup wizard, configure the following information:

- Date and time. Specify the location of the NTP server.

  Note: You must set your keyid and password on an external NTP server to match the keyid and password that you set in the management software. For more information about setting the keyid and password on your NTP server, see the documentation that came with your NTP server.

  If you use the management node as the NTP server, the external NTP server authentication key index and key must be set to match key index and key that are set in the management software.
- Local area network (LAN) settings. Specify the IP address, DNS, and other network settings for both adapters:
  - Management network (Eth0)
  - Data network (Eth1)
- User credentials, including ID, password, and permissions.

Complete the following steps to access the initial setup wizard.

Note: If you encounter problems during the Setup Wizard, see the *Installation and Service Guide* document for troubleshooting information.

1. Connect an Ethernet cable from a notebook computer to a Chassis Management Module (CMM) in the chassis.
2. From a client computer, point a browser to

   `https://default_IP_address_or_host_name:8422/ibm/console`

   where *default_IP_address_or_host_name* is either the IPv4 address or the default host name, FSM-<*MAC address*>, on the network access tag that is attached to the IBM Flex System Manager management node. The static IPv4 address depends on the bay where you installed the management node. If you use the static IP address to connect to the network, make sure that the IP address and subnet of the client computer is set to the same value as the management node (the default subnet is 255.255.255.0). The IP address of the management node must also be in the same local domain as the client computer. To connect to the management node for the first time, you might need to change the IP properties on the client computer.

   The host name can be used if the configuration is assigned through a DHCP server; otherwise, use the IPv4 static IP address on the network access tag.

   Note: The IPv6 LLA on the tag can be used only for an SSH session. You cannot use it to connect through a web browser.
   A page with the Software License Agreement (SLA) is displayed.

   Note: If the network is configured incorrectly, you must use the console breakout cable to correct the mistake. See for more information.
3. Accept the SLA to continue setting up IBM Flex System Manager management software. If you click **Accept**, the Management Server Setup wizard opens.
4. Configure the settings on the Date and Time page.
5. Configure the settings on the System-level User ID and Password page.

   Note: The password that you set for the system-level user ID (the default is USERID) is set automatically for the `pe` user account.
   For more information about the system requirements for passwords, see Setting a new password.
6. Configure the settings on the Network Topology page. Diagrams of both network topologies are shown on this page.

   Important:

   a. The management node console can be connected to the management network or the data network. To configure the management software to access a single network that is using a single IP subnet, configure only the Eth0 interface. To configure Eth0 and Eth1, you must configure them on different IP subnets.
   b. Do not use a DHCP server to assign IP addresses for Eth0 and Eth1; otherwise, the separate management and data networks might be assigned to the same subnet.
   c. The host name must be configured on the network to which you will connect the management node. Configure the host name on the Eth0 interface if you will be connect to the management node on the management network, or configure the host name on the Eth1 interface if you will connect to the management node on the data network.
7. On the Local Area Network (LAN) Adapters page, choose the LAN adapter that you want to configure. To see a network validation and recovery summary when this setup is completed, select the check box below the table. After you select either the management or data network for configuration, the IP Address page opens.
8. Configure the IP addresses for the LAN adapter that you selected in the previous step.

Important:

a. Make sure that the IP address that is assigned to Eth0 is on the same IPv4 subnet or IPv6 network as the IP address that is assigned to the CMM.

b. The Setup wizard enables you to use a DHCP server that will assign IPv4, IPv6, or both types of IP addresses to system-management elements (for example, the CMM, IMM, System-management processors, and network switches). For the Setup wizard to obtain IP addresses automatically, a DHCP server must be attached to the management network. If you want to assign static IP addresses, a DHCP server is not required.

c. IP addresses in the range 192.168.70.200 through 192.168.70.299 are reserved for use by the management software. If you assign an IP address in this range to the Eth0 management network, you are forced to change it to an available IP address.

9. Configure the settings on the Network Settings page.

   Note: The management software supports only one default gateway.

10. Configure the settings on the Domain Name System (DNS) page.

    Important: DNS server configuration is required on the data network (Eth1) for the following management software functions:

    - Using VMControl to manage virtual machines and operating systems that are running on compute nodes
    - Updating the device drivers in the operating systems that are running on IBM Power Systems compute nodes

Approximately 5 minutes after the wizard completes the setup, you are prompted to accept the security certificate for the server. If you want to monitor the status of the process, you must accept this certification.

Depending on the browser that you use, you might have to accept the security certificate every time you log in to the IBM Flex System Manager management software. With Mozilla Firefox, the warning is displayed only during initial setup; if you add the exception during initial setup, the exception is added automatically in the future. However, Microsoft Internet Explorer might require you to accept the security certificate every time you log in.

Important: After the setup is complete, the management node restarts. Continue the next setup process, which is described in Selecting chassis for management. If you are configuring this management software as a backup node for manual failover, no further configuration is needed.

4.3 Install the original image on the secondary node

After you have completed the setup wizard, you can use the Backup and Restore function of the secondary Flex System Manager to install the backup image from the original, or primary node to the new, or secondary node. The process for doing so varies depending on how you have stored the original image.

4.3.1 Restoring and version compatibility

Make sure that you understand the version restrictions for backup images before you restore a backup image.

In most situations that require you to restore a backup of the IBM Flex System Manager management software, make sure that the management software version in the backup file matches the management software version that you use to restore the backup. The following guidelines show the compatible backups for each management software version.

Note: When you restore an IBM Flex System Manager management software, the restored IBM Flex System Manager management software will use the firmware level from the backup.

- In version 1.3.0, you can restore only a backup of version 1.3.0 or version 1.2.1
- With version 1.2.1, you can restore only a backup of version 1.2.1
- With version 1.2.0, you can restore only a backup of version 1.2.0
- With version 1.1.1, you can restore only a backup of version 1.1.1
- With version 1.1.0, you can restore only a backup of version 1.1.0

You cannot restore a backup image from management software version 1.1.1 or earlier on an IBM Flex System Manager management node with management software version 1.2.0 installed. If you must restore an image from version 1.1.1 or earlier, use the IBM Flex System Manager management software Recovery DVDs for the management software version that you want to restore.

If you want to restore from a backup image that is stored locally on the management node hard disk drive, make sure that you use the Recovery DVDs for version 1.1.1 and not version 1.1.0. A problem with version 1.1.0 requires that you noted the local backup image name before performing the recovery. With version 1.1.1, you can use the command-line interface (CLI) to list the local backups; then, you can restore the local backup from the CLI. For more information about restoring an earlier version of the management software, see 4.3.2.4, “Restoring an earlier version of the management software image,” on page 47.

4.3.2 Restoring the management software image

You can restore an IBM Flex System Manager management software image from a backup that is stored on the management node hard disk drive, USB drive, or a secure FTP server (SFTP).

Preparing to restore a backup image

You cannot restore a backup image from management software version 1.1.1 or earlier on an IBM Flex System Manager management node with management software version 1.2.0 installed. If you must restore an image from version 1.1.1 or earlier, use the IBM Flex System Manager management software Recovery DVDs for the management software version that you want to restore.

Before you restore a backup image, make sure that you understand the following conditions.

Configuring the management software after you restore a backup image

After a restore operation is complete, collect inventory for all of the managed resources in your IBM Flex System environment.

If you restored a backup that was taken from an earlier version of the management software, update the management software to the same version as before the restore operation.

Important: If you do not update the management software in this situation, the management software version might be older than other components in your environment, which might cause compatibility problems.

If any managed resources were removed from management after a backup was created, and you restore that backup image, the endpoints for the deleted resources will reappear in the management software. You must delete the endpoints manually to remove them.

Similarly, any managed resources that were discovered after a backup image was created must be re-discovered after that backup is restored.

If a chassis was managed in centralized user management mode, and you restore a backup image that was created before centralized user management mode was enabled, you might have to use the RECOVERY_ID account to re-manage the chassis. See Recovering chassis management with a CMM after a management node failure for more information.

4.3.2.1 Restoring a management software image from the hard disk drive

You can restore an IBM Flex System Manager management software image from a backup that is stored on the management node hard disk drive, USB drive, or a secure FTP server (SFTP).

The management software backup image includes all applied fixes, data on managed chassis, and any custom settings. For information about restoring a backup image from a USB drive or secure FTP server, see 4.3.2.2, "Restoring a management software image from a USB drive" or 4.3.2.3, "Restoring the management software image from a secure FTP server," on page 46.

Notes:

- If the management software has failed and the management node will not boot, you can boot the management software and restore or reinstall the management software image from optical media. See Management software recovery and reinstallation for more information.
- You can use the **listBackups** command to see a list of all of the backups. The list displays the name of the backup file and the location where it is stored.

To restore the management software image with the web interface, click **Restore now** on the Backup and Restore page, select the backup location and file for the image that you want to restore, and click **OK**.

To restore the management software image from the hard disk drive with the **restoreHDD** command in the CLI, complete the following steps:

1. Open a CLI prompt.
2. Use the **restoreHDD** *file name* command, where *file name* is the name of the backup file, to restore the image from the hard disk drive.

4.3.2.2 Restoring a management software image from a USB drive

You can restore an IBM Flex System Manager management software image from a backup that is stored on a USB drive or a secure FTP server (SFTP).

The management software backup image includes all applied fixes, data on managed chassis, and any custom settings. For information about restoring a backup image from a secure FTP server or the management node hard disk drive, see 4.3.2.3, "Restoring the management software image from a secure FTP server," on page 46 or 4.3.2.1, "Restoring a management software image from the hard disk drive."

Note: If the management software has failed and the management node will not boot, you can boot the management software and restore or reinstall the management software image from optical media. See Reinstalling management software components from optical media after replacing the hard disk drive for more information.

Before you restore a management software image from a USB drive, be aware of the following conditions:

- The only supported USB file system formats are FAT32, ext3, and ext4.
- If you use the management software web interface to restore the management software image, the USB drive is mounted automatically as part of the restore process.
- Some USB drives might not be recognized when they are first mounted. If the USB drive is not recognized initially, remove and reinsert the USB drive.
- If you restore from a USB drive that does not support a minimum write speed of 5 MBps, the management software pauses for several minutes, and the management node is inoperable.

To restore the management software image with the web interface, click **Restore now** on the Backup and Restore page, select the backup location and file for the image that you want to restore, and click **OK**.

To restore the management software image with the **restore** command in the CLI, complete the following steps:

1. Insert a USB device into the USB port on the management node. The USB device is mounted automatically.
2. Open a CLI prompt.
3. Use the **restore -l usb** command to restore the image from the USB drive.

4.3.2.3 Restoring the management software image from a secure FTP server

You can restore an IBM Flex System Manager management software image from a backup that is stored on a secure FTP server (SFTP).

Important: To restore a management software backup that was saved to management software to an SFTP server, the destination server must have Linux with Secure Shell (SSH) enabled. Otherwise, the backup operation might have failed.

The management software backup image includes all applied fixes, data on managed chassis, and any custom settings. For information about restoring a backup image from a USB drive or the management node hard disk drive, see 4.3.2.2, “Restoring a management software image from a USB drive,” on page 45 or 4.3.2.1, “Restoring a management software image from the hard disk drive,” on page 45.

Note: If the management software has failed and the management node will not boot, you can boot the management software and restore or reinstall the management software image from optical media. See Reinstalling management software components from optical media after replacing the hard disk drive for more information.

To restore the management software image with the web interface, click **Restore now** on the Backup and Restore page, select the backup location and file for the image that you want to restore, and click **OK**.

To restore the management software image from an SFTP server with the **restore** command in the CLI, complete the following steps:

1. Open a CLI prompt.
2. Use the **restore** command with the SFTP server name, path, user name, and password (see the following example) to back up the software image to SFTP:

```
restore -l sftp -s [sftp server name] -d [path on sftp server]
 -u [sftp user name] -p [sftp_password]
```

4.3.2.4 Restoring an earlier version of the management software image

In some circumstances, you might want to restore a management software image that is earlier than the version that is installed when a management node fails. Use this information to understand the conditions for restoring an earlier management software version.

Before you restore an earlier version of the management software to the management node, make sure that you understand the following conditions:

- You cannot restore a backup image from management software version 1.1.1 or earlier on an IBM Flex System Manager management node with management software version 1.2.0 installed. If you must restore an image from version 1.1.1 or earlier, use the IBM Flex System Manager management software Recovery DVDs for the management software version that you want to restore.
- If you want to restore a backup image that is stored locally on the management node hard disk drive, you might need to restore version 1.1.1 and not version 1.1.0. A problem with version 1.1.0 requires that you noted the local backup image name before performing the recovery; the local backup files are retained after recovery, but the names are lost. With version 1.1.1, you can use the command-line interface (CLI) to list the local backups; then, you can restore the local backup from the CLI.

To restore an earlier version of the management software, complete the following steps.

Important: If you want to restore a local backup after recovering the management software, make sure that you recover to version 1.1.1 (and not version 1.1.0).

1. Use the Recovery DVDs to recover the management software image by completing the procedure in Reinstalling management software components from optical media after replacing the hard disk drive.

   Note: Before you request the Recovery DVDs from IBM Support, see Obtaining the IBM Flex System Manager Recovery DVDs to determine the FRU part number for your version of the management software.
2. Open the management software CLI, and run the **listBackups** command. The output displays all types of management software backups (local hard disk drive, USB, and SFTP). Note the name of the backup file that you want to restore.
3. Depending on the location of your backup file, complete one of the following actions"
   a. To restore a backup from SFTP or USB, use the **restore** to restore the backup image.
   b. To restore a backup from the local management node hard disk drive, use the **restoreHDD** command.

4.3.2.5 Remanaging a CMM after a Restore

Follow these steps to return a Chassis Management Module (CMM) to a managed state after restoring the image due to corruption or FRU replacement.

When a CMM is managed by the IBM Flex System Manager, user management is performed by the IBM Flex System Manager. User accounts and certificates on the CMM are locked, and the necessary certificates are not included in the backup image, which will cause communications between the IBM Flex System Manager and the CMM to fail.

Therefore when the CMM is restored using a backup image, manual intervention is required to enable the CMM to be re-managed by the IBM Flex System Manager. Follow these steps to return the CMM to a managed state after restoring the image.

1. Restore the CMM using an existing backup image.
2. If you are using a backup image that was created while the CMM was in a managed state, disable centralized account management using the procedure below. If you are using a backup image that was created while the CMM was in an unmanaged state, proceed to step 3.
   a. Access the CMM command line via SSH, using the Recovery ID and password from the IBM Flex System Manager.
   b. Set the primary CMM as the target of commands by invoking the command `env -t mm[p]`.
   c. Disable centralized management by invoking the command `fsmcm -off`. The SSH session will end immediately, as disabling centralized management deletes the Recovery ID from the CMM.
3. Access the CMM command line via SSH using restore password from the CMM, and change the password as required on first use.
4. Remanage the CMM using the IBM Flex System Manager.

4.4 Restoring and version compatibility

Make sure that you understand the version restrictions for backup images before you restore a backup image.

In most situations that require you to restore a backup of the IBM Flex System Manager management software, make sure that the management software version in the backup file matches the management software version that you use to restore the backup. The following guidelines show the compatible backups for each management software version.

Note: When you restore an IBM Flex System Manager management software, the restored IBM Flex System Manager management software will use the firmware level from the backup.

- In version 1.3.0, you can restore only a backup of version 1.3.0 or version 1.2.1
- With version 1.2.1, you can restore only a backup of version 1.2.1
- With version 1.2.0, you can restore only a backup of version 1.2.0
- With version 1.1.1, you can restore only a backup of version 1.1.1
- With version 1.1.0, you can restore only a backup of version 1.1.0

You cannot restore a backup image from management software version 1.1.1 or earlier on an IBM Flex System Manager management node with management software version 1.2.0 installed. If you must restore an image from version 1.1.1 or earlier, use the IBM Flex System Manager management software Recovery DVDs for the management software version that you want to restore.

If you want to restore from a backup image that is stored locally on the management node hard disk drive, make sure that you use the Recovery DVDs for version 1.1.1 and not version 1.1.0. A problem with version 1.1.0 requires that you noted the local backup image name before performing the recovery. With version 1.1.1, you can use the command-line interface (CLI) to list the local backups; then, you can restore

the local backup from the CLI. For more information about restoring an earlier version of the management software, see 4.3.2.4, “Restoring an earlier version of the management software image,” on page 47.

4.5 Restoring the management software image

You can restore an IBM Flex System Manager management software image from a backup that is stored on the management node hard disk drive, USB drive, or a secure FTP server (SFTP).

Preparing to restore a backup image

You cannot restore a backup image from management software version 1.1.1 or earlier on an IBM Flex System Manager management node with management software version 1.2.0 installed. If you must restore an image from version 1.1.1 or earlier, use the IBM Flex System Manager management software Recovery DVDs for the management software version that you want to restore.

Before you restore a backup image, make sure that you understand the following conditions.

Configuring the management software after you restore a backup image

After a restore operation is complete, collect inventory for all of the managed resources in your IBM Flex System environment.

If you restored a backup that was taken from an earlier version of the management software, update the management software to the same version as before the restore operation.

Important: If you do not update the management software in this situation, the management software version might be older than other components in your environment, which might cause compatibility problems.

If any managed resources were removed from management after a backup was created, and you restore that backup image, the endpoints for the deleted resources will reappear in the management software. You must delete the endpoints manually to remove them.

Similarly, any managed resources that were discovered after a backup image was created must be re-discovered after that backup is restored.

If a chassis was managed in centralized user management mode, and you restore a backup image that was created before centralized user management mode was enabled, you might have to use the RECOVERY_ID account to re-manage the chassis. See Recovering chassis management with a CMM after a management node failure for more information.

4.5.1 Restoring a management software image from the hard disk drive

You can restore an IBM Flex System Manager management software image from a backup that is stored on the management node hard disk drive, USB drive, or a secure FTP server (SFTP).

The management software backup image includes all applied fixes, data on managed chassis, and any custom settings. For information about restoring a backup image from a USB drive or secure FTP server, see 4.3.2.2, “Restoring a management software image from a USB drive,” on page 45 or 4.3.2.3, “Restoring the management software image from a secure FTP server,” on page 46.

Notes:

- If the management software has failed and the management node will not boot, you can boot the management software and restore or reinstall the management software image from optical media. See Management software recovery and reinstallation for more information.
- You can use the **listBackups** command to see a list of all of the backups. The list displays the name of the backup file and the location where it is stored.

To restore the management software image with the web interface, click **Restore now** on the Backup and Restore page, select the backup location and file for the image that you want to restore, and click **OK**.

To restore the management software image from the hard disk drive with the **restoreHDD** command in the CLI, complete the following steps:

1. Open a CLI prompt.
2. Use the **restoreHDD** *file name* command, where *file name* is the name of the backup file, to restore the image from the hard disk drive.

4.5.2 Restoring a management software image from a USB drive

You can restore an IBM Flex System Manager management software image from a backup that is stored on a USB drive or a secure FTP server (SFTP).

The management software backup image includes all applied fixes, data on managed chassis, and any custom settings. For information about restoring a backup image from a secure FTP server or the management node hard disk drive, see 4.3.2.3, “Restoring the management software image from a secure FTP server,” on page 46 or 4.3.2.1, “Restoring a management software image from the hard disk drive,” on page 45.

Note: If the management software has failed and the management node will not boot, you can boot the management software and restore or reinstall the management software image from optical media. See Reinstalling management software components from optical media after replacing the hard disk drive for more information.

Before you restore a management software image from a USB drive, be aware of the following conditions:

- The only supported USB file system formats are FAT32, ext3, and ext4.
- If you use the management software web interface to restore the management software image, the USB drive is mounted automatically as part of the restore process.
- Some USB drives might not be recognized when they are first mounted. If the USB drive is not recognized initially, remove and reinsert the USB drive.
- If you restore from a USB drive that does not support a minimum write speed of 5 MBps, the management software pauses for several minutes, and the management node is inoperable.

To restore the management software image with the web interface, click **Restore now** on the Backup and Restore page, select the backup location and file for the image that you want to restore, and click **OK**.

To restore the management software image with the **restore** command in the CLI, complete the following steps:

1. Insert a USB device into the USB port on the management node. The USB device is mounted automatically.
2. Open a CLI prompt.
3. Use the **restore -l usb** command to restore the image from the USB drive.

4.5.3 Restoring the management software image from a secure FTP server

You can restore an IBM Flex System Manager management software image from a backup that is stored on a secure FTP server (SFTP).

Important: To restore a management software backup that was saved to management software to an SFTP server, the destination server must have Linux with Secure Shell (SSH) enabled. Otherwise, the backup operation might have failed.

The management software backup image includes all applied fixes, data on managed chassis, and any custom settings. For information about restoring a backup image from a USB drive or the management node hard disk drive, see 4.3.2.2, “Restoring a management software image from a USB drive,” on page 45 or 4.3.2.1, “Restoring a management software image from the hard disk drive,” on page 45.

Note: If the management software has failed and the management node will not boot, you can boot the management software and restore or reinstall the management software image from optical media. See Reinstalling management software components from optical media after replacing the hard disk drive for more information.

To restore the management software image with the web interface, click **Restore now** on the Backup and Restore page, select the backup location and file for the image that you want to restore, and click **OK**.

To restore the management software image from an SFTP server with the **restore** command in the CLI, complete the following steps:

1. Open a CLI prompt.
2. Use the **restore** command with the SFTP server name, path, user name, and password (see the following example) to back up the software image to SFTP:

```
restore -l sftp -s [sftp server name] -d [path on sftp server]
 -u [sftp user name] -p [sftp_password]
```

4.5.4 Restoring an earlier version of the management software image

In some circumstances, you might want to restore a management software image that is earlier than the version that is installed when a management node fails. Use this information to understand the conditions for restoring an earlier management software version.

Before you restore an earlier version of the management software to the management node, make sure that you understand the following conditions:

- You cannot restore a backup image from management software version 1.1.1 or earlier on an IBM Flex System Manager management node with management software version 1.2.0 installed. If you must restore an image from version 1.1.1 or earlier, use the IBM Flex System Manager management software Recovery DVDs for the management software version that you want to restore.
- If you want to restore a backup image that is stored locally on the management node hard disk drive, you might need to restore version 1.1.1 and not version 1.1.0. A problem with version 1.1.0 requires that you noted the local backup image name before performing the recovery; the local backup files are retained after recovery, but the names are lost. With version 1.1.1, you can use the command-line interface (CLI) to list the local backups; then, you can restore the local backup from the CLI.

To restore an earlier version of the management software, complete the following steps.

Important: If you want to restore a local backup after recovering the management software, make sure that you recover to version 1.1.1 (and not version 1.1.0).

1. Use the Recovery DVDs to recover the management software image by completing the procedure in Reinstalling management software components from optical media after replacing the hard disk drive.

   Note: Before you request the Recovery DVDs from IBM Support, see Obtaining the IBM Flex System Manager Recovery DVDs to determine the FRU part number for your version of the management software.
2. Open the management software CLI, and run the **listBackups** command. The output displays all types of management software backups (local hard disk drive, USB, and SFTP). Note the name of the backup file that you want to restore.
3. Depending on the location of your backup file, complete one of the following actions"
   a. To restore a backup from SFTP or USB, use the **restore** to restore the backup image.
   b. To restore a backup from the local management node hard disk drive, use the **restoreHDD** command.

4.5.5 Remanaging a CMM after a Restore

Follow these steps to return a Chassis Management Module (CMM) to a managed state after restoring the image due to corruption or FRU replacement.

When a CMM is managed by the IBM Flex System Manager, user management is performed by the IBM Flex System Manager. User accounts and certificates on the CMM are locked, and the necessary certificates are not included in the backup image, which will cause communications between the IBM Flex System Manager and the CMM to fail.

Therefore when the CMM is restored using a backup image, manual intervention is required to enable the CMM to be re-managed by the IBM Flex System Manager. Follow these steps to return the CMM to a managed state after restoring the image.

1. Restore the CMM using an existing backup image.
2. If you are using a backup image that was created while the CMM was in a managed state, disable centralized account management using the procedure below. If you are using a backup image that was created while the CMM was in an unmanaged state, proceed to step 3.
   a. Access the CMM command line via SSH, using the Recovery ID and password from the IBM Flex System Manager.
   b. Set the primary CMM as the target of commands by invoking the command `env -t mm[p]`.
   c. Disable centralized management by invoking the command `fsmcm -off`. The SSH session will end immediately, as disabling centralized management deletes the Recovery ID from the CMM.
3. Access the CMM command line via SSH using restore password from the CMM, and change the password as required on first use.
4. Remanage the CMM using the IBM Flex System Manager.

4.6 Collect inventory and complete changes

After restoring the backup image to the new Flex System Manager, you must collect inventory from the systems that are now being managed by the new Flex System Manager. You can then use this information to recreate management changes that occurred after the backup image was created.

To learn more about collecting inventory, see Collecting and viewing inventory data in the IBM Flex System documentation information center.

Chapter 5. Validating a system restore

IBM provides additional documentation that will assist you in validating a system restore.

See the firmware updates best practices guides.

Part Number: 88Y7763

Printed in USA

(1P) P/N: 88Y7763