IBM Fabric Manager

Installation and User's Guide

IBM Fabric Manager

Installation and User's Guide

Note

Before using this information and the product it supports, read the information in "Notices" on page 53.

Updated July 2014

This edition applies to version 4.1 of IBM Fabric Manager and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Introduction

IBM® Fabric Manager (IFM) is a solution that enables you to quickly replace and recover IBM BladeCenter® blade servers and IBM Flex System® compute nodes in your environment.

Note: This publication uses the term *server* to refer collectively to IBM BladeCenter blade servers and IBM Flex System compute nodes. This publication uses the term *management module* to refer collectively to the IBM BladeCenter Advanced Management Module (AMM) and the IBM Flex System Chassis Management Module.

IFM assigns Ethernet MAC, Fibre Channel WWN, and SAS WWN addresses so that any servers plugged into those bays take on the assigned addresses. This enables the Ethernet and Fibre Channel infrastructure to be configured once and before any servers are connected to the chassis.

With IFM, you can monitor the health of servers and automatically - without user intervention - replace a failed server from a designated pool of spare servers. After receiving a failure alert, IFM attempts to power off the failing server, read the IFM virtualized addresses and boot target parameters, apply these parameters to the next server in the standby pool, and power on the standby server.

You can also pre-assign MAC and WWN addresses, as well as storage boot targets, for up to 256 chassis or 3584 servers. Using an enhanced graphical user interface, you can create addresses for servers and save the address profiles. Then, you can deploy the addresses to the bays in the same chassis or in up to 256 different chassis. This can be done without any servers installed in the chassis. Additionally, you can create profiles for chassis that have not been installed in the environment by simply associating an IP address to the future chassis.

To obtain the most up-to-date documentation for this product, go to http://pic.dhe.ibm.com/infocenter/flexsys/information/index.jsp.

Before you begin

There are minimum hardware and software requirements that the system must meet before you can install or use IFM.

Hardware requirements

The following notes describe the hardware requirements.

- **Microprocessor:**
  - Minimum requirements:
    - 1 GHz for IBM X-Architecture® compute nodes and IBM BladeCenter blade servers
    - 1.4 GHz for IBM Power Systems™ compute nodes
  - 2 GHz or faster recommended
- **Memory:**
  - 512 MB minimum
  - 2 GB recommended

- **Hard disk drive space:** 1 GB free hard disk drive space required

Supported operating systems

IFM is supported on selected Microsoft Windows and Linux operating systems.

Table 1. IFM supported operating systems

Operating System
Microsoft Windows 2003 (32/64 bit) (SP1 and SP2)
Microsoft Windows 2003 R2 (32/64 bit) (SP1 and SP2)
Microsoft Windows Server 2008 (32/64 bit) (SP1 and SP2)
Microsoft Windows Server 2008 R2 (64 bit) (SP1)
RHEL 5 (32/64 bit) (up to SP5)
RHEL 6 (32/64 bit) (up to SP3)
SLES 10 (32/64 bit) (up to SP2)
SLES 11 (32/64 bit) (up to SP2)

Note:

IBM Java™ 1.7 is also required.

Supported web browsers

This topic provides information about the supported web browsers.

IFM supports the following web browsers.

- Microsoft Internet Explorer 8.0 or 9.0

  Notes:

  – If you use Internet Explorer 8.0, once the default certificate expires, you must change the browser security settings to connect to the IFM console.

  – The change zoom level feature of Internet Explorer is known to cause various display issues. The zoom level should be set to 100% for the best results. Also, avoid changing the zoom level while IFM console tabs or windows are open.
- Mozilla FireFox version 17 Extended Support Release (ESR)

The minimum screen resolution with the web browser maximized is 1024 x 768.

License information

This topic provides license information.

IFM is available as a stand-alone application or as part of the IBM Flex System Manager management software bundle.

- The stand-alone application can be purchased through your IBM business partner as you would purchase any other software and hardware option. After purchasing, go to http://www.ibm.com/systems/x/fod/ and download an activation key.
- When you purchase IFM as part of the IBM Flex System Manager management software bundle, IBM applies the IFM activation key to the IBM Flex System Manager management software at the factory.

The Features on Demand (FoD) website provides a user interface for creating and retrieving keys and is the repository of Features on Demand key information and history. Use the Features on Demand website to register users, activate keys, retrieve keys or authorization codes, and generate reports.

For more information about FoD, go to http://www.ibm.com/support/entry/portal/docdisplay?lndocid=MIGR-5089568.

- To retrieve a customer number, complete the following steps:
  1. Go to http://www.ibm.com/systems/x/fod/.
  2. Click **Manage IBM customer number**.
- To retrieve an authorization code, complete the following steps:
  1. Go to http://www.ibm.com/systems/x/fod/.
  2. Click **Retrieve authorization code**.
  3. Enter the customer number with country code, plant order number, and order part number or product ID. These numbers are on the packing list that comes with your order. The **Your Email address** field is automatically populated with the user email address. In the Other recipients field, separate email addresses with commas.
  4. Click **Submit**.
- To create a customer key, complete the following steps:
  1. Go to http://www.ibm.com/systems/x/fod/.
  2. Click **Request activation key**.
  3. Enter the activation key and click **Continue**.
  4. Enter the unique identifier (UID) specified for feature activation.
  5. Click **Generate key**.
- To retrieve a customer key, complete the following steps:
  1. Go to http://www.ibm.com/systems/x/fod/.
  2. Click **Retrieve history**.
  3. Select the **Search history via machine type and serial number**.
  4. Select one or more keys to email or download.

Accessibility features for IFM

Accessibility features help users who have a disability, such as restricted mobility or limited vision, to use information technology products successfully.

Accessibility features

The IBM Flex System Information Center is accessibility-enabled. The accessibility features of the information center include:

- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- The attachment of alternative input and output devices

Keyboard navigation

This product uses standard Microsoft® Windows® navigation keys.

Related accessibility information

You can view the IBM Flex System publications in Adobe® Portable Document Format (PDF) using the Adobe Acrobat® Reader. The PDFs are provided on a CD that is packaged with the product, or you can access them through the IBM Flex System Information Center.

IBM and accessibility

See the IBM Human Ability and Accessibility Center for more information about the commitment that IBM has to accessibility.

Documentation and related information

This topic provides information about documentation and related information.

In addition to this *Installation and User's Guide*, the following IFM resources are available on the Web.

- **IBM BladeCenter documentation and technical support**

  See http://www.ibm.com/supportportal to locate the most recent versions of all IBM BladeCenter documentation, and also obtain support for IBM hardware and systems-management software.
- **IBM BladeCenter Interoperability Guide**

  You can obtain compatibility and interoperability information about IBM BladeCenter products from this IBM Redpaper™ publication. To obtain the most recent version, go to http://www.redbooks.ibm.com/abstracts/redpbcig.html.
- **IBM Fabric Manager**

  To access an overview of IFM, go to http://www-03.ibm.com/systems/flex/fabricmanager/bto/index.html.
- **IBM Flex System Information Center**

  To obtain the most up-to-date documentation for this product, go to http://pic.dhe.ibm.com/infocenter/flexsys/information/index.jsp.
- **IBM ServerProven® compatibility**

  You can obtain compatibility information about IBM Flex System products from http://www.ibm.com/systems/info/x86servers/serverproven/compat/us.

Notices and statements in this document

This topic provides information about notices and statements.

The following notices and statements are used in this document:

- **Note:** These notices provide important tips, guidance, or advice.
- **Important:** These notices provide information or advice that might help you avoid inconvenient or problem situations.
- **Attention:** These notices indicate potential damage to programs, devices, or data. An attention notice is placed just before the instruction or situation in which damage might occur.
- **Caution:** These statements indicate situations that can be potentially hazardous to you. A caution statement is placed just before the description of a potentially hazardous procedure step or situation.

- **Danger:** These statements indicate situations that can be potentially lethal or extremely hazardous to you. A danger statement is placed just before the description of a potentially lethal or extremely hazardous procedure step or situation.

Chapter 2. Considerations

This topic describes information that you must consider when you setup and use IFM.

Chassis and server considerations

This topic describes information that you must consider when you configure the hardware you manage with IFM.

Hardware support

IFM is supported on selected IBM BladeCenter devices and IBM Flex System devices.

Table 2. Supported devices

IBM BladeCenter devices	• BladeCenter E • BladeCenter ER • BladeCenter H • BladeCenter HT • BladeCenter S
IBM Flex System devices	IBM Flex System Enterprise Chassis

Enabling additional secure connections

This topic provides information about enabling additional secure connections for IBM Flex System compute nodes.

(IBM Flex System devices only) You must configure the CMM to enable IFM access. To set the TCP Command Mode Protocol on the CMM Web interface, complete the following steps.

1. From the CMM Web interface, click **Mgt Module Management > Network**.
2. Click the **TCP Command Mode** tab and make sure that the **Secure command mode connections** field is set to a minimum of 5 (20 is the maximum value).

Standby management module

Because a management module failure results in a configuration loss, it is best practice to install a standby management module when using IFM.

The IFM configuration is not included in the management module configuration backup. Such a backup would allow IFM configuration updates from a file that might be outdated. This would cause inconsistencies with the configuration of other chassis.

The IFM configuration is chassis-based and does not transfer with the physical management module. When a management module is moved to a new chassis, it clears out its IFM configuration, and the IFM configuration must be reapplied on the new management module.

Note: When a management module is moved to a new chassis, it clears the configuration for all bays except for bays that have servers powered-on with a valid IFM configuration that is already in use. For these bays, the management module uses the IFM configuration as defined on the servers.

If the management module configuration is reset to factory defaults, the IFM configuration is handled as if a new management module was installed in the chassis.

If the primary management module fails, the standby management module contains the IFM configuration and takes over.

Note: You might have to wait approximately 2 minutes while the active management module transfers firmware and configuration information to the standby management module.

Setting up boot from SAN

To take full advantage of the IFM solution, set up your server environment to boot from SAN.

- For more information about the IBM 4 Gb SAN solution, go to http://www.redbooks.ibm.com/abstracts/sg247313.html?Open.
- To obtain the Emulex IBM HBA Installation and Management white paper, go to http://www.emulex.com/white/hba/IBMBlade.pdf.

Replacing a server in the same bay

When you replace a server in a bay that is IFM enabled, the IFM parameters are automatically applied to the new server before it is given power permission. The boot sequence is not part of the IFM configuration and it is not pushed automatically.

Replacing the management module in a single management module environment

You can replace the management module in a single management module environment.

About this task

When you replace a management module and you don't have a standby management module in the chassis, the IFM configuration is cleared. If the current management module is functioning, insert the new management module in the second bay as a standby management module for a few minutes. This allows the primary management module to synchronize the IFM configuration with the standby management module before the primary management module is removed. If this is not possible, you can reapply the IFM configuration after inserting the new management module. By default, the management module clears its IFM configuration when inserted into a new chassis. However, if any of the servers are already powered on when the management module is inserted into a new chassis, the management module takes the IFM configuration from those servers.

If the management module was reinserted into the same chassis it was previously in, it continues to use the IFM configuration that is defined on the management module. During the period that the management module was not in the chassis, the IFM configuration might have changed. In this case, inconsistencies and address duplications can occur.

If the management module configuration is reset to factory defaults, the IFM configuration is cleared the same way as if a new management module is inserted into a chassis. Also, the IFM configuration is not included in the management module configuration file, so when restoring the management module configuration from a file, the IFM configuration does not change.

Notes:

- You might have to wait longer if the management module you insert in the standby bay does not have the same firmware level as the primary. In that case, the standby management module is flashed first and then the data is synchronized.
- (IBM Flex System devices only) If an error occurs during the CMM replacement procedure, complete the following steps.
  1. From the CMM Web interface, select **Mgt Module Management > Properties > Advanced Failover**.
  2. Wait several minutes while the original CMM becomes the primary CMM again. Wait one hour for the configuration to synchronize.
  3. To complete the CMM replacement, repeat Step 1.

Multi-bay servers and the server offset parameter

Some servers fill more than a single bay in the chassis. As a result, they can access more ports than a single-bay server.

The maximum number of ports available to a single bay is 8. Ports beyond the eight ports of the first server are accessed using a server offset. The server offset is a 0 indexed value and the additional bays are mezzanine bays.

Table 3. IBM BladeCenter blade servers - slot offset and the adapter identifier

Slot offset	Adapter type
0	Combination form factor horizontal (CFFH), Combination form factor vertical (CFFV), and Combination I/O vertical (CIOV)
1	CFFH, CFFV, and CIOV
2	CFFH, CFFV, and CIOV
3	CFFH, CFFV, and CIOV

Table 4. IBM Flex System compute nodes - compute node offset and the mezzanine bay identifier

Compute-node offset	Mezzanine bays
0	1 and 2
1	3 and 4
2	5 and 6
3	7 and 8

Redundant servers

This topic provides information about redundant servers.

The failover function for IFM consists of a primary IFM server, which is a normally running the IFM application, and a secondary IFM server, which monitors the health of the primary IFM server, and can take over processing, if necessary.

You can have only one IFM application installed, but you can define a properties file (standby.prop) to configure the failover function, invoking appropriate behavior as required to monitor and failover, if necessary.

Configuration

This topic provides information about configuring redundant servers.

The standby.prop file includes the following parameters.

Table 5. Standby.prop file parameters

Parameter	Description
`primaryIP=9.72.217.181`	IP address of the primary IFM server
`primaryID=USERID`	User ID of the primary IFM server
`primaryPW=PASSW0RD`	Password of the primary IFM server
`retryLimit=3`	Number of tries to attempt before failover
`backupInterval=30000`	Number of milliseconds to wait to request data from the primary IFM server

The standby.prop file must be placed in the ~/ofm/data folder of the secondary IFM server.

Based on the values in the standby.prop file, the secondary IFM server requests the configuration data from the primary server in the form of a jar file. If this request fails, the secondary IFM server will retry, based on the number of attempts in the `retryLimit` parameter. The jar file (primary.jar) is placed in the ~/ofm/tmp folder. If the request to the primary fails the number of attempts, the secondary unjars the primary.jar file in the data folder and begins a normal startup as the new primary IFM server.

Administration considerations

This topic provides information about administration considerations for redundant servers.

The administrator is responsible for creating the ~/data folder before the secondary IFM server is started up, and for configuring the standby.prop file in the folder.

Besides logs written into the ifmServer.log on the secondary IFM server, there is no indication that the original primary IFM server has failed and that the secondary IFM server has become the new primary IFM server.

Mapping of devices to ports

This topic provides information about mapping devices to ports.

IBM BladeCenter devices

(IBM BladeCenter devices only) BladeCenter devices number ports by bay and offset. BladeCenter devices provide four offsets per bay and eight physical ports (or 16 virtual ports) per offset.

- Ports 1 and 2 are reserved for the on-board Ethernet devices.
- Ports 3 and 4 are reserved for standard expansion cards.
- Ports 5 to 8 are reserved for high-speed expansion cards.

Note: Map high-speed two-port combination form factor horizontal (CFFH) converged network adapters to ports 5 and 7. The mapping between the IFM ports and the switch numbering on the BladeCenter chassis is dependent on the chassis. For example, the BCS chassis routes both on-board Ethernet devices to I/O Module bay 1.

The following table defines the mapping of the IFM ports to the switch numbering on the IBM BladeCenter chassis.

Table 6. IBM BladeCenter IO module numbering

	IBM BladeCenter model			
IFM port	**H**	**E**	**HT**	**S**
1	1	1	1	1
2	2	2	2	1
3	3	3	3	3
4	4	4	4	4
5	7	N/A	7	2
6	8	N/A	8	2
7	9	N/A	9	N/A
8	10	N/A	10	N/A

IBM Flex System devices

(IBM Flex System devices only) For IBM Flex System devices, ports are numbered in bay, offset, and mezzanine order. Flex System devices offer four offsets per bay, 2 mezzanines per offset, and 8 physical ports (16 virtual mezzanine). The mapping of ports to the devices on the compute node is not limited by fabric type.

The following table defines the mapping of the IFM ports to the switch numbering on the IBM Flex System chassis.

Table 7. IBM Flex System IO module numbering

Mezzanine 1		**Mezzanine 2**	
IFM Port	**IO module**	**IFM Port**	**IO module**
1	1	1	3
2	2	2	4
3	1	3	3
4	2	4	4
5	1	5	3
6	2	6	4

Table 7. IBM Flex System IO module numbering (continued)

Mezzanine 1		**Mezzanine 2**	
IFM Port	**IO module**	**IFM Port**	**IO module**
7	1	7	3
8	2	8	4

Support for Power Systems servers

This topic provides information about the IFM management of Power Systems servers.

(IBM Flex System devices only) IFM is not supported with SAS adapters on Power Systems servers. IFM management of Fibre Channel boot targets is not supported on Power Systems servers. You can pre-assign Fibre Channel boot targets in the configuration using SMS menus.

Configuring the management module to send traps

This topic provides information about configuring the management module to send traps.

(IBM BladeCenter devices only) The IBM BladeCenter system chassis requires Simple Network Management Protocol (SNMP) version 1 to be configured. To configure the AMM to send traps, complete the following steps.

1. From the AMM interface access the **MM Control - Network Protocols** page.
2. Click on the **Simple Network Management Protocol (SNMP)** link and make sure that SNMP traps and SNMPv1 agent are enabled and configured.
3. Set the **Access Type** to **Trap** for at least one community.
4. Make sure that the IP or hostname of the IFM server is listed as one of the three addresses for the community.
5. If the community is not named, do one of the following:
   - Set the **Community Name** to **Trap**. This is the default value.
   - Locate the server.prop file (default location is /ofm/data) and add or change the following entry: `CommunityName=<community name>`. Where `<community name>` is the name of the community (if the IFM server is already running, changing this value will necessitate a restart of IFM for the change to take effect).
6. Setup event recipients:
   a. Access the **MM Control - Alerts** page.
   b. Configure at least one **Remote Alert Recipient**:
      - Select **SNMP over LAN** as the **Notification Method**.
      - Select **Receive all alerts**.
      - Enable the remote alert recipient.
   c. In the **Monitored Alerts** section, select all options under **Critical Events**, **Warning Events**, and **Informational Events**.
7. Setup the SNMP trap recipient port:
   a. Access the **MM Control - Port Assignments** page.
   b. Complete one of the following:
      - Set the **SNMP Traps Port** to **50990**.

- Locate the server.prop file (default location is /ofm/data) and add or change the following entry: `SNMPTrapPort=<traps port>`. Where `<traps port>` is the port currently configured for SNMP Traps (if your IFM server is already running, changing this value will necessitate a restart of IFM for the change to take effect).

(IBM Flex System devices only) To configure the IBM Flex System CMM to send traps, complete the following steps.

1. Select **Event Recipients** from the **Events** menu.
2. Click **Global Settings**.
3. Select all options under **Critical Events**, **Warning Events**, and **Informational Events**.
4. Click **OK**.

Configuring a dedicated user account

This topic provides information about configuring a dedicated user account.

You can configure a dedicated user account, for example, to prevent invalid credentials supplied to IFM from locking out chassis administration for any other user account, or to make sure that IFM initiated auditable events are plainly discernible from other user events.

(IBM BladeCenter devices only) To setup a new user account, complete the following steps.

1. Access the **MM Control - Login Profiles** page.
2. Click on a free slot (Login ID marked as**~ not used** ~).
3. Type a **Login ID** and **Password**.
4. Set the **Maximum simultaneous active sessions** to **0**.
5. Set the **Role** to **Supervisor**.

(IBM Flex System devices only) To setup a new user account, complete the following steps.

1. Access the **Mgt Module Management - User Accounts** page.
2. Click **Create User**.
3. Type a **User name** and **Password**.
4. Set the **Maximum simultaneous active sessions** to **0**.
5. Click **Next**.
6. Select **Default Supervisor Group**.
7. Click **Finish**.

Configuring IFM for secure sockets layer

This topic provides information about secure sockets layer.

IFM supports the use of secure sockets layer (SSL) to provide a secure communication method to access IFM from a web browser. A default SSL configuration comes with IFM for use during installation and testing. Use an installation-specific configuration during normal operation.

Setting up SSL

This topic provides information about setting up secure sockets layer.

SSL keys and certificates are held in a keystore file. The keystore file provided with IFM is located in the product directory. For production, choose a private directory with restricted access to hold the keystore file. Even though it is password protected, the password is configured into the runtime environment so it might be vulnerable to theft. Check with your security administrator to see if the installation already has a keystore file.

Generating keys and certificates

This topic provides information about generating keys and certificates.

Note: The examples in this topic use the keytool utility provided with the Java Runtime Environment (JRE). The examples in this topic assume that the command is available through the PATH environment variable.

The following command generates a key pair and certificate directly into a keystore file:

```
cd <ksdir>
keytool -keystore <ksfile> -alias jetty -genkey -keyalg RSA
```

The term <ksdir> is the directory used to hold the keystore file. The term <ksfile> is the name of the keystore file. Do not include the “<>” characters. For example:

```
cd /etc
</jetty></ksfile></ksdir></ksfile>
```

The following command prompts for information about the certificate and for passwords to protect both the keystore file and the keys within it. The only mandatory response is to provide the fully qualified hostname of the server at the `What is your first  and last name?` prompt.

```
keytool -keystore jettyks -alias jetty -genkey -keyalg RSA
Enter keystore password: secret
Re-enter new password: secret
What is your first  and last name?
[Unknown]:  ifm.ibm.com
What is the name of your organizational unit?
[Unknown]: IFM User
What is the name of your organization?
[Unknown]:
What is the name of your City or Locality?
[Unknown]:
What is the name of your State or Province?
Unknown]:
What is the two-letter country code for this unit?
[Unknown]:
Is CN=ifm.ibm.com,
OU=IFM User, O=Unknown, L=Unknown, ST=Unknown, C=Unknown correct?
(type "yes" or "no") [no]:   yes

Enter key password  for <jetty>:
(RETURN if same as  keystore password):
```

Requesting trusted certificates

This topic provides information about requesting trusted certificates.

The keys and certificates generated with the keytool utility are sufficient to run SSL. However, the browser does not automatically trust the certificate you have generated and it prompts you to accept the certificate. To obtain a certificate trusted by most common browsers, request a certificate authority (CA) to sign your key/certificate.

The following command generates a CSR for a certificate already in the keystore file:

```
keytool -certreq -alias jetty -keystore <ksfile> -file <csrfile>
```

The term <ksfile> is the name of the keystore file. The term <csrfile> is the name of the generated CSR. Do not include the "<>" characters.

Once a CA has sent you a certificate, load it into the keystore file. Signed certificates are typically returned in the PEM format.

```
 keytool -keystore <ksfile> -import -alias jetty -file <crtfile> -trustcacerts
```

The term <ksfile> is the name of the keystore file. The term <crtfile> is the name of the file containing the signed certificate. Do not include the "<>" characters.

Protecting the keystore file

This topic provides information about protecting the keystore file.

If you have generated a new keystore file specifically for use with IFM, it is best practice to protect it against unauthorized modification. Place the keystore file in the IFM data directory. The default for this directory is /ofm/data on Windows and /opt/ibm/ofm/data on Linux. Also, do not allow universal read access to the keystore file, and only allow write access for system administrators and the user ID that runs IFM.

Windows users can alter file permissions from Windows Explorer. Remove the access for the SYSTEM group and, if necessary, grant read and write permission for the IFM user ID. Linux users can assign the ownership of the keystore file to the IFM user and remove universal access using a command shell.

```
chown <ifmuser> <ksfile>
chmod 640 <ksfile>
```

The term <ifmuser> is the user ID under which IFM runs. The term <ksfile> is the fully qualified name of the keystore file. Do not include the "<>" characters.

Configuring IFM to use certificates

This topic provides information about configuring IFM to use certificates.

The IFM server configuration file must be modified to point to the keystore file you have created and also to provide the password for the keystore file. Locate the server.prop file (default location is /ofm/data) and add the following entries:

```
sslKeystore=<ksfile>
sslPassword=<kspassword>
```

The term <ksfile> is the fully qualified name of the keystore file. The term <crtfile> is the password for the keystore file. Do not include the "<>" characters. For example:

```
 sslKeystore=/etc/jettyks
 sslPassword=passw0rd
```

Configuring and using failover monitoring

This topic provides information about configuring and using failover monitoring.

Failover operation

This topic provides information about failover operation.

When a failover monitor detects a triggering event, IFM invokes a failover operation and performs the following actions:

1. Removes existing deployment data from the standby server.
2. Powers off the standby server, if it is powered on, unless **Ignore Power** is enabled on the Deployments panel.
3. Attempts to copy the deployment data to the standby server.
4. If IFM is unable to copy the deployment data, IFM backs out the changes to the backup server and selects the next server from the standby pool and retries.
5. Once the deployment data is successfully copied to the backup server, IFM attempts to copy VLAN data, if specified by the settings in the failover monitor.

Notes:

- To avoid a loss of data during a failover event, set up the standby pools to match the monitored pools.
- (IBM BladeCenter devices only) For failover to occur to a standby server, the standby server must be powered off, unless **Ignore Power** is enabled on the Deployments panel.
- (IBM Flex System devices only) You must provide the SNMV3 receiver IP address and the SNMV3 receiver password for the chassis. To define the values, select **Edit** on the Hardware Devices panel.

Configuring the management module to enable failover

You must configure the management module to send traps to the IFM server.

(IBM BladeCenter devices only) The IBM BladeCenter chassis requires Simple Network Management Protocol (SNMP) version 1 to be configured.

1. From the AMM interface access the **MM Control - Network Protocols** page.
2. Click on the **Simple Network Management Protocol (SNMP)** link and make sure that SNMP traps and SNMPv1 agent are enabled and configured.
3. Set the **Access Type** to **Trap** for at least one community.
4. Make sure that the IP address or hostname of the IFM server is listed as one of the three addresses for the community.
5. If the community is not named, define a name and set the **Community Name** to **Trap**.

(IBM Flex System devices only) To configure the IBM Flex System CMM to send traps, complete the following steps.

1. Enable SNMPv3 from the Management Module interface:
   a. Select **Network** from the **Mgt Module Management** menu.
   b. Click on the **SNMP** tab.
   c. Under **Simple Network Management Protocol (SNMP)**, select **Enable SNMPv3 Agent**.

   d. Click **Apply**.
2. Setup event recipients from the Management Module interface:
   a. Select **Event Recipients** from the **Events** menu.
   b. Click **Global Settings**.
   c. Select all options under **Critical Events**, **Warning Events**, and **Informational Events**.
   d. Click **OK**.

Recovering from a failover event

Before attempting to recover a failed server, you can prevent erroneous triggering events from occurring that invoke unnecessary failover events.

If the failover monitor has no other servers to actively monitor, you can pause the monitor and begin problem determination. If the failover monitor is monitoring other servers, move the server to a bay not being monitored. With the server in that bay, you can power on the server while investigating the condition, without causing a failover event.

Once the problem is resolved, power down the backup server and set **IFM Mode** to **Disabled** from the Hardware Devices panel. This prevents duplicate addresses from being configured in the event the standby server is powered on for reasons other than a subsequent failover attempt. Then, push the deployment data from the Deployments panel to the server.

Alternatively, you can perform a reverse failover from the backup server back to the repaired server. Select **Manual Failover** from the Hardware Devices panel. Define a standby pool that only contains the bay containing the repaired server to ensure failover will not attempt to use a different server. Specify the same failover settings that the failover monitor used.

Setting the out-of-band mode

This topic provides information about setting the out-of-band mode for servers that support both the `CMMPush` and `IFMPull` modes.

Use the `oobMode` property in the server.prop file to define the mode of operation for servers that support both the `CMMPush` mode and `IFMPull` mode. If the entry is not defined, the default mode is `CMMPush` mode.

With `IFMPull` mode, IFM sources block data from the IFM LDAP server. With `CMMPush` mode, the CMM or AMM pushes the IFM configuration to the server.

If the entry is `IFMPull` mode, IFM attempts first to enable `IFMPull` mode. If the attempt fails, IFM then attempts `CMMPush` mode. If the server is one device in a bay that contains two servers, only the `IFMPull` mode is attempted. If the attempt fails, the device is flagged as **Unavailable** on the Hardware Devices panel.

Chapter 3. Using IFM

This topic describes how to install, configure, and use IFM.

Configuration overview

This topic provides an overview of the steps to perform a typical IFM configuration.

To configure the typical IFM installation, complete the following steps.

1. Define the hardware in the configuration on the Hardware Devices panel.
2. Turn off all servers in the configuration.
3. Create hardware pools on the Hardware Pools panel. Hardware pools define the available hardware.
4. Create address pools or use the predefined address pools on the Address Pools panel. Address pools define the range of available MAC addresses.
5. Create a template or use the predefined templates on the Templates panel. A template is a set of data designed to describe a specific configuration within IFM. This data is generic in format and aids IFM in the configuration of the hardware endpoints. Templates are reusable across multiple profiles and deployments.
6. Create a profile on the Profiles panel. A profile groups generic data into a single entity. The profile associates templates, hardware pools, and address pools for the purpose of creating a deployment.
7. Deploy a profile through the Profiles panel. A deployment is specific information related to the chassis, servers, and ports included in the hardware pool. The generic information associated through the profile is reused as needed and assigned during the deployment process.
8. Edit the deployment (if necessary) through the Deployments panel.
9. Push the deployment to the hardware through the Deployments panel.
10. Turn on the servers.
11. View the results (it takes a few minutes for the results to become available after power on).
12. Create failover monitors. Failover monitors define the server events to be monitored and the criteria for selecting the standby hardware to activate in case of a failure.

Notes:

1. All servers must be powered off and IFM mode enabled from the Hardware Devices panel before an IFM template or data can be pushed.
2. For failover to occur to a standby server, the standby server must be powered off and IFM mode disabled from the Hardware Devices panel.

Installing IFM for Windows

To install IFM for Windows, complete the following steps.

Procedure

1. Download the IFM executable install file.

2. Using an account with either local or domain administrator privilege, log on to the operating system.
3. Double-click the IFM executable install file and follow the installation wizard instructions.

Installing IFM for Linux

To install IFM for Linux, complete the following steps.

Procedure

1. Download the IFM binary install file.
2. Run the binary file using root access and follow the installation wizard.

Starting IFM

To start IFM from a Windows or Linux operating system, complete the following steps.

Procedure

1. Double-click the Start IFM Server icon.
2. Alternately, navigate to the install directory and then with root or administrator privilege, run the **IfmServer** (**IfmServer.exe** on Windows) command.
3. Once the IFM server starts, enter `https://`*`server name`*`:8044/` to connect to the user interface. Where *server name* is the IFM server.

   Important: IFM is set initially with a user name of `USERID` and password of `PASSW0RD` (with a zero, not the letter O). After you start IFM for the first time, you must change the password. If you reuse `PASSW0RD` as the password, you must change it the next time you start IFM.

Stopping IFM

To stop IFM, complete the following steps.

1. Navigate to the IFM installation directory in a command prompt.
2. Run the **IfmServerStop** (**IFMServerStop.exe** on Windows) command.

Uninstalling IFM

To uninstall IFM, complete the following steps.

1. Navigate to the program shortcut.
2. Click the Uninstall IFM executable file.

Hardware devices

To add, delete, and manage hardware devices, complete the following steps.

Before you begin

The following notes describe information that you must consider when you add, delete, and manage hardware devices:

- The IP address can be any valid address in one of the following formats:

  IPv4 dotted notation (for example, 192.168.0.1)

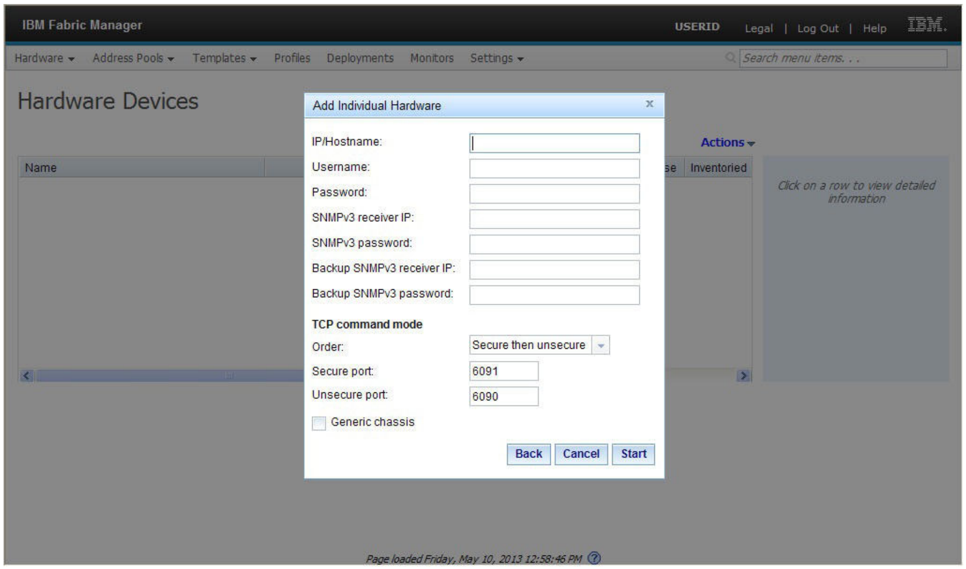
IPv6 hexadecimal notation (for example, FE80::3BA7:94FF:FE07:CBD0)

Human-readable Web addresses

- For larger installations, it is best practice to use human-readable addresses only if the domain-name-server (DNS) is on the local network. If the DNS is not local, the lookup time can slow the parsing substantially, especially if there is an error and the name is not found.

Procedure

1. Select **Hardware**; then select **Devices**. The summary view shows information about the hardware inventory. You can also select a line to view detailed information.



Add Individual Hardware

IP/Hostname:

Username:

Password:

SNMPv3 receiver IP:

SNMPv3 password:

Backup SNMPv3 receiver IP:

Backup SNMPv3 password:

TCP command mode

Order: Secure then unsecure

Secure port: 6091

Unsecure port: 6090

□ Generic chassis

Page loaded Friday, May 10, 2013 12:58:46 PM

License indicates if an enterprise activation key is active for the chassis.

Source shows the source of the data for programming ports on the network adapters. See "Setting the out-of-band mode" on page 17.

- **CMM:** For IBM Flex System devices, the information is from the CMM.
- **AMM:** For IBM BladeCenter devices, the information is from the AMM.
- **IFM:** The virtualization data is from the IFM LDAP server. To push deployments from bays that contain two servers, this value must be **IFM**.
- **CP:** (configuration patterns) The server was configured externally.
- **Unknown:** The mode definition failed.
- **Series of dots (...):** Source information does not apply to this device.

IFM Status shows the basic operating status of the devices. To view detailed results for individual ports, click the **IFM Status** field for the server. **IFM Status** is only available when **Power State** is **On** and **IFM Mode** is **Enabled**.

Table 8. IFM status

Power State	IFM Mode	IFM Status
Off	Disabled	Not available (N/A)
Off	Enabled	Not available (N/A)
On	Disabled	Not available (N/A)
On	Enabled	• **Normal:** The server is operating normally. • **Error:** An error has occurred. • **Pending:** The IFM Status is updating.

2. Select an action from the following choices:
   - **Toggle Power**

     Select this choice to toggle server power on and off.
   - **Toggle IFM Mode**

     Select this choice to change the mode for an individual server. Mode toggles between **Enabled** and **Disabled**. When you toggle **Disabled**, the system ignores all ports belonging to the bay. The **Disabled** choice is available only when power to the server is off.
   - **Manual Failover**

     Select this choice to force the failover process to start and transfer activity to a compatible blade in a standby pool. For failover to occur to a standby server, the standby server must be powered off, and **IFM Mode** set to **Disabled**. To allow greater flexibility, some settings might be ignored when finding a matching replacement standby server in the standby pool. Unlike the failover monitor, this selection triggers the failover without an inducing failover event.
   - **Add**

     Enter the userid and password of the management modules to begin the **Add** action.
     - **Add single chassis**

       Select this choice to add a chassis from a single IP address. Click **Generic chassis** to add the chassis to the database but not log in or gather inventory.
     - **Add a range of chassis**

       Select this choice to add a chassis from a range of IP addresses.
     - **Add chassis from file or URL**

       Select this choice to import IP addresses from a file or URL. A maximum of 100 IP addresses can be imported and any additional IP addresses are ignored without warning. The file must be a text file. You can enter only one valid IPv4 or IPv6 address per line.

     Enter the IP addresses or hostnames of the management modules for hardware device discovery.

     The following information applies only when using SNMPv3 with IBM BladeCenter blade servers or IBM Flex System compute nodes.
     - **SNMPv3 receiver IP** and **SNMPv3 receiver password** are the IP address and password of the primary recipient of the SNMPv3 traps and incoming LDAP connections. This applies to the managed servers using `IFMPull` mode.
     - **Backup SNMPv3 receiver IP** and **Backup SNMPv3 receiver password** are the IP address and password of the secondary recipient of the SNMPv3 traps and incoming LDAP connections. If a backup IFM instance is configured for high availability, you must define the backup SNMPv3 receiver IP address and password for proper redirection of SNMPv3 traps and LDAP connections to the new primary IFM server.

       Note: If a backup IFM instance is configured for high availability, you must define the primary and secondary SNMPv3 IP addresses and passwords to configure bays that contain two servers in one bay.

- The management module only sends one SNMPv3 trap to the most recent receiver IP address that registers to it; therefore, two IFM servers cannot monitor the same management module.
- You must add an SNMPv3 password to have the chassis monitored for failover events. The password must be at least 8 characters long. The SNMPv3 password is registered to the management module during failover monitor creation and can be different from the management module login password. Different management modules can use different SNMPv3 passwords, but it is not necessary that they are different.
- If the SNMPv3 password or IP receiver is added or changed, the change does not become effective until all monitors using it are removed or paused and then started.

Click **Next** to immediately log into the chassis and gather inventory. For the TCP Command Mode, specify the discovery order and the associated ports. A dialogue window opens and indicates the progress of the discovery process.

- **Edit**

  Select this choice to edit the chassis credentials.

- **Remove**

  Select this choice to remove the chassis and all associated servers from inventory.

- **Refresh**

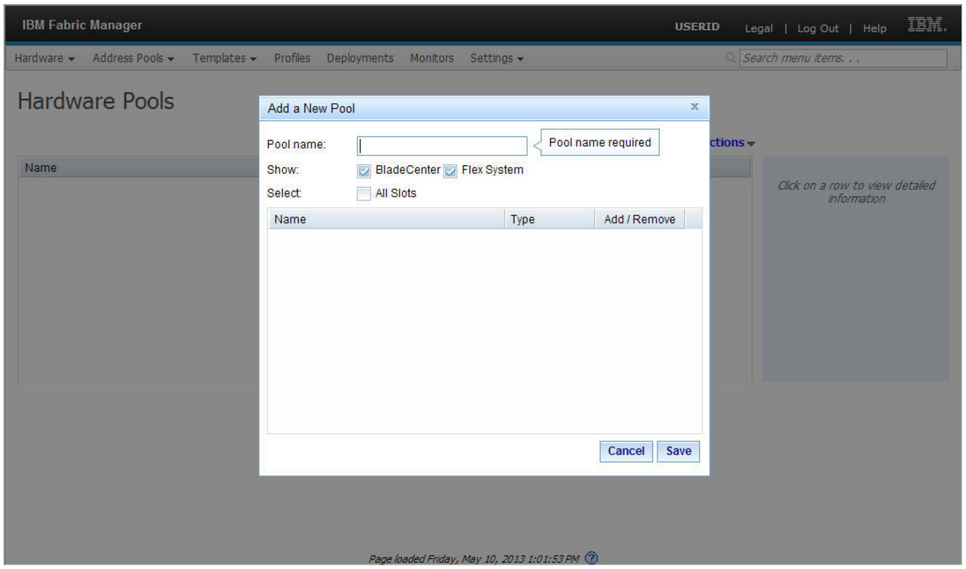
  Select this choice to collect and refresh the hardware inventory.

Hardware pools

To add, change, and remove a hardware pool, complete the following steps.

Procedure

1. Select **Hardware**; then select **Pools**. The summary view shows information about the hardware pools. You can also select a line to view detailed information.



Pool name:
Pool name required

Show: ☑ BladeCenter ☑ Flex System

Select: □ All Slots

Name	Type	Add / Remove

Page loaded Friday, May 10, 2013 1:01:53 PM

2. Select an action from the following choices:
   - **Add**

Select this choice to add a hardware pool. The hardware pools are bay based so you can add servers that are not yet present. You can expand a chassis to select the individual servers. You can also filter the chassis by IBM BladeCenter or IBM Flex System devices.

The maximum number of bays depends on the chassis model. You can only define a port for a bay that has already been defined with a bay entry. Attempting to define a port for an undefined bay results in an error.

- **Edit**

  Select this choice to edit the hardware pool.
- **Remove**

  Select this choice to remove a hardware pool.

Hardware tags

To add, edit, and remove a hardware tag, complete the following steps.

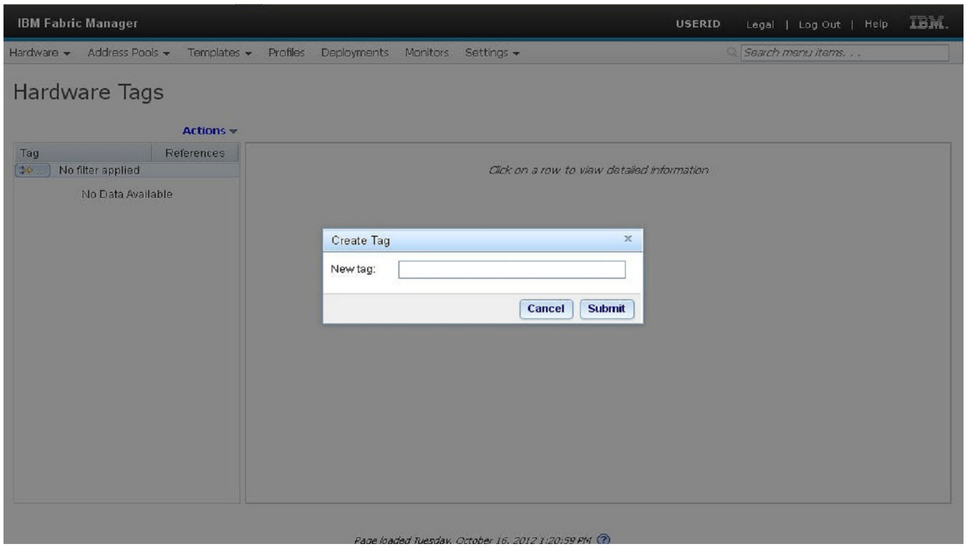
About this task

The following notes describe information that you must consider when you add, edit, or remove a hardware tag:

- A hardware tag is user-defined informational text that you can assign to one or more chassis or servers.
- You can assign one or more hardware tags to each device.
- During a failover operation, all hardware tags are assigned to the replacement server. Therefore, a hardware tag might not apply to the new server.

Procedure

1. Select **Hardware**; then select **Tags**. The summary view shows information about the hardware tags. You can also select a line to view detailed information.



Hardware Tags

Tag	References
No filter applied	
No Data Available	

Click on a row to view detailed information

Create Tag

New tag:

Page loaded Tuesday, October 16, 2012 1:20:59 PM

2. Select an action from the following choices:
   - **Add**

     Select this choice to add a hardware tag. Enter the text message and the reference numbers of the devices to which you want to assign the message. The reference number for each device is listed on the Hardware devices detailed panel.

- **Edit**

  Select this choice to edit the hardware tag.
- **Remove**

  Select this choice to remove the selected hardware tag. This action removes the hardware tag and all references to it.

Address pools

To add, edit, or remove an address pool, complete the following steps.

About this task

Attention: Duplication of MAC addresses can cause serious issues with your network. Fibre Channel address duplication can lead to data corruption, if more than one server is attempting to access the same volume at the same time.

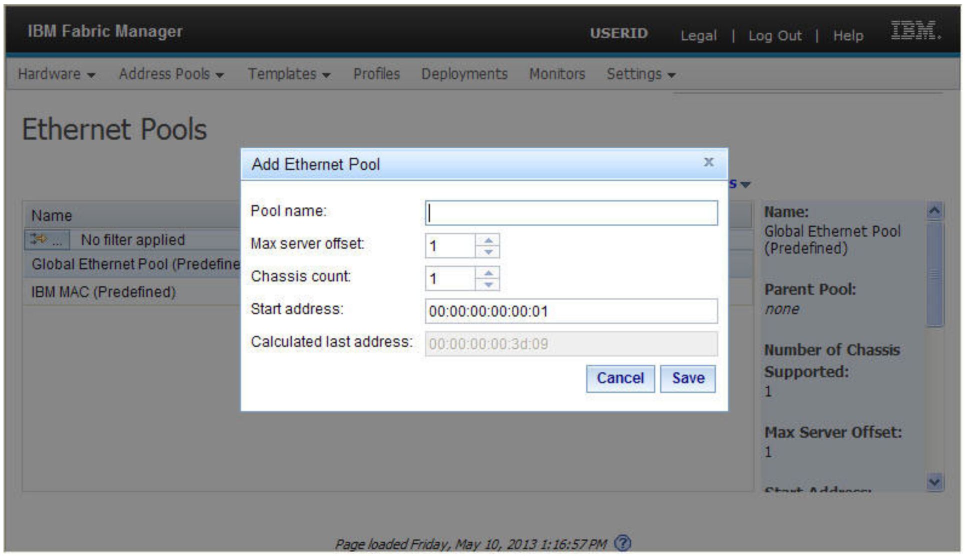
The following notes describe information that you must consider when you add, edit, or remove an address pool:

- Some applications check the adapter type and vendor using the address. You can select ranges that meet the requirements of the type of adapter that you are using. Each vendor has allocated a special range for IFM which guarantees that these addresses do not conflict with any previous or future burned-in addresses.
- For Fibre Channel addresses there are two ranges for each vendor: one for odd-numbered ports and one for even-numbered ports.

  Note: For some devices this might not be the appropriate allocation. For example, a Fibre Channel high speed adapter is connected to ports 6 and 8, which are both allocated out of the second range. This device might appear as two different devices rather then a single device.
- The worldwide node name (WWNN) is for a Fibre Channel device attached to the port. Not all applications require this value, and some adapters supply this value themselves by creating a number based on a transformation of the worldwide port name (WWPN).
- The WWPN is for Fibre Channel devices attached to the port. Invalid addresses result in an error and the line is ignored.

Procedure

1. Select **Address Pools**.



Pool name:

Max server offset: 1

Chassis count: 1

Start address: 00:00:00:00:00:01

Calculated last address: 00:00:00:00:3d:09

Name: Global Ethernet Pool (Predefined)

Parent Pool: *none*

Number of Chassis Supported: 1

Max Server Offset: 1

2. Select **Ethernet**, **Fibre Channel**, or **SAS**. The summary view shows information about the address pools. You can also select a line to view detailed information. IFM comes with several predefined read-only parent pools. A parent pool can have multiple child pools but all addresses within them must be unique. **Max Server Offset** is the maximum width of any server associated with the pool. This is a 0 indexed value. For single-bay servers this value is 0.
3. Select an action from the following choices:
   - **Add**

     Select this choice to add an address pool. You can select the default Ethernet ranges or create your own. When you create a new pool, the currently selected pool is used as the parent.
   - **Edit**

     Select this choice to edit the address pool.
   - **Remove**

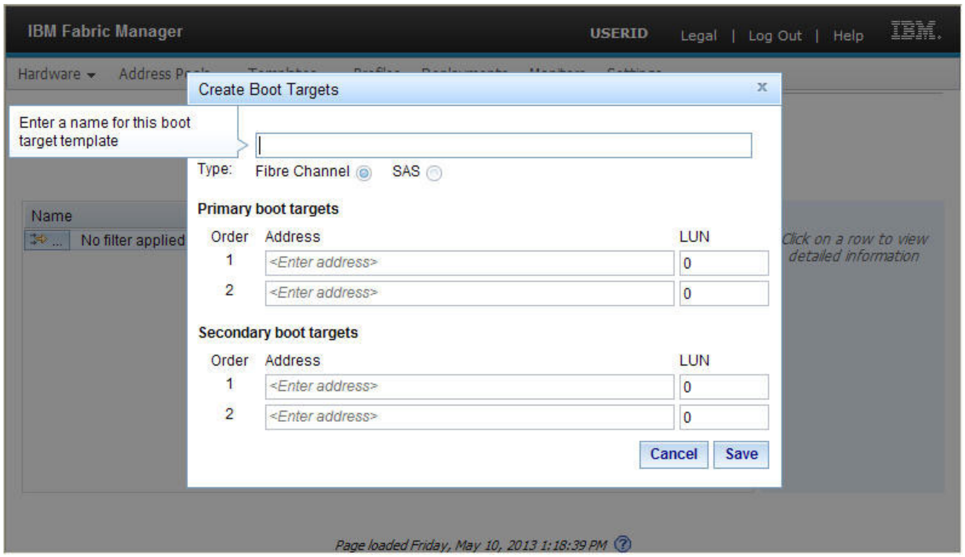
     Select this choice to remove the selected address pool.

Templates

To add, edit, and remove a boot target, chassis, and vNIC template, complete the following steps.

Procedure

1. Select **Templates**. The summary view shows information about the templates. You can also select a line to view detailed information.



Create Boot Targets

Enter a name for this boot target template

Type: Fibre Channel ● SAS ○

Primary boot targets

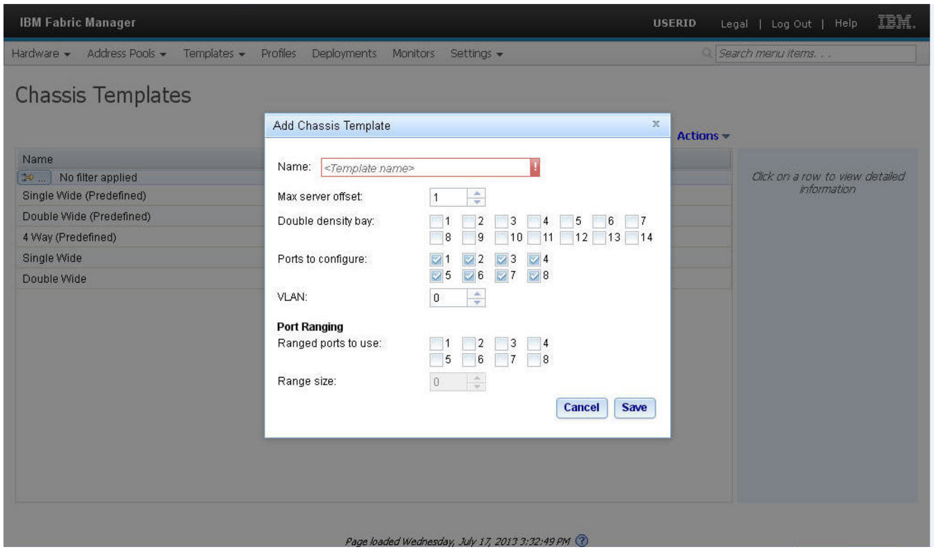
Order	Address	LUN
1	<Enter address>	0
2	<Enter address>	0

Secondary boot targets

Order	Address	LUN
1	<Enter address>	0
2	<Enter address>	0

2. Select a template from the following choices.
   - **Boot Target**

     Select this choice to add, edit, or remove the default primary and secondary boot target information. A single template can be applied to multiple profiles.



Add Chassis Template

Name: <Template name>

Max server offset: 1

Double density bay: □ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8 □ 9 □ 10 □ 11 □ 12 □ 13 □ 14

Ports to configure: ☑ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7 ☑ 8

VLAN: 0

Port Ranging

Ranged ports to use: □ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8

Range size: 0

   - **Chassis**

     Select this choice to add, edit, or remove the default chassis information. A single template can be applied to multiple profiles.

     Some Ethernet adapters can have a range of MAC addresses per port. The range is defined by specifying two MAC addresses per port: MAC A and MAC B. Enter a range size between 2 and 256. The default value is 16.

     Max Server Offset is the maximum width of any server associated with the pool. This is a 0 indexed value. For single-bay servers this value is 0. For two-bay servers this value is 1.

     VLAN is the generic VLAN address. This VLAN tag is used only by the UEFI for the PXE boot. You must apply OS VLAN tags at the OS level.

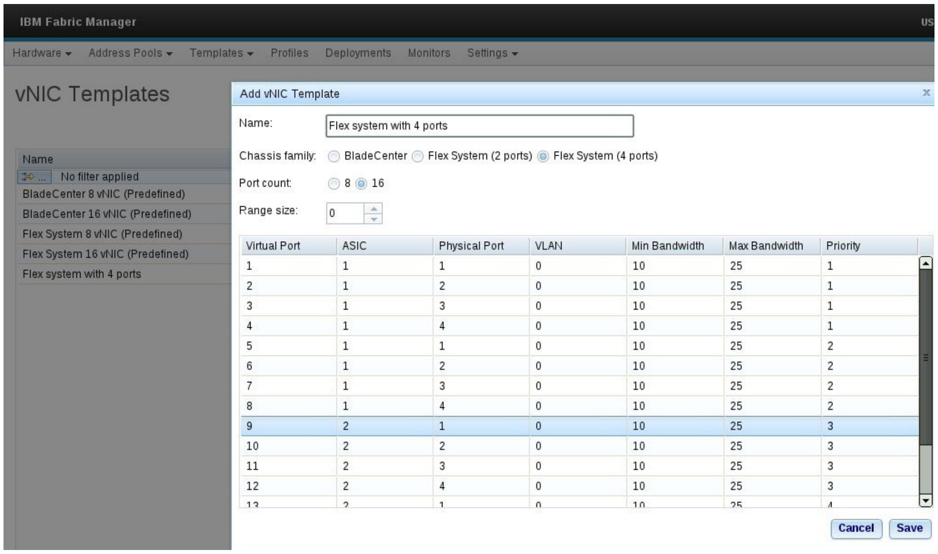
     Use **Double density bay** to define the bays that contain two servers in one bay.

Use **Ranged ports to use** to define the bays that can accept a range of addresses.

Range size defines the range size of MAC addresses. Enter a range size between 2 and 256.

- **vNIC**

  Select this choice to add, edit, or remove the default layout and QOS settings for the virtual NIC ports. A single template can be applied to multiple profiles.



Name
No filter applied
BladeCenter 8 vNIC (Predefined)
BladeCenter 16 vNIC (Predefined)
Flex System 8 vNIC (Predefined)
Flex System 16 vNIC (Predefined)
Flex system with 4 ports

Name: Flex system with 4 ports

Chassis family: ○ BladeCenter ○ Flex System (2 ports) ● Flex System (4 ports)

Port count: ○ 8 ● 16

Range size: 0

Virtual Port	ASIC	Physical Port	VLAN	Min Bandwidth	Max Bandwidth	Priority
1	1	1	0	10	25	1
2	1	2	0	10	25	1
3	1	3	0	10	25	1
4	1	4	0	10	25	1
5	1	1	0	10	25	2
6	1	2	0	10	25	2
7	1	3	0	10	25	2
8	1	4	0	10	25	2
9	2	1	0	10	25	3
10	2	2	0	10	25	3
11	2	3	0	10	25	3
12	2	4	0	10	25	3
13	2	1	0	10	25	4

  Min Bandwidth is the minimum bandwidth percentage associated with the virtual port. Minimum bandwidth must be smaller than the maximum bandwidth and must be at least 10. **Max Bandwidth** is the maximum bandwidth percentage associated with the virtual port. The total of the minimum bandwidth and maximum bandwidth must be 100.

  To define virtual ports requiring a MAC B assignment, specify a range size greater than 0. When the deployment is generated, the vNIC entries will contain MAC B assignments for each of the virtual ports based on the range size.

  Additionally, the port assignment order can be controlled by selecting **BladeCenter**, **Flex System (2 ports)**, or **Flex System (4 ports)** which will use the predetermined order in which the virtual ports are assigned to the physical ports. You can use this feature to select the layout to support the installed network cards.

3. Select an action from the following choices:

   - **Add**

     Select this choice to add a template.

   - **Edit**

     Select this choice to edit the template.

   - **Remove**

     Select this choice to remove the selected template.

Profiles

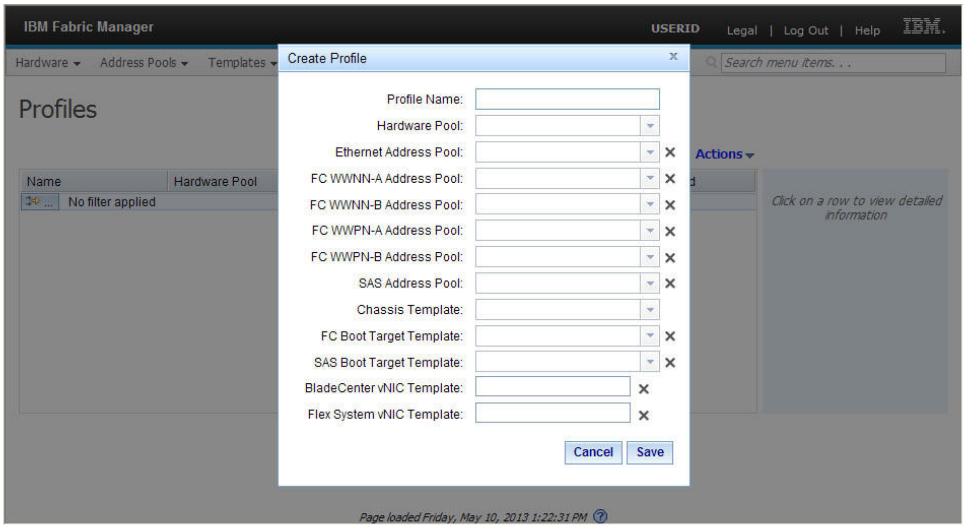
To add, edit, remove, and deploy a profile, complete the following steps.

Before you begin

By default, when you choose to assign MAC addresses, they are assigned for each port. These configurations match a single-bay server. They are generic configurations and contain a virtual address for each hardware type. As a result, when you change the type of server or adapter, you do not need to modify the configuration. To generate a configuration that assigns an address to a subset of the ports, you can edit the deployment and select which type of address to assign to each port.

Procedure

1. Select **Profiles**. The summary view shows information about the profiles. You can also select a line to view detailed information.



2. Select an action from the following choices:
   - **Add**

     Select this choice to add a profile. You select a hardware pool, address pool, chassis template, boot target template, and vNIC template for the profile. Optionally, you can select an IBM BladeCenter vNIC template or IBM Flex System vNIC template.
   - **Edit**

     Select this choice to edit the profile.
   - **Copy**

     Select this choice to copy the profile.
   - **Remove**

     Select this choice to remove the selected profile.
   - **Deploy**

     Select this choice to deploy the profile. Deployment translates the profile into port-specific information.

Deployments

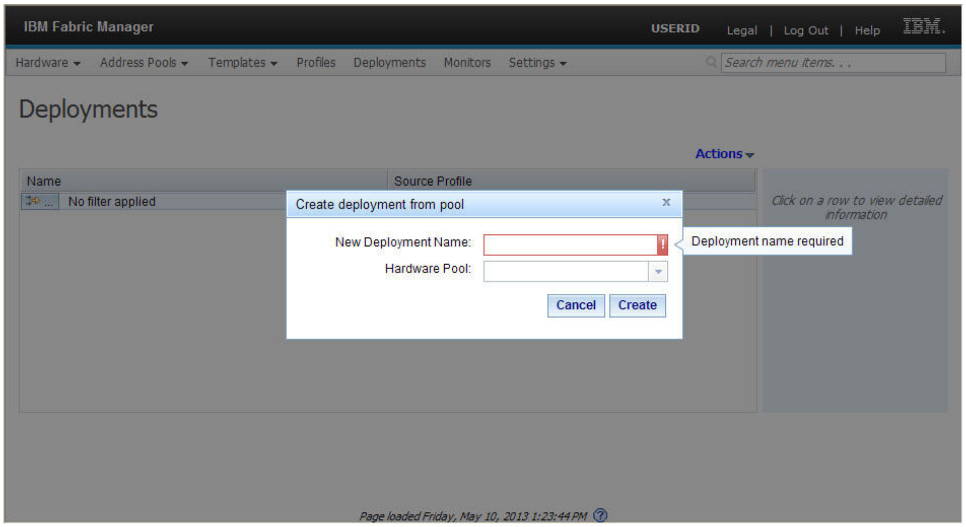
To edit, remove, and push a deployment, complete the following steps.

Procedure

1. Select **Deployments**. The summary view shows information about the deployments. Select a line to view detailed information.

   Boot order is the target the interface uses during the boot process.

   Deploying a profile creates port specific information from the generalized data associated with the profile. Any changes made to profile elements after deployment will not be reflected in an already created deployment. A new deployment would have to be made for changes to be reflected. The newly created deployment is displayed.



Create deployment from pool

New Deployment Name:

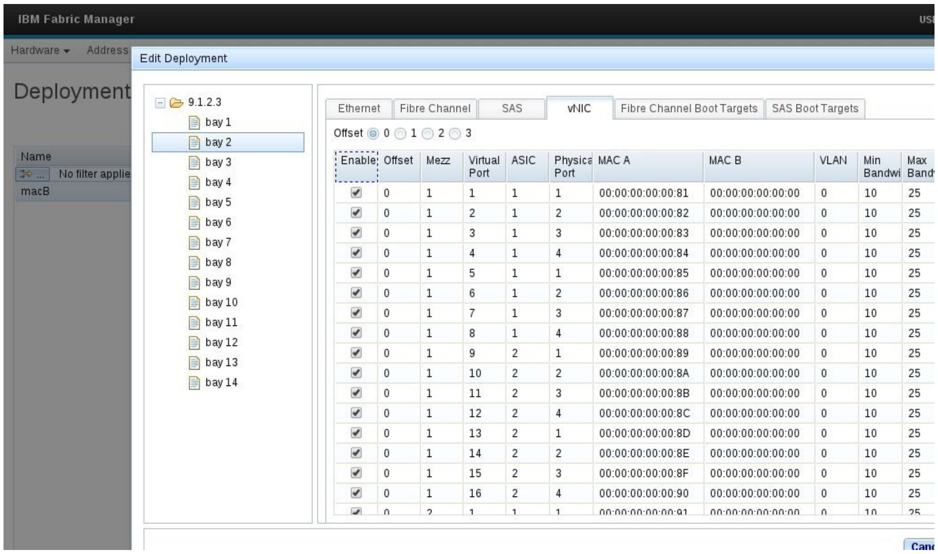
Hardware Pool:

Deployment name required

Page loaded Friday, May 10, 2013 1:23:44 PM

2. Select an action from the following choices:
   - **Edit**

     Select this choice to modify data associated with a deployment. You can select from a list of chassis and servers in the deployment. You can click on a specific server to edit the information on a per-port basis.



Edit Deployment

Offset ● 0 ○ 1 ○ 2 ○ 3

Enable	Offset	Mezz	Virtual Port	ASIC	Physica Port	MAC A	MAC B	VLAN	Min Bandwi	Max Band
☑	0	1	1	1	1	00:00:00:00:00:81	00:00:00:00:00:00	0	10	25
☑	0	1	2	1	2	00:00:00:00:00:82	00:00:00:00:00:00	0	10	25
☑	0	1	3	1	3	00:00:00:00:00:83	00:00:00:00:00:00	0	10	25
☑	0	1	4	1	4	00:00:00:00:00:84	00:00:00:00:00:00	0	10	25
☑	0	1	5	1	1	00:00:00:00:00:85	00:00:00:00:00:00	0	10	25
☑	0	1	6	1	2	00:00:00:00:00:86	00:00:00:00:00:00	0	10	25
☑	0	1	7	1	3	00:00:00:00:00:87	00:00:00:00:00:00	0	10	25
☑	0	1	8	1	4	00:00:00:00:00:88	00:00:00:00:00:00	0	10	25
☑	0	1	9	2	1	00:00:00:00:00:89	00:00:00:00:00:00	0	10	25
☑	0	1	10	2	2	00:00:00:00:00:8A	00:00:00:00:00:00	0	10	25
☑	0	1	11	2	3	00:00:00:00:00:8B	00:00:00:00:00:00	0	10	25
☑	0	1	12	2	4	00:00:00:00:00:8C	00:00:00:00:00:00	0	10	25
☑	0	1	13	2	1	00:00:00:00:00:8D	00:00:00:00:00:00	0	10	25
☑	0	1	14	2	2	00:00:00:00:00:8E	00:00:00:00:00:00	0	10	25
☑	0	1	15	2	3	00:00:00:00:00:8F	00:00:00:00:00:00	0	10	25
☑	0	1	16	2	4	00:00:00:00:00:90	00:00:00:00:00:00	0	10	25
☑	0	2	1	1	1	00:00:00:00:00:91	00:00:00:00:00:00	0	10	25

   - **Remove**

     Select this choice to remove the selected profile.

   - **Push**

Select this choice to communicate the deployment to the port-specific hardware. If the communication fails, the endpoint hardware is skipped but IFM continues to push the deployment to the other hardware endpoints.

If the target hardware does not support the full IFM data set, IFM will cater the data to match the hardware.

The device must be powered off for the deployment change to take effect. This process takes some time, and cannot be canceled once it has started.

During the push process, pre-deployment actions are available.

- **Enable**

  Select this choice to enable all nodes in the chassis that are powered on to use the new deployment profile. You can also enable nodes individually.
- **Disable**

  Select this choice to cause IFM to ignore all ports belonging to the bay. You can also disable nodes individually.
- **Ignore**

  Select this choice to continue using current deployment information and ignore the new deployment information.
- **Ignore Power**

  Select this choice to attempt deployment regardless of the power state.
- **Compare with current data**

  Select this choice to compare the new data changes with a read-only view of the current data that the device is using. The current data is called harvested data. You can review the harvested data and modify the new data before communicating the deployment to the port-specific hardware.

- **Create**

  Select this choice to bypass a deployment configuration and use the current data that the device is already using.
- **Import**

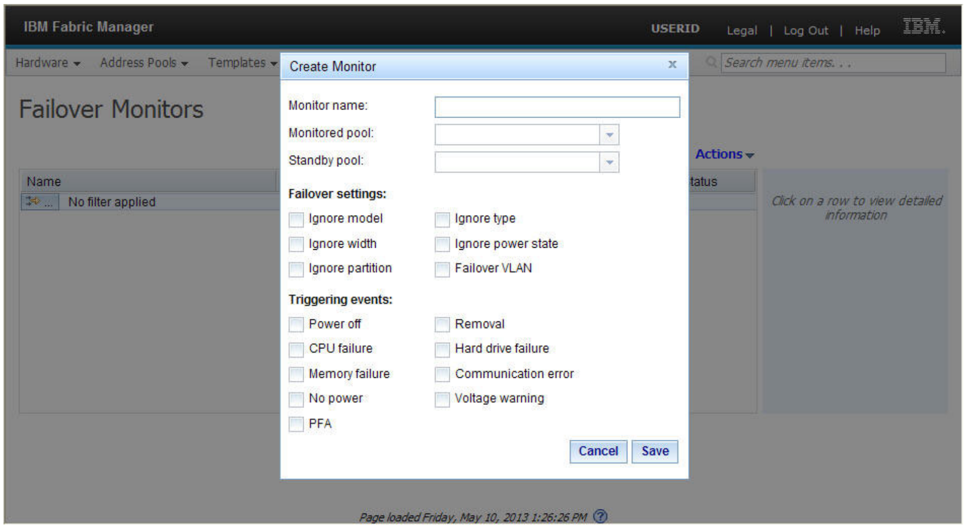
  Select this choice to bypass a deployment configuration and use a pre-existing comma separated value (CSV) configuration file.

Failover monitors

Failover monitoring allows you to select events to monitor and automatically enact server failover when an event occurs. You also select a standby pool. The types of events which can be monitored include server loss of power and hard drive failure. When failover occurs, activity is transferred to a compatible server in the standby pool. To add, edit, remove, start, and pause a failover monitor, complete the following steps.

Procedure

1. Select **Monitors**. The summary view shows information about the failover monitor. You can also select a failover monitor to view detailed information.



Create Monitor

Monitor name:
Monitored pool:
Standby pool:

Failover settings:

□ Ignore model □ Ignore type
□ Ignore width □ Ignore power state
□ Ignore partition □ Failover VLAN

Triggering events:

□ Power off □ Removal
□ CPU failure □ Hard drive failure
□ Memory failure □ Communication error
□ No power □ Voltage warning
□ PFA

Cancel Save

2. Select an action from the following choices:
   - **Add**

     Select this choice to add a failover monitor configuration. You select the failover settings that define the failover servers and select the triggering events to be monitored.

     Select **Failover VLAN** under **Failover settings** to add the standby bay Ethernet port to the VLAN when a failover occurs. The failover operation does not add the Port VLAN ID (PVID) settings.
   - **Edit**

     Select this choice to edit the failover monitor configuration.
   - **Remove**

     Select this choice to remove the selected failover monitor configuration.
   - **Start**

     Select this choice to start monitoring using the configuration. IFM monitors the hardware in the pool for events and performs a failover should an event occur.
   - **Pause**

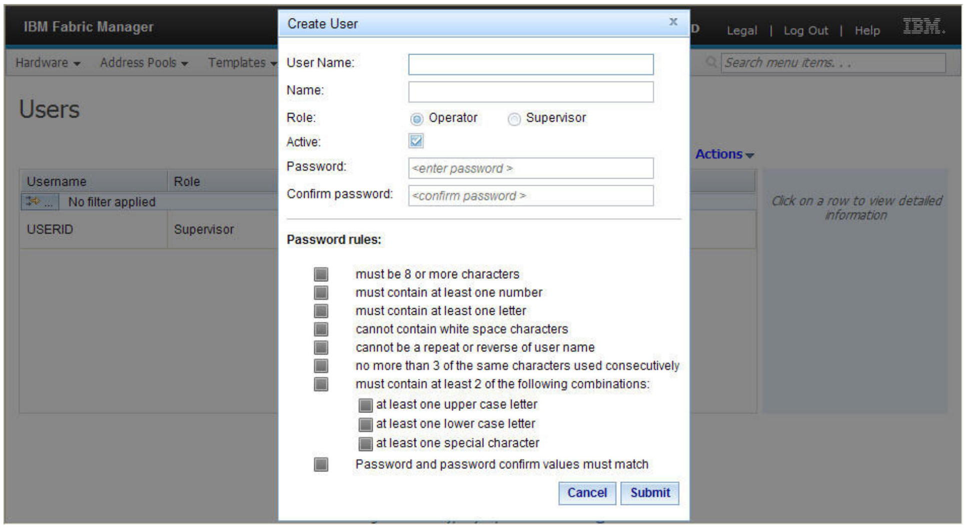
     Select this choice to pause monitoring using the configuration.

Users

To add, edit, and remove a user account, complete the following steps.

Procedure

1. Select **Settings**; then select **Users**. The summary view shows information about the user accounts. You can also select a line to view detailed information.



Username	Role
No filter applied	
USERID	Supervisor

Create User

User Name:

Name:

Role: ● Operator ○ Supervisor

Active: ☑

Password: <enter password >

Confirm password: <confirm password >

Password rules:

- ■ must be 8 or more characters
- ■ must contain at least one number
- ■ must contain at least one letter
- ■ cannot contain white space characters
- ■ cannot be a repeat or reverse of user name
- ■ no more than 3 of the same characters used consecutively
- ■ must contain at least 2 of the following combinations:
  - ■ at least one upper case letter
  - ■ at least one lower case letter
  - ■ at least one special character
- ■ Password and password confirm values must match

Cancel Submit

2. Select an action from the following choices:
   - **Add**

     Select this choice to add a user account. You define the role (read-only access or read/write access) and also define the password for the user account.
   - **Edit**

     Select this choice to edit the user account. Only a user account with read/write access can edit another user account.
   - **Change Password**

     Select this choice to edit the password for the user account.
   - **Remove**

     Select this choice to remove the selected user account. Only a user account with read/write access can remove another user account.

     Notes:
     - If you remove the last user account with read/write access, IFM creates a default user account with read/write access the next time it starts.
     - If you remove the last user account with any level of access, IFM becomes immediately unauthenticated.

Activation key

For all of the functions in IFM to be available, each chassis must be licensed for use with IFM. Rather than applying hundreds of licenses to the system individually, you can add a single IBM Feature On Demand (FoD) activation key to IFM.

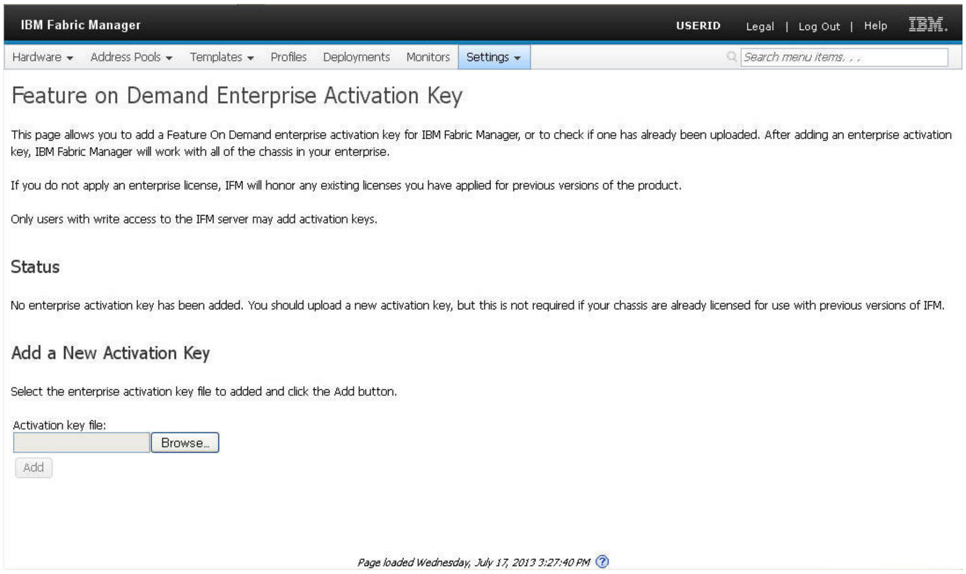
Before you begin

Go to http://www.ibm.com/systems/x/fod/ to request and download an activation key for IFM through the Feature on Demand (FoD) web site.

To add the activation key to IFM, complete the following steps.

Procedure

1. Click **Settings** in the IFM navigation bar and select **Activation Keys**.



Feature on Demand Enterprise Activation Key

This page allows you to add a Feature On Demand enterprise activation key for IBM Fabric Manager, or to check if one has already been uploaded. After adding an enterprise activation key, IBM Fabric Manager will work with all of the chassis in your enterprise.

If you do not apply an enterprise license, IFM will honor any existing licenses you have applied for previous versions of the product.

Only users with write access to the IFM server may add activation keys.

Status

No enterprise activation key has been added. You should upload a new activation key, but this is not required if your chassis are already licensed for use with previous versions of IFM.

Add a New Activation Key

Select the enterprise activation key file to added and click the Add button.

Activation key file:

Page loaded Wednesday, July 17, 2013 3:27:40 PM

2. Click **Browse** and select the activation key file.
3. Click **Add**.

Results

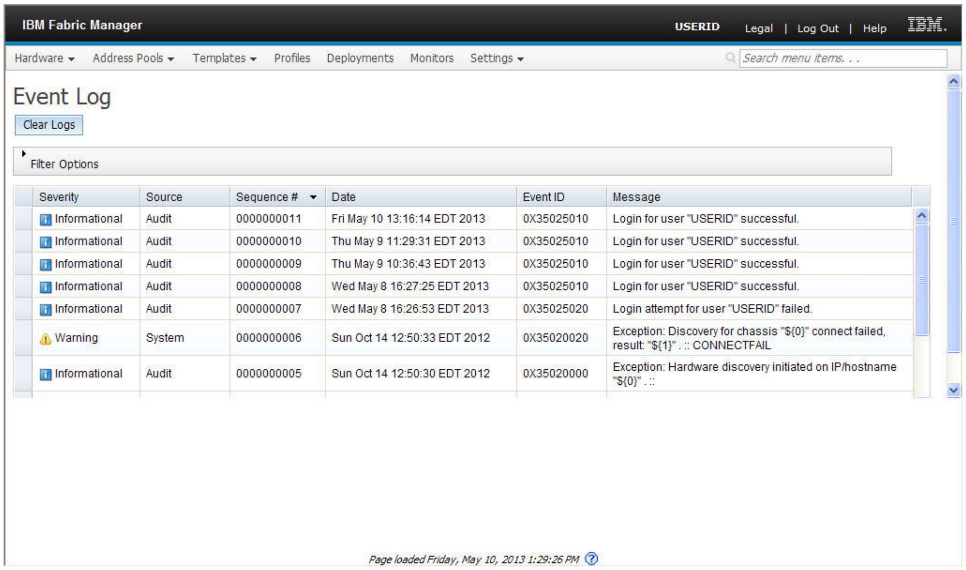
After you add an activation key, any chassis discovered through the Hardware Devices panel indicates with a checkmark in the License column that all of the IFM functionality is enabled for the chassis.

Event log

The event log contains all system-generated events and user-generated events. To view and manage audit and system generated line items on the event log, complete the following steps.

Procedure

1. Select **Settings**; then select **Logs**. The summary view shows information about the events. You can also select a line to view detailed information.



Event Log

Severity	Source	Sequence #	Date	Event ID	Message
Informational	Audit	0000000011	Fri May 10 13:16:14 EDT 2013	0X35025010	Login for user "USERID" successful.
Informational	Audit	0000000010	Thu May 9 11:29:31 EDT 2013	0X35025010	Login for user "USERID" successful.
Informational	Audit	0000000009	Thu May 9 10:36:43 EDT 2013	0X35025010	Login for user "USERID" successful.
Informational	Audit	0000000008	Wed May 8 16:27:25 EDT 2013	0X35025010	Login for user "USERID" successful.
Informational	Audit	0000000007	Wed May 8 16:26:53 EDT 2013	0X35025020	Login attempt for user "USERID" failed.
Warning	System	0000000006	Sun Oct 14 12:50:33 EDT 2012	0X35020020	Exception: Discovery for chassis "${0}" connect failed, result: "${1}" . :: CONNECTFAIL
Informational	Audit	0000000005	Sun Oct 14 12:50:30 EDT 2012	0X35020000	Exception: Hardware discovery initiated on IP/hostname "${0}" . ::

Page loaded Friday, May 10, 2013 1:29:26 PM

2. View the following information:
   - **Severity**

     An indication of the level of concern for the event. The following severities can be displayed:
     - **Critical:** The event is a failure or critical condition that impairs service or an expected function.
     - **Warning:** The event is not as severe as an error, but if possible, the condition should be corrected before it becomes an error.
     - **Informational:** The event was recorded for audit purposes.
   - **Source**

     This value is in one of the following categories:
     - **Audit:** The event is the result of a user activity.
     - **System:** The event is the result of any system-generated event.
   - **Sequence**

     The order in which the events are created.
   - **Date**

     The time and date the event was generated.
   - **Event ID**

     A hexadecimal identifier that uniquely identifies an event. You can also select an event ID to view detailed information.
   - **Message**

     The logged message string that appears for an event.
3. Select an action from the following choices:
   - **Clear Logs**

     Select this choice to clear the summary view of all events. The sequence number is not affected.
   - **Filter Options**

     Select this choice to customize the summary view. You can select the information for the events to display.

Security configuration

To upload and install a security configuration, complete the following steps.

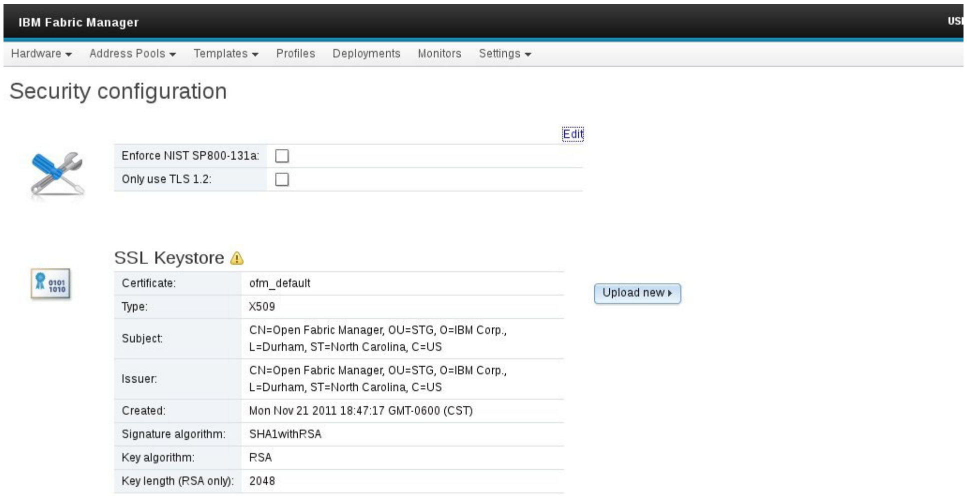
About this task

IFM supports the use of secure sockets layer (SSL) to provide a secure communication method to access IFM from a web browser. A default SSL configuration comes with IFM for use during installation and testing. Use this panel to upload an installation-specific configuration for use during normal operation.

You can also use this panel to edit and save National Institute of Standards and Technology (NIST) and Transport Layer Security (TLS) security settings. Click **Edit** and select the security setting. If you select NIST, TLS is disabled. To use TLS, you must restart the compute node.

Procedure

1. Click **Settings** in the IFM navigation bar and select **Security**.



Security configuration

Enforce NIST SP800-131a:	□
Only use TLS 1.2:	□

SSL Keystore ⚠

Certificate:	ofm_default
Type:	X509
Subject:	CN=Open Fabric Manager, OU=STG, O=IBM Corp., L=Durham, ST=North Carolina, C=US
Issuer:	CN=Open Fabric Manager, OU=STG, O=IBM Corp., L=Durham, ST=North Carolina, C=US
Created:	Mon Nov 21 2011 18:47:17 GMT-0600 (CST)
Signature algorithm:	SHA1withRSA
Key algorithm:	RSA
Key length (RSA only):	2048

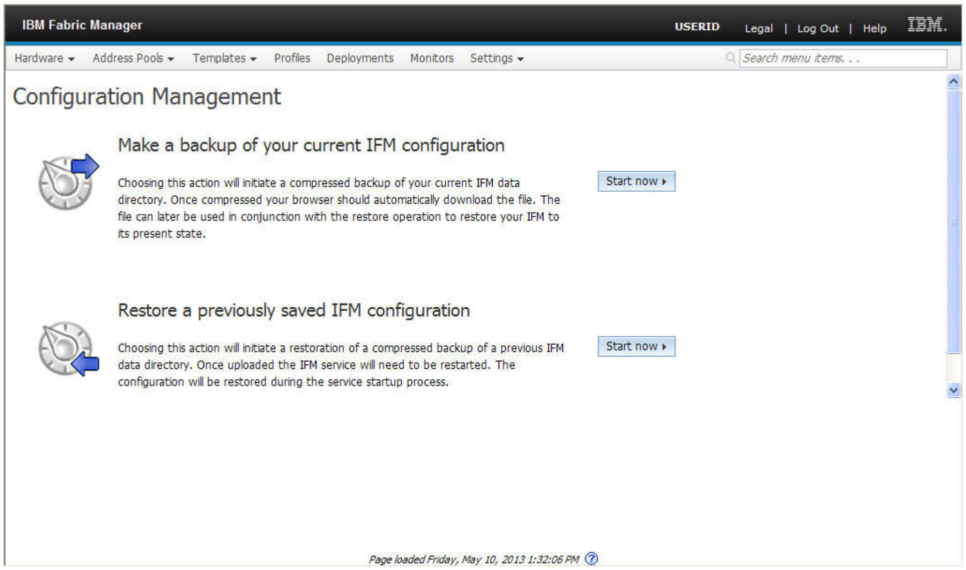
2. Click **Upload new**.
3. Click **Browse** and select the activation file.
4. If required, enter the **Keystore password**.
5. Click **Upload**.

Configuration management

To make a backup of the IFM configuration or restore a previously stored configuration, complete the following steps.

Procedure

1. Select **Settings**; then select **Backup & Restore**.



Configuration Management

Make a backup of your current IFM configuration

Choosing this action will initiate a compressed backup of your current IFM data directory. Once compressed your browser should automatically download the file. The file can later be used in conjunction with the restore operation to restore your IFM to its present state.

Restore a previously saved IFM configuration

Choosing this action will initiate a restoration of a compressed backup of a previous IFM data directory. Once uploaded the IFM service will need to be restarted. The configuration will be restored during the service startup process.

Page loaded Friday, May 10, 2013 1:32:06 PM

2. Select an action from the following choices:
   - **Make a backup of your current IFM configuration**

     Select **Start now** to make a backup of your current IFM configuration. Follow the instructions on the panel to proceed.
   - **Restore a previously saved IFM configuration**

     Select **Start now** to restore a previously saved IFM configuration. Follow the instructions on the panel to proceed.

High-availability configuration

IFM runs on a primary server. You can configure another server running IFM to be a secondary server. The secondary server monitors the health of the primary server and replaces it, if the primary server fails.

About this task

The secondary server monitors the primary server by periodically requesting a copy of the IFM data from the primary server. If the copy cannot be obtained because the primary server fails or a network connectivity failure occurrs, the secondary server starts as the primary IFM server, and is configured using the last copy of the data received from the primary server. The secondary server must have at least one copy of the IFM data, otherwise it will start as a new IFM server, with no data copied from the primary IFM server.

Note:

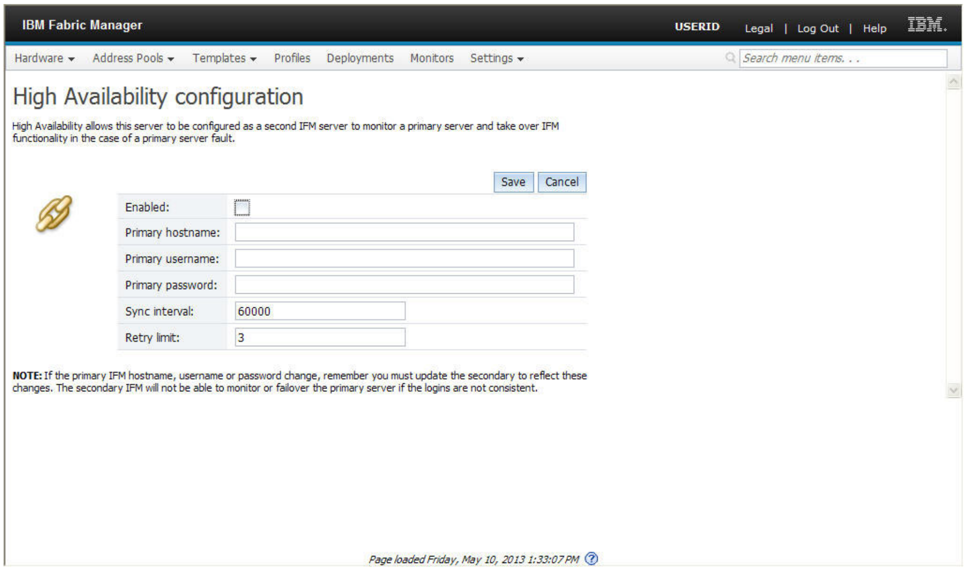
- If you make changes to the high-availability configuration, you must stop and restart the server to apply the changes.
- If a secondary server replaces the failed primary server, a data discrepancy might exist between the secondary server and primary server. How much of a discrepancy depends on the length of time between the last copy received and when the failover occurred.

- If the primary IFM hostname, username or password changes, you must update the secondary server to reflect these changes. The secondary IFM does not monitor or failover the primary server if the IFM hostname, username or password do not match.
- If you enable a server as a secondary server, a primary server must also exist.

To define a secondary IFM server for high availability, complete the following steps.

Procedure

1. Select **Settings**; then select **High Availability**.



High Availability configuration

High Availability allows this server to be configured as a second IFM server to monitor a primary server and take over IFM functionality in the case of a primary server fault.

Enabled:	□
Primary hostname:	
Primary username:	
Primary password:	
Sync interval:	60000
Retry limit:	3

NOTE: If the primary IFM hostname, username or password change, remember you must update the secondary to reflect these changes. The secondary IFM will not be able to monitor or failover the primary server if the logins are not consistent.

Page loaded Friday, May 10, 2013 1:33:07 PM

2. Select **Edit** to change the information.
   - **Enabled**

     Select this choice to define the server as a secondary IFM instance.
   - **Primary hostname**

     The IP address of the primary server that the secondary server is replacing.
   - **Primary username**

     The primary server user name.
   - **Primary password**

     The primary server password.
   - **Sync interval**

     The number of milliseconds before contacting the primary server.
   - **Retry limit**

     The maximum number of attempts made to contact the primary server.

Chapter 4. Configuring the IBM Flex System CN4022 2-Port Adapter

(IBM Flex System devices only) This topic provides information about configuring the IBM Flex System CN4022 2-Port Adapter.

To configure the IBM Flex System CN4022 2-Port Adapter for use in IFM, define the virtualization mode through the UEFI utility. Two virtualization modes are available:

- pNIC - The adapter displays the physical characteristics of the ports through the uEFI utility.
- vNIC - The adapter displays the virtual characteristics of the adapter through the uEFI utility.

pNIC virtual mode

(IBM Flex System devices only) The following topic provides information about the pNIC virtual mode.

About this task

In pNIC virtual mode the IBM Flex System CN4022 2-Port Adapter shows the physical characteristics of the adapter through the uEFI utility. The adapter contains two physical ports with the Ethernet, iSCSI offload and FCoE offload personalities automatically enabled. Each port has one MAC (Ethernet) address, one MAC (iSCSI) address, and one WWN (Fibre Channel) address. The MAC addresses have factory default values that can be changed.

Procedure

To configure the IBM Flex System CN4022 2-Port Adapter for use in IFM using the pNIC virtualization mode, complete the following steps:

1. From the uEFI utility, select **System Settings** > **Network** and select the port to configure.
2. Select the pNIC virtualization mode from the Main Configuration Page.

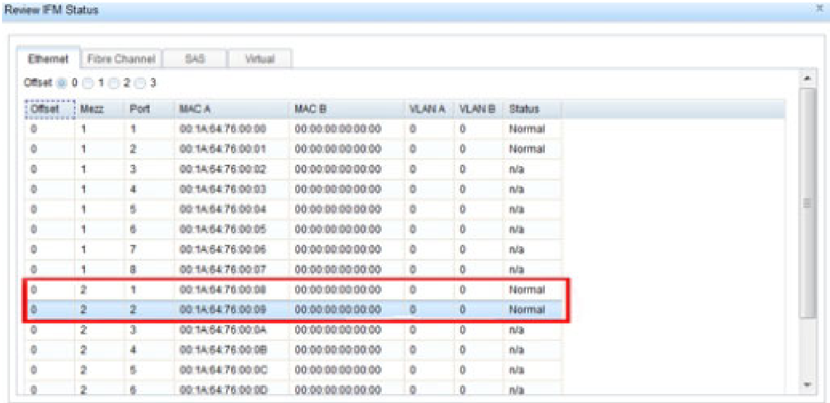
   The **Permanent MAC Address** is the same for each port. After IFM is applied, the **Virtual MAC Address** is different for each port and is used by the adapter and the device drivers in the OS.
3. Use the information in “Profiles” on page 28 to apply an IFM pattern to the IBM Flex System CN4022 2-Port Adapter.

What to do next

Optionally, you can verify the configuration of the adapter through the uEFI utility, IFM, and the CMM CLI mode.

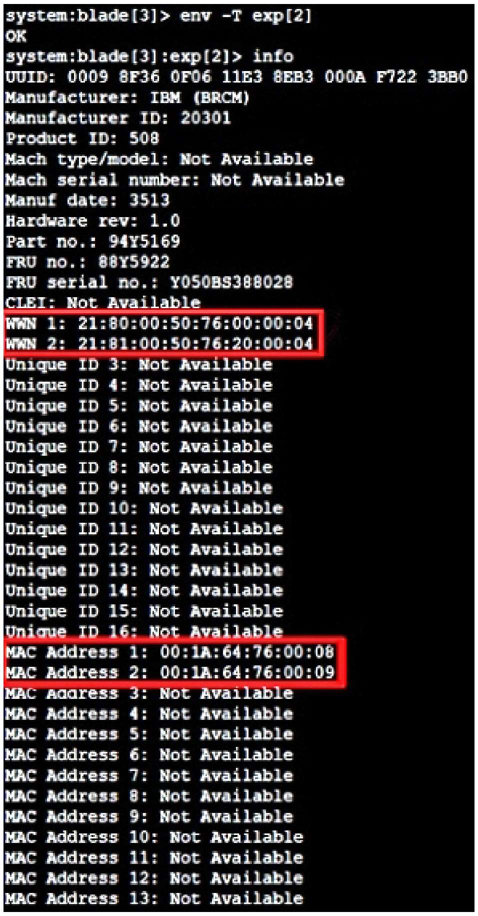
1. Verify that the adapter uses the new addresses from the IFM configuration. The compute node has a new virtual MAC address on the Main Configuration Page.
2. Verify that IFM reflects the address consumption. The adapter is inserted in Mezz 2, and has 2 ports. Both Port 1 and Port 2 have Normal status, which

means the ports consumed the new addresses.



Offset	Mezz	Port	MAC A	MAC B	VLAN A	VLAN B	Status
0	1	1	00:1A:64:76:00:00	00:00:00:00:00:00	0	0	Normal
0	1	2	00:1A:64:76:00:01	00:00:00:00:00:00	0	0	Normal
0	1	3	00:1A:64:76:00:02	00:00:00:00:00:00	0	0	n/a
0	1	4	00:1A:64:76:00:03	00:00:00:00:00:00	0	0	n/a
0	1	5	00:1A:64:76:00:04	00:00:00:00:00:00	0	0	n/a
0	1	6	00:1A:64:76:00:05	00:00:00:00:00:00	0	0	n/a
0	1	7	00:1A:64:76:00:06	00:00:00:00:00:00	0	0	n/a
0	1	8	00:1A:64:76:00:07	00:00:00:00:00:00	0	0	n/a
0	2	1	00:1A:64:76:00:08	00:00:00:00:00:00	0	0	Normal
0	2	2	00:1A:64:76:00:09	00:00:00:00:00:00	0	0	Normal
0	2	3	00:1A:64:76:00:0A	00:00:00:00:00:00	0	0	n/a
0	2	4	00:1A:64:76:00:0B	00:00:00:00:00:00	0	0	n/a
0	2	5	00:1A:64:76:00:0C	00:00:00:00:00:00	0	0	n/a
0	2	6	00:1A:64:76:00:0D	00:00:00:00:00:00	0	0	n/a

3. To verify Fibre Channel consumption from the uEFI utility, go to the Main Configuration Page for the port. To verify Fibre Channel consumption through IFM, see “Hardware devices” on page 20.
4. You can verify the address consumption through the CMM CLI mode.



```
system:blade[3]> env -T exp[2]
OK
system:blade[3]:exp[2]> info
UUID: 0009 8F36 0F06 11E3 8EB3 000A F722 3BB0
Manufacturer: IBM (BRCM)
Manufacturer ID: 20301
Product ID: 508
Mach type/model: Not Available
Mach serial number: Not Available
Manuf date: 3513
Hardware rev: 1.0
Part no.: 94Y5169
FRU no.: 88Y5922
FRU serial no.: Y050BS388028
CLEI: Not Available
WWN 1: 21:80:00:50:76:00:00:04
WWN 2: 21:81:00:50:76:20:00:04
Unique ID 3: Not Available
Unique ID 4: Not Available
Unique ID 5: Not Available
Unique ID 6: Not Available
Unique ID 7: Not Available
Unique ID 8: Not Available
Unique ID 9: Not Available
Unique ID 10: Not Available
Unique ID 11: Not Available
Unique ID 12: Not Available
Unique ID 13: Not Available
Unique ID 14: Not Available
Unique ID 15: Not Available
Unique ID 16: Not Available
MAC Address 1: 00:1A:64:76:00:08
MAC Address 2: 00:1A:64:76:00:09
MAC Address 3: Not Available
MAC Address 4: Not Available
MAC Address 5: Not Available
MAC Address 6: Not Available
MAC Address 7: Not Available
MAC Address 8: Not Available
MAC Address 9: Not Available
MAC Address 10: Not Available
MAC Address 11: Not Available
MAC Address 12: Not Available
MAC Address 13: Not Available
```

vNIC virtual mode

(IBM Flex System devices only) The following topic provides information about the vNIC virtual mode.

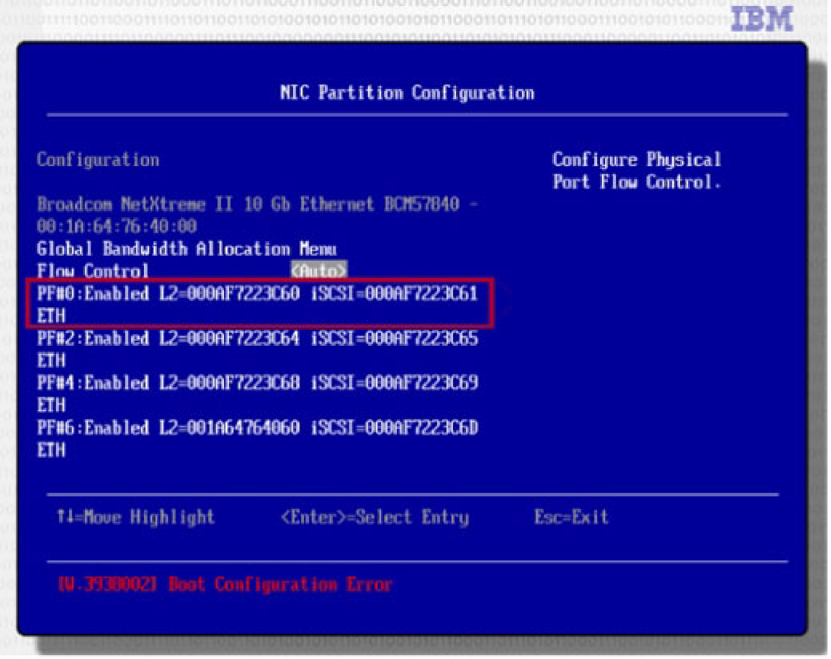
About this task

In vNIC virtual mode the IBM Flex System CN4022 2-Port Adapter shows the virtual characteristics of the adapter. The adapter supports four virtual ports. Each port can be configured for personalities of Ethernet, iSCSI offload, and FCoE offload. Because the adapter has two physical ports, you can have a maximum of eight Ethernet ports and four storage offload personalities. These are all virtual. The default is for eight Ethernet ports to be enabled and all storage offloads to be disabled. Each of these are enabled or disabled for each virtual port through the uEFI utility.

Procedure

To configure the IBM Flex System CN4022 2-Port Adapter for vNIC virtual mode, complete the following steps:

1. From the uEFI utility, select **System Settings** > **Network** and select the port.
2. To set all ports to Ethernet, and configure eight virtual Ethernet ports, complete the following steps:
   a. Access the NIC Partition Configuration Page from the Main Configuration Page.

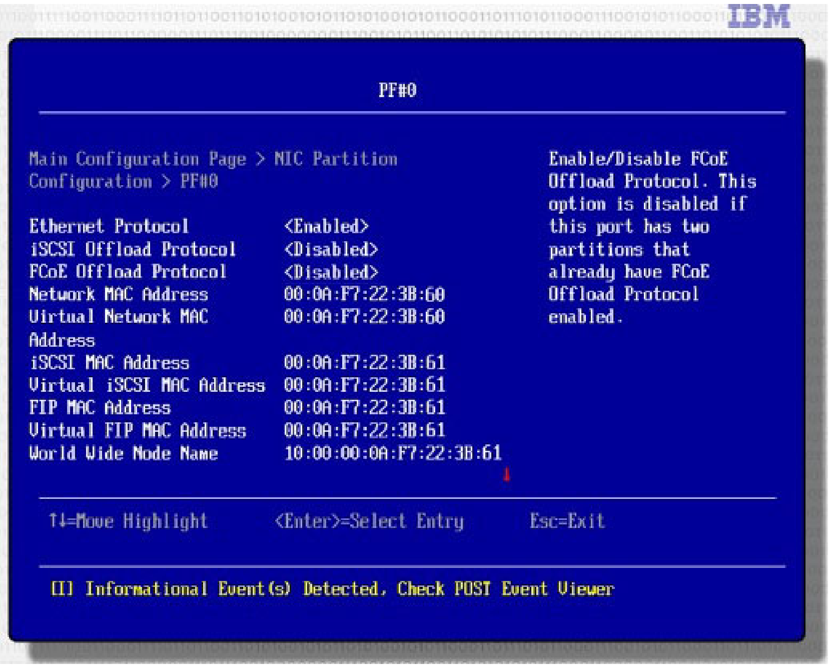


```
                         NIC Partition Configuration

Configuration                                          Configure Physical
                                                       Port Flow Control.
Broadcom NetXtreme II 10 Gb Ethernet BCM57840 -
00:1A:64:76:40:00
Global Bandwidth Allocation Menu
Flow Control                     <Auto>
PF#0:Enabled L2=000AF7223C60 iSCSI=000AF7223C61
ETH
PF#2:Enabled L2=000AF7223C64 iSCSI=000AF7223C65
ETH
PF#4:Enabled L2=000AF7223C68 iSCSI=000AF7223C69
ETH
PF#6:Enabled L2=001A64764060 iSCSI=000AF7223C6D
ETH

  ↑↓=Move Highlight       <Enter>=Select Entry       Esc=Exit

  [W.39300021 Boot Configuration Error
```

Each physical port has four PCI functions (PFs) which are set to Ethernet mode (ETH). The PCI function index represents the index of the virtual port of the adapter. The physical port 1 has the even index values: 0, 2, 4, and 6 (zero indexed). The physical port 2 has odd index values: 1, 3, 5, and 7.

Notes:
- All modes can be disabled.
- Only one Fibre Channel mode can be enabled per physical PHY port.
- You can enable one or two iSCSI modes per physical port.
- One FCoE mode and one iSCSI mode can be enabled per physical port.

   b. Select PF#0 to view the details of the virtual port.



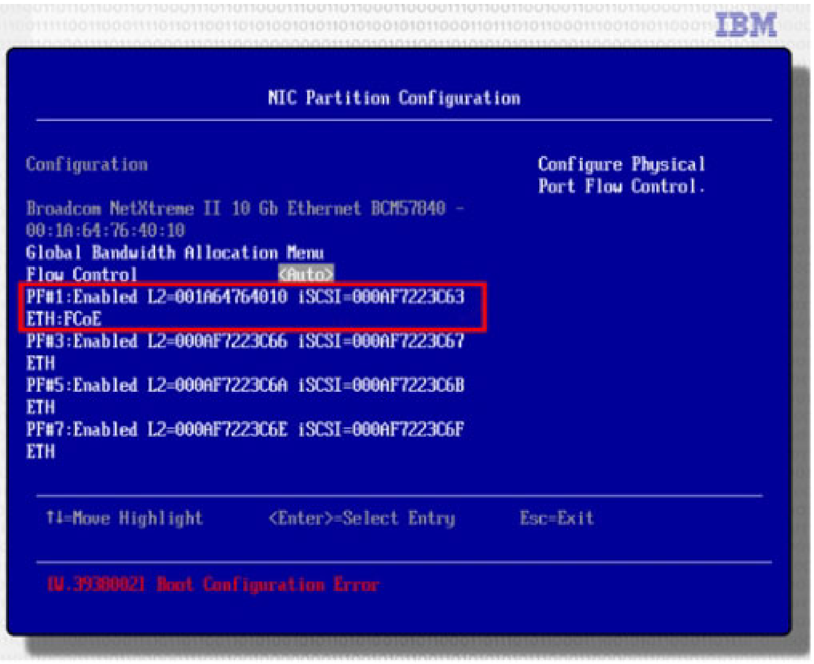
```
                              PF#0

Main Configuration Page > NIC Partition               Enable/Disable FCoE
Configuration > PF#0                                  Offload Protocol. This
                                                      option is disabled if
Ethernet Protocol          <Enabled>                  this port has two
iSCSI Offload Protocol     <Disabled>                 partitions that
FCoE Offload Protocol      <Disabled>                 already have FCoE
Network MAC Address        00:0A:F7:22:3B:60          Offload Protocol
Virtual Network MAC        00:0A:F7:22:3B:60          enabled.
Address
iSCSI MAC Address          00:0A:F7:22:3B:61
Virtual iSCSI MAC Address  00:0A:F7:22:3B:61
FIP MAC Address            00:0A:F7:22:3B:61
Virtual FIP MAC Address    00:0A:F7:22:3B:61
World Wide Node Name       10:00:00:0A:F7:22:3B:61

 ↑↓=Move Highlight      <Enter>=Select Entry      Esc=Exit

 [I] Informational Event(s) Detected, Check POST Event Viewer
```

Note that the Ethernet mode is enabled and both FC and iSCSI are disabled. The MAC address is set to the factory defaults.

c. Use the information in "Profiles" on page 28 to apply an IFM pattern to the IBM Flex System CN4022 2-Port Adapter.

3. To set all ports to Ethernet and configure eight virtual Ethernet ports and one Fibre Channel port, complete the following steps:

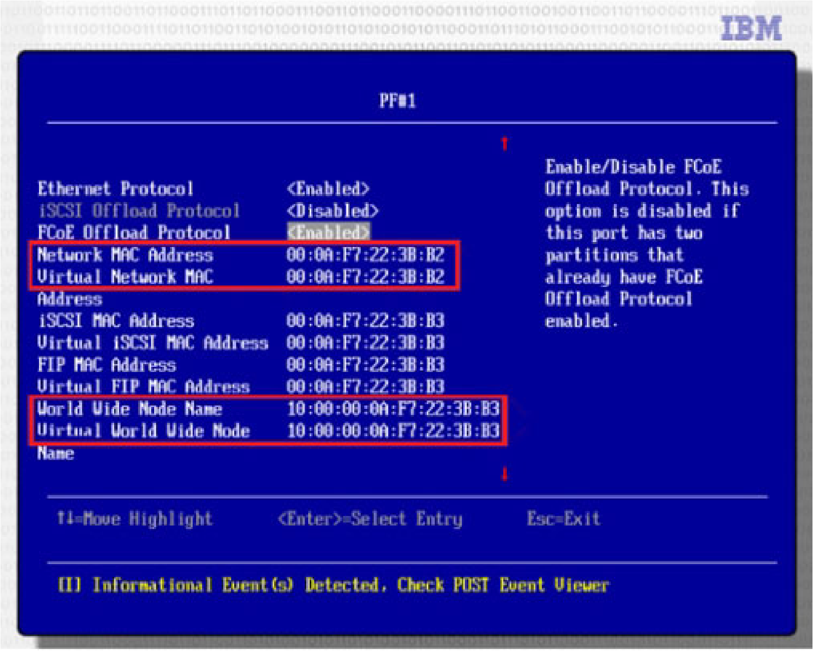
   a. Access the NIC Partition Configuration Page from the Main Configuration Page to configure the adapter.



```
                       NIC Partition Configuration

Configuration                                          Configure Physical
                                                       Port Flow Control.
Broadcom NetXtreme II 10 Gb Ethernet BCM57840 -
00:1A:64:76:40:10
Global Bandwidth Allocation Menu
Flow Control                <Auto>
PF#1:Enabled L2=001A64764010 iSCSI=000AF7223C63
ETH:FCoE
PF#3:Enabled L2=000AF7223C66 iSCSI=000AF7223C67
ETH
PF#5:Enabled L2=000AF7223C6A iSCSI=000AF7223C6B
ETH
PF#7:Enabled L2=000AF7223C6E iSCSI=000AF7223C6F
ETH

 ↑↓=Move Highlight      <Enter>=Select Entry      Esc=Exit

 [W.3938002] Boot Configuration Error
```

Note that each physical port has four PCI functions (PFs) which are set to Ethernet mode (ETH), except the PF#1 for the physical port 2.

   b. Select PF#1 to view the details of the virtual port.

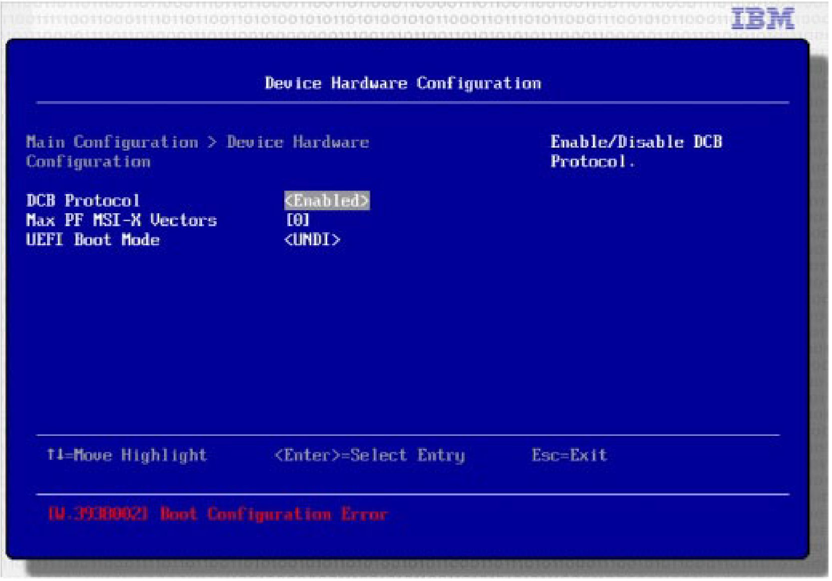


```
                              PF#1

                                                   Enable/Disable FCoE
Ethernet Protocol         <Enabled>                Offload Protocol. This
iSCSI Offload Protocol    <Disabled>               option is disabled if
FCoE Offload Protocol     <Enabled>                this port has two
Network MAC Address       00:0A:F7:22:3B:B2        partitions that
Virtual Network MAC       00:0A:F7:22:3B:B2        already have FCoE
Address                                            Offload Protocol
iSCSI MAC Address         00:0A:F7:22:3B:B3        enabled.
Virtual iSCSI MAC Address 00:0A:F7:22:3B:B3
FIP MAC Address           00:0A:F7:22:3B:B3
Virtual FIP MAC Address   00:0A:F7:22:3B:B3
World Wide Node Name      10:00:00:0A:F7:22:3B:B3
Virtual World Wide Node   10:00:00:0A:F7:22:3B:B3
Name

 ↑↓=Move Highlight      <Enter>=Select Entry      Esc=Exit

 [I] Informational Event(s) Detected. Check POST Event Viewer
```

Note that the Ethernet mode and FC mode are enabled and iSCSI is disabled. The MAC address and WWN are set to the factory defaults.

c. Use the information in “Profiles” on page 28 to apply an IFM pattern to the IBM Flex System CN4022 2-Port Adapter.

4. You can enable **DCB Protocol** from the Device Hardware Configuration page to setup an exception to the configuration. If Ethernet is disabled for functions 0 or 1, the interface will still consume the MAC address. This is whether or not FCoE or iSCSI is enabled on the interface.

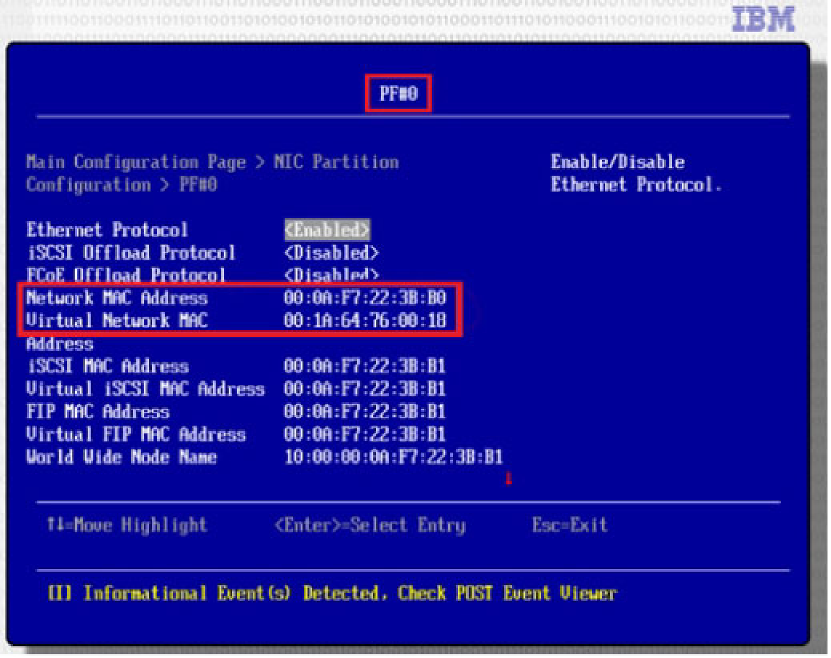


```
                     Device Hardware Configuration

Main Configuration > Device Hardware                 Enable/Disable DCB
Configuration                                        Protocol.

DCB Protocol              <Enabled>
Max PF MSI-X Vectors      [0]
UEFI Boot Mode            <UNDI>

 ↑↓=Move Highlight      <Enter>=Select Entry      Esc=Exit

 [W.3930002] Boot Configuration Error
```

What to do next

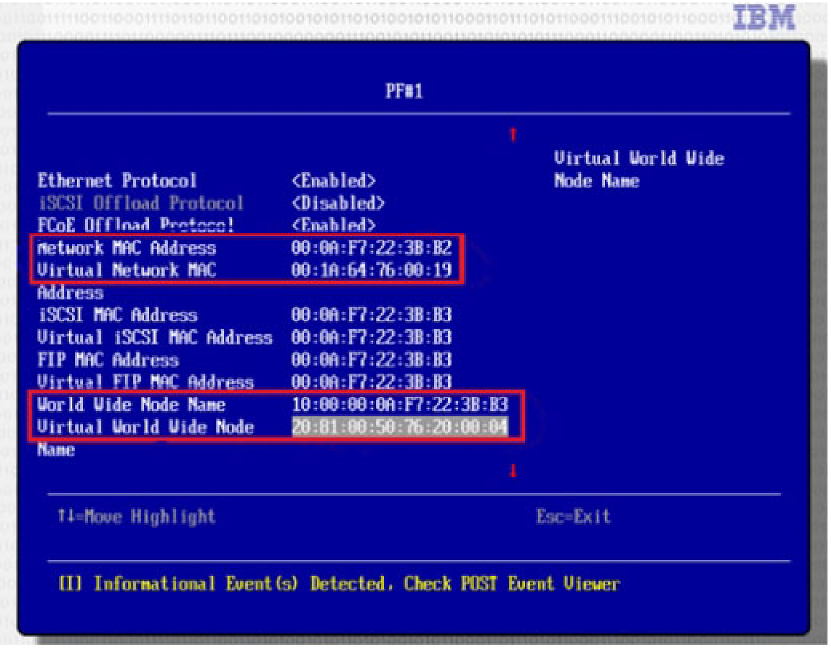
Optionally, you can verify the configuration of the adapter through the uEFI utility, IFM, and the CMM CLI mode.

1. Verify that the adapter uses the new addresses from the IFM configuration. Note that the compute node has a new virtual MAC address.



```
                              PF#0

Main Configuration Page > NIC Partition          Enable/Disable
Configuration > PF#0                             Ethernet Protocol.

Ethernet Protocol          <Enabled>
iSCSI Offload Protocol     <Disabled>
FCoE Offload Protocol      <Disabled>
Network MAC Address        00:0A:F7:22:3B:B0
Virtual Network MAC        00:1A:64:76:00:18
Address
iSCSI MAC Address          00:0A:F7:22:3B:B1
Virtual iSCSI MAC Address  00:0A:F7:22:3B:B1
FIP MAC Address            00:0A:F7:22:3B:B1
Virtual FIP MAC Address    00:0A:F7:22:3B:B1
World Wide Node Name       10:00:00:0A:F7:22:3B:B1

  ↑↓=Move Highlight      <Enter>=Select Entry      Esc=Exit

  [I] Informational Event(s) Detected, Check POST Event Viewer
```

If you configured one virtual port for Fibre Channel, the WWN value will consume, too. The new addresses that the compute node will have are the addresses from **Virtual MAC Addresses** and the addresses from **Virtual World Wide Node**.

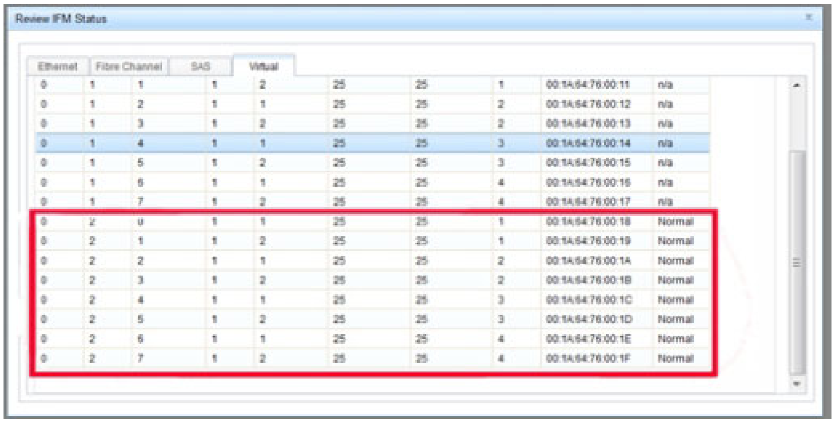


```
                              PF#1

                                                 Virtual World Wide
Ethernet Protocol          <Enabled>             Node Name
iSCSI Offload Protocol     <Disabled>
FCoE Offload Protocol      <Enabled>
Network MAC Address        00:0A:F7:22:3B:B2
Virtual Network MAC        00:1A:64:76:00:19
Address
iSCSI MAC Address          00:0A:F7:22:3B:B3
Virtual iSCSI MAC Address  00:0A:F7:22:3B:B3
FIP MAC Address            00:0A:F7:22:3B:B3
Virtual FIP MAC Address    00:0A:F7:22:3B:B3
World Wide Node Name       10:00:00:0A:F7:22:3B:B3
Virtual World Wide Node    20:01:00:50:76:20:00:04
Name

  ↑↓=Move Highlight                                Esc=Exit

  [I] Informational Event(s) Detected, Check POST Event Viewer
```

To verify Fibre Channel consumption through IFM, see “Hardware devices” on page 20.

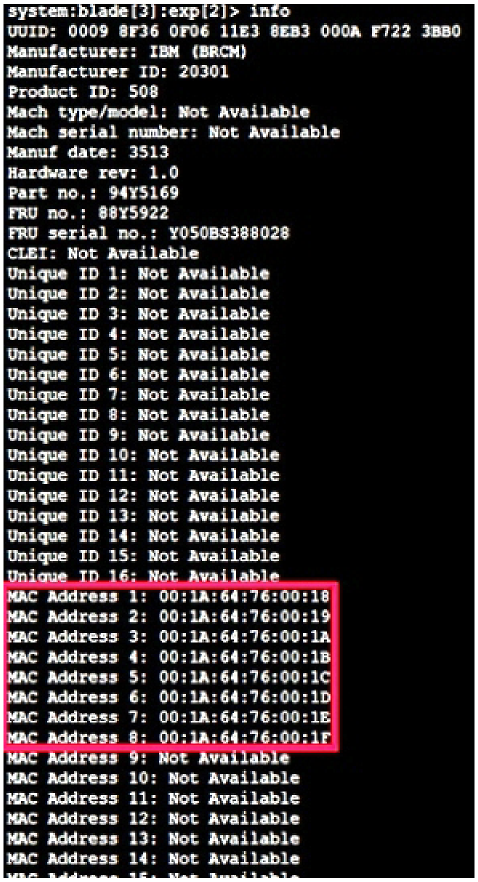
2. You can verify that IFM reflects the address consumption. Note that the adapter is inserted in Mezz 2, and has eight virtual ports. All ports have Normal status, which means the ports consumed the new addresses. If you configured one virtual port for Fibre Channel, virtual port 2 has both Ethernet mode and FC

mode, which has a user-defined value.



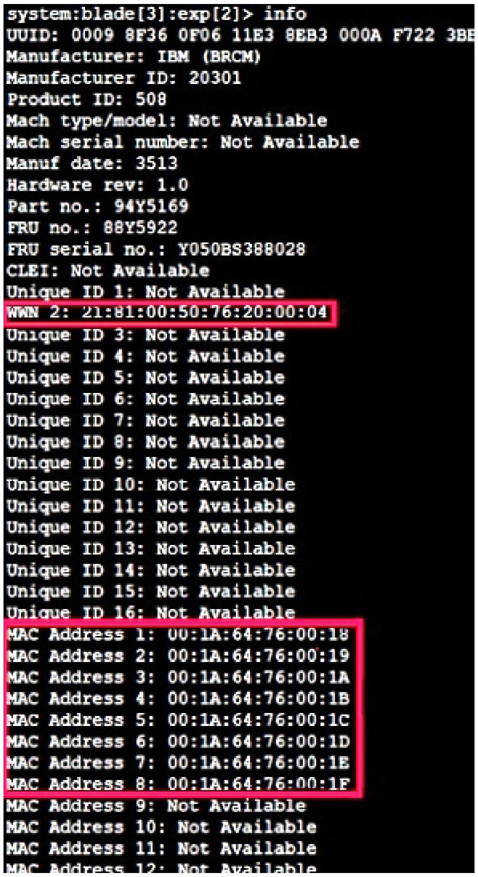
0	1	1	1	2	25	25	1	00:1A:64:76:00:11	n/a
0	1	2	1	1	25	25	2	00:1A:64:76:00:12	n/a
0	1	3	1	2	25	25	2	00:1A:64:76:00:13	n/a
0	1	4	1	1	25	25	3	00:1A:64:76:00:14	n/a
0	1	5	1	2	25	25	3	00:1A:64:76:00:15	n/a
0	1	6	1	1	25	25	4	00:1A:64:76:00:16	n/a
0	1	7	1	2	25	25	4	00:1A:64:76:00:17	n/a
0	2	u	1	1	25	25	1	00:1A:64:76:00:18	Normal
0	2	1	1	2	25	25	1	00:1A:64:76:00:19	Normal
0	2	2	1	1	25	25	2	00:1A:64:76:00:1A	Normal
0	2	3	1	2	25	25	2	00:1A:64:76:00:1B	Normal
0	2	4	1	1	25	25	3	00:1A:64:76:00:1C	Normal
0	2	5	1	2	25	25	3	00:1A:64:76:00:1D	Normal
0	2	6	1	1	25	25	4	00:1A:64:76:00:1E	Normal
0	2	7	1	2	25	25	4	00:1A:64:76:00:1F	Normal

3. You can verify the address consumption in CMM through the CLI mode.



```
system:blade[3]:exp[2]> info
UUID: 0009 8F36 0F06 11E3 8EB3 000A F722 3BB0
Manufacturer: IBM (BRCM)
Manufacturer ID: 20301
Product ID: 508
Mach type/model: Not Available
Mach serial number: Not Available
Manuf date: 3513
Hardware rev: 1.0
Part no.: 94Y5169
FRU no.: 88Y5922
FRU serial no.: Y050BS388028
CLEI: Not Available
Unique ID 1: Not Available
Unique ID 2: Not Available
Unique ID 3: Not Available
Unique ID 4: Not Available
Unique ID 5: Not Available
Unique ID 6: Not Available
Unique ID 7: Not Available
Unique ID 8: Not Available
Unique ID 9: Not Available
Unique ID 10: Not Available
Unique ID 11: Not Available
Unique ID 12: Not Available
Unique ID 13: Not Available
Unique ID 14: Not Available
Unique ID 15: Not Available
Unique ID 16: Not Available
MAC Address 1: 00:1A:64:76:00:18
MAC Address 2: 00:1A:64:76:00:19
MAC Address 3: 00:1A:64:76:00:1A
MAC Address 4: 00:1A:64:76:00:1B
MAC Address 5: 00:1A:64:76:00:1C
MAC Address 6: 00:1A:64:76:00:1D
MAC Address 7: 00:1A:64:76:00:1E
MAC Address 8: 00:1A:64:76:00:1F
MAC Address 9: Not Available
MAC Address 10: Not Available
MAC Address 11: Not Available
MAC Address 12: Not Available
MAC Address 13: Not Available
MAC Address 14: Not Available
MAC Address 15: Not Available
```

If you configured one virtual port for Fibre Channel, you can verify the WWN address consumption in CMM through the CLI mode.



```
system:blade[3]:exp[2]> info
UUID: 0009 8F36 0F06 11E3 8EB3 000A F722 3BE
Manufacturer: IBM (BRCM)
Manufacturer ID: 20301
Product ID: 508
Mach type/model: Not Available
Mach serial number: Not Available
Manuf date: 3513
Hardware rev: 1.0
Part no.: 94Y5169
FRU no.: 88Y5922
FRU serial no.: Y050BS388028
CLEI: Not Available
Unique ID 1: Not Available
WWN 2: 21:81:00:50:76:20:00:04
Unique ID 3: Not Available
Unique ID 4: Not Available
Unique ID 5: Not Available
Unique ID 6: Not Available
Unique ID 7: Not Available
Unique ID 8: Not Available
Unique ID 9: Not Available
Unique ID 10: Not Available
Unique ID 11: Not Available
Unique ID 12: Not Available
Unique ID 13: Not Available
Unique ID 14: Not Available
Unique ID 15: Not Available
Unique ID 16: Not Available
MAC Address 1: 00:1A:64:76:00:18
MAC Address 2: 00:1A:64:76:00:19
MAC Address 3: 00:1A:64:76:00:1A
MAC Address 4: 00:1A:64:76:00:1B
MAC Address 5: 00:1A:64:76:00:1C
MAC Address 6: 00:1A:64:76:00:1D
MAC Address 7: 00:1A:64:76:00:1E
MAC Address 8: 00:1A:64:76:00:1F
MAC Address 9: Not Available
MAC Address 10: Not Available
MAC Address 11: Not Available
MAC Address 12: Not Available
```

vNIC template considerations

(IBM Flex System devices only) This topic describes information that you must consider when you setup and use vNIC templates.

Consider the following information about setting up vNIC templates for the IBM Flex System CN4022 2-Port Adapter:

- The **Profile** and **VLAN** fields have no effect in defining templates for the IBM Flex System CN4022 2-Port Adapter.
- The **Max Bandwidth** field defines a cap on how much a virtual port can use as a percentage of the link speed. At 10 Gb each percentage is 100 Mbps. If all ports are set to 100, they share equally and if a port is not in use, its bandwidth can be spread among the other ports.

  Bandwidth weight is used to arbitrate how each channel takes precedence in the event of oversubscription. If they are non-zero then the channels with the highest number get precedence over channels of lower value. If they are all 0 then they share equal weight again and no port has precedence.

For more information about vNIC templates, see “Templates” on page 26.

Chapter 5. Solving problems

Use this information to diagnose and correct problems that might occur when you use IFM.

If you cannot locate and correct a problem by using the information in this topic, see "Getting help and technical assistance," on page 49.

When you collect IFM log information for service personnel, do not restart the IFM server before copying the LAX.log file to a new location. This file is found in the ofm/data directory and contains important service data. However, it is over written when the IFM server starts.

Table 9. IFM common problems

Problem	Solution
An address manager template configuration did not apply	Turn off the server or select the template power-on override option.
Cannot connect to the IFM console	If using Internet Explorer 8.0, check the browser security settings.
Failover monitor is not initiated Failover monitor fails to power on the standby server	1. Make sure that the management module is configured correctly for SNMP traps (see "Configuring the management module to send traps" on page 12). 2. Make sure that the management module that is being monitored for failovers has registered the correct SNMPv3 password and SNMPv3 receiver IP address. To verify, send a test alert from the management module and check in the logs that it is received. 3. Make sure that this IFM server is the only one registered for traps from the management module. 4. Make sure that the monitor is started, and that the correct triggering events in the monitor are checked. 5. Check for a mismatch between the template configuration and the hardware configuration. 6. Make sure that you set the server IFM mode to **Disable** before applying the template.
IFM console is not responding.	If you have just started the IFM server, try the request again later. At startup, the IFM server refreshes the inventory and during that time the IFM console may not respond. Otherwise try restarting the IFM server. If the problem persists, contact IBM support.
IFM tasks not available on the management module	Make sure that a IFM license is installed on the management module.
No chassis show up in the Available chassis box	Make sure that the chassis have been completely discovered.

Table 9. IFM common problems (continued)

Problem	Solution
No servers show up in the available servers section	Make sure that the servers and the chassis have been completely detected.
Template failed to be applied	1. Check that the servers are not turned on. 2. Check that you have discovered all of the chassis in the domain.
Standby Server Pool failed after manually applying to a server	1. Check that the servers in the standby pool have the same model and type as the source server. 2. Check that the standby server pool does not contain only the source server (a failover attempt to the same server always fails). 3. Check that the servers in the standby server are powered off. 4. Make sure that the plug-in for your network switches has been installed.
Standby Server Pool failed to be applied after creating an event action plan and applying the event action plan to a server	1. Check the logs to make sure the event that you are filtering on was actually triggered. 2. Make sure that the event action plan was applied to the correct server. 3. Check that the event was sent to the server object and not just to the chassis.
Unable to download IFM software	Check the product activation code shipped with your order. To download IFM, go to http://www-03.ibm.com/systems/flex/fabricmanager/bto/index.html.

Appendix. Getting help and technical assistance

If you need help, service, or technical assistance or just want more information about IBM products, you will find a wide variety of sources available from IBM to assist you.

Use this information to obtain additional information about IBM and IBM products, determine what to do if you experience a problem with your IBM system or optional device, and determine whom to call for service, if it is necessary.

Before you call

Before you call, make sure that you have taken these steps to try to solve the problem yourself.

If you believe that you require IBM to perform warranty service on your IBM product, the IBM service technicians will be able to assist you more efficiently if you prepare before you call.

- Check for updated software, firmware, and operating-system device drivers for your IBM product. The IBM Warranty terms and conditions state that you, the owner of the IBM product, are responsible for maintaining and updating all software and firmware for the product (unless it is covered by an additional maintenance contract). Your IBM service technician will request that you upgrade your software and firmware if the problem has a documented solution within a software upgrade.

  Determine whether the firmware and device drivers for the devices in the IBM Flex System Enterprise Chassis are up to date. You can use the IBM Flex System Manager Update Manager to automatically acquire, install, and manage firmware and device-driver updates for the devices in the chassis.
- If you have installed new hardware or software in your environment, check http://www.ibm.com/systems/info/x86servers/serverproven/compat/us to make sure that the hardware and software is supported by your IBM product.
- Go to http://www.ibm.com/supportportal to check for information to help you solve the problem.
- Gather the following information to provide to IBM Support. This data will help IBM Support quickly provide a solution to your problem and ensure that you receive the level of service for which you might have contracted.
  - Hardware and Software Maintenance agreement contract numbers, if applicable
  - Machine type number (IBM 4-digit machine identifier)
  - Model number
  - Serial number
  - Current system UEFI and firmware levels
  - Other pertinent information such as error messages and logs
- Submit a manual service request through the IBM Flex System Manager management software. When you submit a manual service request, service data about the problem is included in the request, which will help IBM Support more quickly begin to diagnose the problem.

- Go to http://www.ibm.com/support/entry/portal/Open_service_request to submit an Electronic Service Request. Submitting an Electronic Service Request will start the process of determining a solution to your problem by making the pertinent information available to IBM Support quickly and efficiently. IBM service technicians can start working on your solution as soon as you have completed and submitted an Electronic Service Request.

Using the documentation

Information about your IBM system and preinstalled software, if any, or optional device is available in the documentation that comes with the product. That documentation can include printed documents, online documents, readme files, and help files.

See the troubleshooting information in your system documentation for instructions for using the diagnostic programs. The troubleshooting information or the diagnostic programs might tell you that you need additional or updated device drivers or other software. IBM maintains pages on the World Wide Web where you can get the latest technical information and download device drivers and updates. To access these pages, go to http://www.ibm.com/supportportal.

You can find the most up-to-date information for the IBM Flex System product family at http://pic.dhe.ibm.com/infocenter/flexsys/information/index.jsp.

Getting help and information from the World Wide Web

Up-to-date information about IBM products and support is available on the World Wide Web.

On the World Wide Web, up-to-date information about IBM systems, optional devices, services, and support is available at http://www.ibm.com/supportportal.

You can find the most up-to-date product information for the IBM Flex System product family at http://pic.dhe.ibm.com/infocenter/flexsys/information/index.jsp.

How to send DSA data to IBM

Use the IBM Enhanced Customer Data Repository to send diagnostic data to IBM.

Before you send diagnostic data to IBM, read the terms of use at http://www.ibm.com/de/support/ecurep/terms.html.

You can use any of the following methods to send diagnostic data to IBM:

- **Standard upload:** http://www.ibm.com/de/support/ecurep/send_http.html
- **Standard upload with the system serial number:** http://www.ecurep.ibm.com/app/upload_hw
- **Secure upload:** http://www.ibm.com/de/support/ecurep/send_http.html#secure
- **Secure upload with the system serial number:** https://www.ecurep.ibm.com/app/upload_hw

Software service and support

Through IBM Support Line, you can get telephone assistance, for a fee, with usage, configuration, and software problems with your IBM products.

For information about which products are supported by Support Line in your country or region, see http://www.ibm.com/services/supline/products.

For more information about Support Line and other IBM services, see http://www.ibm.com/services or see http://www.ibm.com/planetwide for support telephone numbers. In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

Hardware service and support

You can receive hardware service through your IBM reseller or IBM Services.

To locate a reseller authorized by IBM to provide warranty service, go to http://www.ibm.com/partnerworld and click **Find Business Partners**. For IBM support telephone numbers, see http://www.ibm.com/planetwide. In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

In the U.S. and Canada, hardware service and support is available 24 hours a day, 7 days a week. In the U.K., these services are available Monday through Friday, from 9 a.m. to 6 p.m.

IBM Taiwan product service

Use this information to contact IBM Taiwan product service.

台灣IBM產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

IBM Taiwan product service contact information:

IBM Taiwan Corporation
3F, No 7, Song Ren Rd.
Taipei, Taiwan
Telephone: 0800-016-888

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product, and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies.

A current list of IBM trademarks is available on the web at “Copyright and trademark information” at http://www.ibm.com/legal/copytrade.shtml .

Adobe and PostScript are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc., in the United States, other countries, or both and is used under license therefrom.

Intel, Intel Xeon, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Important notes

Processor speed indicates the internal clock speed of the microprocessor; other factors also affect application performance.

CD or DVD drive speed is the variable read rate. Actual speeds vary and are often less than the possible maximum.

When referring to processor storage, real and virtual storage, or channel volume, KB stands for 1024 bytes, MB stands for 1,048,576 bytes, and GB stands for 1,073,741,824 bytes.

When referring to hard disk drive capacity or communications volume, MB stands for 1,000,000 bytes, and GB stands for 1,000,000,000 bytes. Total user-accessible capacity can vary depending on operating environments.

Maximum internal hard disk drive capacities assume the replacement of any standard hard disk drives and population of all hard disk drive bays with the largest currently supported drives that are available from IBM.

Maximum memory might require replacement of the standard memory with an optional memory module.

IBM makes no representation or warranties regarding non-IBM products and services that are ServerProven, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. These products are offered and warranted solely by third parties.

IBM makes no representations or warranties with respect to non-IBM products. Support (if any) for the non-IBM products is provided by the third party, not IBM.

Some software might differ from its retail version (if available) and might not include user manuals or all program functionality.

Particulate contamination

Attention: Airborne particulates (including metal flakes or particles) and reactive gases acting alone or in combination with other environmental factors such as humidity or temperature might pose a risk to the device that is described in this document.

Risks that are posed by the presence of excessive particulate levels or concentrations of harmful gases include damage that might cause the device to malfunction or cease functioning altogether. This specification sets forth limits for particulates and gases that are intended to avoid such damage. The limits must not be viewed or used as definitive limits, because numerous other factors, such as temperature or moisture content of the air, can influence the impact of particulates or environmental corrosives and gaseous contaminant transfer. In the absence of specific limits that are set forth in this document, you must implement practices that maintain particulate and gas levels that are consistent with the protection of human health and safety. If IBM determines that the levels of particulates or gases in your environment have caused damage to the device, IBM may condition provision of repair or replacement of devices or parts on implementation of appropriate remedial measures to mitigate such environmental contamination. Implementation of such remedial measures is a customer responsibility.

Table 10. Limits for particulates and gases

Contaminant	Limits
Particulate	• The room air must be continuously filtered with 40% atmospheric dust spot efficiency (MERV 9) according to ASHRAE Standard 52.2[1]. • Air that enters a data center must be filtered to 99.97% efficiency or greater, using high-efficiency particulate air (HEPA) filters that meet MIL-STD-282. • The deliquescent relative humidity of the particulate contamination must be more than 60%[2]. • The room must be free of conductive contamination such as zinc whiskers.
Gaseous	• Copper: Class G1 as per ANSI/ISA 71.04-1985[3] • Silver: Corrosion rate of less than 300 Å in 30 days

1. ASHRAE 52.2-2008 - Method of Testing General Ventilation Air-Cleaning Devices for Removal Efficiency by Particle Size. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.
2. The deliquescent relative humidity of particulate contamination is the relative humidity at which the dust absorbs enough water to become wet and promote ionic conduction.
3. ANSI/ISA-71.04-1985. Environmental conditions for process measurement and control systems: Airborne contaminants. Instrument Society of America, Research Triangle Park, North Carolina, U.S.A.

Documentation format

The publications for this product are in Adobe Portable Document Format (PDF) and should be compliant with accessibility standards. If you experience difficulties when you use the PDF files and want to request a web-based format or accessible PDF document for a publication, direct your mail to the following address:

Information Development
IBM Corporation
205/A015

3039 E. Cornwallis Road
P.O. Box 12195
Research Triangle Park, North Carolina 27709-2195
U.S.A.

In the request, be sure to include the publication part number and title.

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Index

Part Number: 00FH387

Printed in USA

(1P) P/N: 00FH387