IBM Systems
IBM BladeCenter Open Fabric Manager

Installation and User's Guide

IBM Systems
IBM BladeCenter Open Fabric Manager

Installation and User's Guide

Note

Before using this information and the product it supports, read the general information in "Getting help and technical assistance," on page 63 and "Notices" on page 67.

Thirteenth Edition (September 2014)

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

Contents

Chapter 1. Introduction

IBM® BladeCenter® Open Fabric Manager (BOFM) is a solution that enables you to quickly replace and recover blades in your environment.

It does this by assigning Ethernet MAC, Fibre Channel WWN and SAS WWN addresses to the BladeCenter slots in such a way that any blades plugged into those slots take on the assigned addresses. This enables the Ethernet and Fibre Channel infrastructure to be configured once and before any blades are connected to the BladeCenter chassis.

There are two separate offerings of BladeCenter Open Fabric Manager. The main Open Fabric Manager function is provided in the Basic BOFM offering. Additional capabilities are available with the Advanced BOFM V4.x offering.

Basic Open Fabric Manager

With Basic Open Fabric Manager, you can pre-assign MAC and WWN addresses, as well as storage boot targets, for up to 100 chassis or 1400 blade servers. Using the management module Web interface, you can create addresses for blade servers, save the addresses to a configuration file, deploy the addresses to the blade slots in the same chassis or in up to 100 different chassis. This can be done without any blade servers installed in the chassis.

Advanced Open Fabric Manager V4.x

With Advanced Open Fabric Manager V4.x, you can monitor the health of blade servers and automatically - without user intervention - replace a failed blade from a designated pool of spare blades. After receiving a failure alert, Advanced BOFM attempts to power off the failing blade, read the BOFM virtualized addresses and boot target parameters, apply these parameters to the next blade in the standby blade pool, and power on the standby blade.

When the switch failover feature is enabled in Advanced BOFM, VLAN configuration on the switch associated with a failed blade is automatically migrated to the switch associated to the standby blade.

You can also pre-assign MAC and WWN addresses, as well as storage boot targets, for up to 256 chassis or 3584 blade servers. Using an enhanced graphical user interface, you can create addresses for blade servers, save the address profiles; deploy the addresses to the blade slots in the same chassis or in up to 100 different chassis. This can be done without any blade 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.

Backward compatibility

The current version of IBM BladeCenter Open Fabric Manager is version 4.1 which supports the BOFM v2 data structure by default. If a chassis does not support the BOFM v2 data structure, advanced BOFM automatically converts the configuration settings to be backward compatible with the BOFM v1 data structure. During the conversion process, the following configuration information is deleted:

- Ethernet addresses assigned to virtual ports

- The third and fourth boot targets
- Offset larger than 1

Before you begin

There are minimum hardware and software requirements the system must meet before you can install or use Basic BOFM and Advanced BOFM.

Hardware requirements

To review the installation requirements and supported hardware for the Advanced BOFM, see http://www.ibm.com/systems/bladecenter/hardware/openfabric/openfabricmanager.html.

Supported software

Advanced BOFM is supported on selected Microsoft Windows and Linux operating systems on x86 architecture.

Table 1. Advanced BOFM supported operating systems

Operating System
Microsoft Windows 2003 (SP1, SP2) (32/64 bit)
Microsoft Windows Server 2008 (SP1, SP2) (32/64 bit)
Microsoft Windows Server 2008 R2 (64 bit)
RHEL 4 (up to SP8) (32/64 bit)
RHEL 5 (up to SP5) (32/64 bit)
SLES 9 (up to SP4) (32/64 bit)
SLES 10 (up to SP2) (32/64 bit)
SLES 11 (32/64 bit)

Note:

The following software is also required:
- Sun Java SE 1.6
- A valid Basic BOFM licence and Advanced BOFM licence for each blade chassis. For more information, see “License information”

License information

See http://www.ibm.com/systems/bladecenter/hardware/openfabric/openfabricmanager.html for information about obtaining a Basic BOFM license and Advanced BOFM license.

The number of days remaining on the evaluation license is available from the BladeCenter Advanced Management Module (AMM) Web interface. When the evaluation license expires, you must install a permanent license.

Accessibility features for BOFM

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

Accessibility features

Accessibility for the BladeCenter Open Fabric Manager is provided through the BladeCenter Advanced Management Module command-line interface. The remote control video feed is not accessible to a screen reader.

The BladeCenter 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 Java access bridge must be installed to make Java applets available to the JAWS screen reader)
- 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 publications for IBM BladeCenter 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 BladeCenter 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

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

- **BladeCenter Open Fabric Manager**

  To access an overview of Open Fabric Manager, view the hardware requirements, obtain a license to use Basic BOFM and Advanced BOFM, and access links to download the product, go to http://www.ibm.com/systems/bladecenter/hardware/openfabric/openfabricmanager.html.
- **IBM ServerProven compatibility**

  You can obtain compatibility information about IBM System x® and IBM BladeCenter products from http://www.ibm.com/systems/info/x86servers/serverproven/compat/us/.
- **IBM Systems and servers documentation and technical support**

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

Notices and statements in this document

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. Overview

This topic provides a technical overview of BladeCenter Open Fabric Manager, including the configuration file and the standby AMM.

Configuration file

The BOFM configuration file is the central tool for managing the BOFM domain and contains the definitions that you need for a domain of up to 100 chassis. You can generate it automatically, save it, and edit it to conform to the needs of a specific domain and then apply it to the domain. You also have the option of creating your own configuration file.

The configuration file is a Comma Separated Value (CSV) file. Each non-blank and non-comment line defines a single entity within a domain. The entities currently defined are BladeCenters, Slots, and Port Entries, where a port is a single network device within a slot, which can have multiple definitions – one for each interface type.

The file is organized hierarchically by chassis, slots, and ports, with ample comment lines included to act as a guide to editing the file, if needed. It is best practice to maintain the original structure as much as possible in order to retain the readability of the file. For certain purposes it might be appropriate to extract a smaller section of the domain into a new file so that you can update a particular chassis or a particular blade individually.

To view a sample configuration file, see “Sample configuration file” on page 11.

Comments section

There are two types of comments: line comments and field comments.

```
// this is a line comment
localhost/# this is a field comment    ,bladecenter   ,apply
```

Line comments start with two slashes (//). The system ignores anything between this symbol and the end of the line. You can insert line comments anywhere in the file. However, inserting a comment inside a pair of quote marks results in a `No closing quote` error.

You can insert field comments in any field. Field comments start with a slash-hash (/#). The system ignores anything between this symbol and the end of the field. Inserting a field comment inside a pair of quotes does not cause an error.

Comments are included in the maximum line-length (currently 512 bytes including newlines). Very long comments should be broken over several lines to improve readability and to prevent exceeding the line-length limit. If you exceed the line-length limit, the system issues an error message.

BladeCenter section

```
//BladeCenterIP       ,Type,        ,Mode
  bladecenter2.ibm.com  ,BladeCenter   ,apply
```

The BladeCenter section contains three parameters: the **IP address of the BladeCenter**, the entity **Type** (BladeCenter), and the **Mode**.

IP Address (required)
The IP Address can be any valid BladeCenter address in one of the following formats:

- Advanced BOFM supports IPv4 dotted notation (for example, `192.168.0.1`)
- Basic BOFM supports IPv6 dotted notation (for example, `192.168.0.1`)
- Human-readable Internet addresses (for example, `bladecenter2.ibm.com`)

  Note: Fully-qualified hostname is required for this format as indicated above (.ibm.com is required).

For larger sites, 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.

Type (required)
The type is BladeCenter. Any variation of upper and lowercase is acceptable.

Mode (required)
The mode is one of two options: apply or ignore. When ignore is selected, the system discards all slots and ports belonging to that BladeCenter. This allows an entire BladeCenter to be commented-out without the need to modify each individual line, and without regard for the ordering of the file.

The BladeCenter section should always come before slots belonging to it, and only one BladeCenter section can exist for a particular BladeCenter. If no BladeCenter section exists, when a slot is defined, the system uses a reasonable default definition for the BladeCenter. The default definition is based on the IP address of the slot and its mode is `apply`.

You can define up to 100 BladeCenters with their blades and ports in a single file.

Slot section

```
//BladeCenterIP  ,Type   ,Slot,  ,Mode    ,Profile
  localhost      ,slot   ,1     ,enable   ,"TempProfile BC-1Slot-1"
```

The slot section represents a single slot within a BladeCenter. Its association to the BladeCenter is through the IP address of the BladeCenter. A slot entry is required before any port entries can be defined for that slot. Failure to define a slot before using it for a port results in an error. You can only define a slot once. Multiple definitions result in errors.

The slot section consists of five parameters: IP Address, Type, Slot, Mode, and Profile.

IP Address (required)
The IP Address can be any valid BladeCenter address in one of two formats: IPv4 or human-readable internet addresses. If you have not previously defined a BladeCenter with that address, the system defines one using reasonable defaults.

Type (required)
Always contains the value slot. Any combination of upper and lowercase is acceptable.

Slot (required)
Identifies the BladeCenter slot. This is a numeric value from 1 to 14. For a given type of BladeCenter the actual number of slots may be less than 14.

Mode (optional)
Can be one of three values:

- **Enable**: The AMM pushes the BOFM configuration to the blade.
- **Disable**: The AMM clears the BOFM configuration on the blade, so the blade goes to factory addresses.
- **Ignore**: The BOFM configuration of this slot is unchanged by the configuration file.

The default value is `disable`.

Profile (optional)
A string value of up to 31 characters. You can use it to attach a human-friendly string to a particular blade. When you generate the configuration file, the system creates a value based on the cardinal position of the BladeCenter in the file and the slot number. You can edit this value, but make sure that you stay within the 31 character limit. If you exceed this limit, the system truncates the string and issues a warning. If no profile is given, the system creates one based on the IP address.

Port section

There are currently three types of port entries. The IP Address, Slot, and Type parameters are common to all port types.

IP Address (required)
The IP Address can be any valid BladeCenter address in one of two formats: IPv4 or human-readable internet addresses. If no BladeCenter has previously been defined with that address, the system issues an error message.

Slot (required)
Identifies the BladeCenter slot. This is a numeric value from 1 to 14. For a given type of BladeCenter the actual number of slots may be less than 14. You can only define a port for a slot that has already been defined with a slot entry (see "Slot section" on page 6). Attempting to define a port for an undefined slot results in an error.

Offset (optional)
A value between 0 and 3. For single-slot blades this value is 0. See "Mapping of devices to ports" on page 11 and "Multi-slot blades and the port offset parameter" on page 12 for more information.

Type (required)
The port type. Any combination of upper and lowercase is acceptable.

- **Eth**: In addition to the four common parameters, the Ethernet port entry also contains the following parameters.

  Port (required)
  The port to which the data is written. This is a value between 1 and 8, where 1 and 2 are reserved for the built-in on-board Ethernet cards. See "Mapping of devices to ports" on page 11 and "Multi-slot blades and the port offset parameter" on page 12 for more information.

  MAC1 (required)
  The primary MAC address that is written to the Ethernet card attached to the port. It is a 48-bit EUI value represented in the field as six

hexadecimal bytes (using values 0 - 9 and A - F, and not preceded by 0x) separated by colons, for example, 12:34:56:78:90:AB. Invalid addresses cause an error and the system ignores the line. Address 00:00:00:00:00:00 is a valid address, which will be used by the hardware in place of the burned-in address, but will not be shown as so in the Hardware VPD.

VLAN1 (optional)
The VLAN you use for this Ethernet connection. An empty field is equivalent to a value of zero, and the system informs the NIC that no VLAN was selected. Values are 0 - 4095. This field defaults to zero.

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

MAC2 (optional)
The secondary MAC address for Ethernet cards that support this option. If you do not supply a value for this field it is not applied.

VLAN2 (optional)
The secondary VLAN that the system uses for those cards that support a secondary MAC address. This field is applied only if MAC2 and VLAN2 contain a supported value. Values are 0 - 4095. A value of zero is equivalent to an empty field.

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

Following is an example of the Ethernet entry parameters:

```
//IP     ,Type  ,Slot  ,Offset ,Port  ,MAC_1             ,VLAN1 ,MAC_2 ,VLAN2
localhost  ,eth   ,1     ,0    ,1     ,25:00:c9:00:00:00
```

Note: In the generated file Eth is expanded to Ethernet, but this is not required.

- **FC**: In addition to the common parameters, the Fibre Channel port entry also contains the following parameters.

  Port (required)
  The port to which the data is written. This is a value between 3 and 8 (1 and 2 are reserved for the built-in on-board Ethernet cards). See "Mapping of devices to ports" on page 11 and "Multi-slot blades and the port offset parameter" on page 12 for more information.

  WWNN (optional)
  The worldwide node name for the Fibre Channel device attached to the port. It is a 64-bit EUI value represented in the field as eight hexadecimal bytes (using values 0 - 9 and A - F, and not preceded by 0x) separated by colons. Not all applications require this value, and some interface cards supply this value themselves by creating a number based on a transformation of the WWPN.

  WWPN (required)
  The worldwide port name for the Fibre Channel device attached to the port. It is a 64-bit EUI value represented in the field as eight hexadecimal bytes (using values 0 - 9 and A - F, and not preceded by 0x) separated by colons. Invalid addresses result in an error and the line is ignored.

  Boot-order (optional)
  The target the interface uses during the boot process. Values are none, first, second, or both. If the value is first, second, or both, the boot

process tries to use the equivalent target to boot the blade (targets can have a priority of first or second). This parameter defaults to none.

Following is an example of the Fibre Channel entry parameters:

```
//IP      ,Type  ,Slot  ,Offset ,Port  ,WWNN                   ,WWPN             ,Boot-order
localhost ,fc   ,1     ,0    ,3    ,2f:fc:00:00:c9:00:00:00, 2f:fc:00:00:c9:00:00:00  ,none
```

- **FCTarget**: In addition to the common parameters, the Fibre Channel Target port entry also contains the following parameters.

  Priority (required)
  The value of this parameter can be `first` or `second`. `first` denotes the primary target for the blade and `second` denotes the secondary target.

  WWPN (required)
  The worldwide port name of the target. It is a 64-bit EUI value represented in the field as eight hexadecimal bytes (using values 0 - 9 and A - F, and not preceded by `0x`) separated by colons. Invalid addresses result in an error and the line is ignored.

  LUN (required)
  The LUN of the target. For numbers less than four bytes long this can be specified as a decimal or hexadecimal number, where hexadecimal numbers are preceded by `0x`. For longer numbers, you must use the standard EUI notation (eight pairs of hexadecimal characters, divided by colons).

- Following is an example of the Fibre Channel Target entry parameters:

```
//IP       ,Type      ,Slot  ,Priority  ,WWPN                     ,LUN
localhost  ,fctarget  ,1     ,first     ,ff:ff:ff:ff:ff:ff:ff:ff   ,0
```

- **SAS**: In addition to the common parameters, the SAS port entry also contains the following parameters.

  Port (required)
  The port to which the data is written. This is a value between 3 and 8 (1 and 2 are reserved for the built-in on-board Ethernet cards). See "Mapping of devices to ports" on page 11 and "Multi-slot blades and the port offset parameter" on page 12 for more information.

  WWPN (required)
  The worldwide port name for the SAS device attached to the port. It is a 64-bit EUI value represented in the field as eight hexadecimal bytes (using values 0 - 9 and A - F, and not preceded by `0x`) separated by colons. Invalid addresses result in an error and the line is ignored.

  Boot-order (optional)
  The target the interface uses during the boot process. Values are none, first, second, or both. If the value is first, second, or both, the boot process tries to use the equivalent target to boot the blade (targets can have a priority of first or second). This parameter defaults to none.

Following is an example of the Fibre Channel entry parameters:

```
//IP      ,Type  ,Slot  ,Offset ,Port  ,WWPN,                  ,Boot-order
localhost ,sas   ,1     ,0    ,3    ,50:05:07:60:1a:80:00:02  ,none
```

- **SASTarget**: In addition to the common parameters, the SAS Target port entry also contains the following parameters.

  Priority (required)
  The value of this parameter can be `first` or `second`. `first` denotes the primary target for the blade and `second` denotes the secondary target.

WWPN (required)
The worldwide port name of the target. It is a 64-bit EUI value represented in the field as eight hexadecimal bytes (using values 0 - 9 and A - F, and not preceded by 0x) separated by colons. Invalid addresses result in an error and the line is ignored.

LUN (required)
The LUN of the target. For numbers less than four bytes long this can be specified as a decimal or hexadecimal number, where hexadecimal numbers are preceded by 0x. For longer numbers, you must use the standard EUI notation (eight pairs of hexadecimal characters, divided by colons).

- Following is an example of the Fibre Channel Target entry parameters:

```
//IP       ,Type      ,Slot  ,Priority  ,WWN                      ,LUN
localhost  ,sastarget  ,1     ,first     ,11:11:11:11:11:11:11:11  ,0
```

- **Virtual**: In addition to the common parameters, the virutal port entry also contains the following parameters.

Port (required)
The physical port to which the data is written. This is either 5 or 7. See "Mapping of devices to ports" on page 11 and "Multi-slot blades and the port offset parameter" on page 12 for more information.

vPort (required)
The virtual port number. This is a value between 1 and 8. See "Mapping of devices to ports" on page 11 and "Multi-slot blades and the port offset parameter" on page 12 for more information.

minBand (required)
The minimum bandwidth associated with each virtual port. If value is set 0, then the port is disabled. Total minimum bandwidth for a physical port must be 100. Minimum bandwidth must be smaller than maximum bandwidth.

maxBand (required)
The maximum bandwidth associated with each virtual port. If minimum bandwidth is 0, then maximum bandwidth must be 0, as well. Maximum bandwidth must be greater than or equal to minimum bandwidth.

VLAN (optional)
The VLAN you use for this virtual Ethernet connection. An empty field is equivalent to a value of zero, and the system informs the NIC that no VLAN was selected. Values are 0 - 4095. This field defaults to zero.

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

Following is an example of the virtual port entry parameters:

```
//IP      ,Type  ,Slot  ,Offset ,Port  ,vPort  ,MAC             ,minBand   ,maxBand   ,Priority   ,vlan
localhost ,virtual   ,1     ,0    ,5    ,1  ,00:1a:64:76:00:08  ,25     ,25     ,1      ,0
```

Other format features of the configuration file

The configuration file also contains the following characteristics and requirements:

- **Case:** Characters in the configuration file are not case sensitive.
- **Whitespace:** The file is largely whitespace agnostic. Whitespace is stripped before the fields are parsed. To make editing easier for you when you choose not

to edit in a spreadsheet program, whitespace is added to the end of fields in the generated files. This whitespace is entirely optional and you can remove it.

- **Newlines:** The file supports spreadsheets that use the UNIX line-feed only convention (OpenOffice Calc) and the DOS carriage-return/line-feed convention (Excel). It also supports line-feed only and carriage-return/line-feed text editors.
- **Line-length:** The maximum line length is 512 characters. This is the absolute length of the line. It includes comments, whitespace carriage-returns, line feeds and other hidden characters. Exceeding this length results in a line error and the line is discarded.

Sample configuration file

This topic contains a sample configuration file.

```
// GENERATED FILE STARTS

// Blade Center 192.168.0.1
//IP         ,Type (Center) ,Mode
192.168.0.1  ,bladecenter    ,apply

//IP        ,Type (Slot) ,Slot  ,Mode    ,Profile
192.168.0.1  ,slot        ,1    ,enable  ,"TempProfile BC-2Slot-1"

//IP        ,Type  ,Slot  ,Port ,MAC_1           ,VLAN1 ,MAC_2  ,VLAN2
192.168.0.1  ,eth  ,1    ,1    ,25:00:c9:00:00:70  ,0
192.168.0.1  ,eth  ,1    ,2    ,25:00:c9:00:00:71  ,0
192.168.0.1  ,eth  ,1    ,3    ,25:00:c9:00:00:72  ,0
192.168.0.1  ,eth  ,1    ,4    ,25:00:c9:00:00:73  ,0

//IP      ,Type  ,Slot  ,Port  ,WWPN,                    ,Boot-order
localhost ,fc   ,1      ,3    ,2f:fc:00:00:c9:00:00:00  ,none

//IP       ,Type      ,Slot  ,Priority  ,WWN                       ,LUN
localhost  ,fctarget  ,1     ,first     ,00:00:00:00:00:00:00:00  ,0
```

Mapping of devices to ports

The mapping of ports to the devices on the blade is as follows:

- 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 BOFM ports and the switch numbering on the chassis is dependant 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 BOFM ports to the switch numbering on the chassis.

Table 2. Chassis IO/M numbering

	Chassis IO/M numbering				
BOFM port	BC1	BCT	BCH	BCHT	BCS
1	1		1	1	1
2	2		2	2	1
3	3		3	3	3

Table 2. Chassis IO/M numbering (continued)

	Chassis IO/M numbering				
4	4		4	4	4
5	n/a	n/a	7	7	2
6	n/a	n/a	8	8	n/a
7	n/a	n/a	9	9	2
8	n/a	n/a	10	10	n/a

Multi-slot blades and the port offset parameter

Some blades fill more than a single slot in the chassis. As a result, they can access more ports than a single-slot blade.

The maximum number of ports available to a single slot is 8. The maximum number of ports available to a single blade is 128 (a blade can fill four slots, which is the maximum number of slots any blade can occupy at this time).

Ports beyond the eight ports of the first blade are referred to by using the port Offset parameter. Port 1 Offset 0 refers to the first built-in Ethernet port of a single or multi-slot blade. Port 1 Offset 1 refers to the third built-in Ethernet port of a blade that is double-width or more.

```
//IP          ,Type  ,Slot  ,Offset  ,Port ,MAC_1              ,VLAN1
localhost     ,eth   ,1     ,0       ,1    ,25:00:c9:00:00:00   ,1
localhost     ,eth   ,1     ,0       ,2    ,25:00:c9:00:00:01   ,2
localhost     ,eth   ,1     ,1       ,1    ,25:00:c9:00:00:00   ,1
localhost     ,eth   ,1     ,1       ,2    ,25:00:c9:00:00:01   ,2
```

The first two ports of each offset are reserved for the Ethernet attached card or built-in Ethernet (at offset = 0). Attempting to apply a Fibre Channel (FC) port specification to Port 1, Offset 2 causes an error. The parser prompts you that the port is reserved for Ethernet use only.

Standby AMM

Because an AMM failure results in a configuration loss, it is best practice to install a standby AMM when using BOFM.

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

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

Note: When an AMM is moved to a new chassis, it clears the configuration for all slots except for slots that have blades powered-on with a valid BOFM configuration that is already in use. For these slots, the AMM uses the BOFM configuration as defined on the blades.

If the AMM configuration is reset to factory defaults, the BOFM configuration is handled as if a new AMM was installed in the chassis.

If the primary AMM fails, the standby AMM contains the BOFM configuration and takes over. As an additional precaution, you should always save your BOFM configuration file or files via the BOFM interface whenever changes are made or a new configuration is applied.

If you only have one AMM installed in the chassis and you must replace it, before you replace it, insert the new AMM as a standby unit, let it power on and wait for a few minutes. This allows the BOFM configuration to be transferred to the new unit. You can remove the old unit and you do not have to reapply the BOFM configuration.

Note: You might have to wait longer than a few minutes, if the AMM you insert in the standby slot does not have the same firmware level as the primary.

Chapter 3. Preparing for BOFM

To prepare your environment for BOFM, you must upgrade the firmware of the AMMs and blades, including the BMC, BIOS, and additional expansion cards in your environment. In addition, optimum use of BOFM requires that you setup your blade environment to boot from SAN.

Important: UXSPs simplify the updating of all of your firmware. However, before you can upgrade your firmware on Emulex and Qlogic drivers, you must ensure that these fiber channel cards are already installed and operating properly. If you are not using UXSPs, follow the instructions in "Steps to update firmware without an OS" on page 17.

Upgrading firmware

Before you can use BOFM, you must first update the firmware of the chassis and blades, including BMC, BIOS, and additional expansion cards in your environment.

About this task

Attention: Installing the wrong firmware or device-driver update might cause the blade to malfunction. Before you install a firmware or device-driver update, read any readme and change history files that are provided with the downloaded update. These files contain important information about the update and the procedure for installing the update, including any special procedure for updating from an early firmware or device-driver version to the latest version.

Steps to update AMM firmware using the AMM Web interface

Procedure

1. Login to the AMM Web interface and select **Firmware Update** on the left pane, under **MM Control**. The Update MM Firmware page opens in the right pane.
2. On the Update MM Firmware page, click **Browse** to find the AMM flash file.
3. A separate Choose file window opens. Select the AMM flash file and click **Open**. The AMM flash file is shown in the field next to **Browse** on the Update MM Firmware page.
4. Click **Update** on the Update MM Firmware page and wait for the firmware to be uploaded to the AMM. If a standby MM is installed, the firmware on the standby MM automatically updates to the same level.
5. Click **Continue** to perform the flash.
6. Once the flashing is complete, you must reboot the AMM.

What to do next

On reboot, the new firmware is active and the standby AMM firmware is automatically updated.

Steps to update AMM firmware using UpdateXpress for BladeCenter (UXBC)

Procedure

1. Download Python interpreter, version 2.3 or later from http://www.python.org. The UXBC uses the Python update scripts to update the firmware of the applicable systems. To run the Python scripts, you must install Python interpreter on the administrative system.

   Note: Python also comes with most Linux distributions.
2. Download the latest UpdateXpress CD2 from http://www.ibm.com/supportportal.
3. Go to http://www.ibm.com/support/fixcentral/systemx/groupView?query.productGroup=ibm%2FBladeCenter and select your blade type from the list. This action directs you to a page for your blade type. Click **Management Module**. You can then select from a list of available AMM firmware updates. After you download the package, unzip the package and save it to the applicable server or network location for distribution to the target systems.
4. To save the firmware updates for a BladeCenter management module, complete the following steps:
   a. Copy the firmware update package to a network directory that you can access from the administrative console.

      Note: Do not unzip the firmware update package in the \BladeCenterUpdates directory. Each firmware update package includes a readme file. If you unzip the package in the \BladeCenterUpdates directory, the UXBC readme file is replaced with the update package readme file.
   b. Make a note of the directory path. This information is used to create the response file when BladeScanner is run.

Steps to update AMM firmware using BladeScanner and ChassisUpdate

Procedure

1. Use BladeScanner to create a response file.

   Note: Running ChassisUpdate with the -s (scan) switch (with valid Management Module login credentials) also creates a default response file.
2. Make note of the file name and directory location of the response file that you want to use.
3. In the MM section of the response file, set the paths of the AMM firmware updates and make sure mmdisable is set to false.

```
### MANDATORY Fields ###
# These fields must be specified.

# This is a mandatory field that specifies the dotted IP
# address of the BladeCenter Management Module.
mmipaddr=192.168.70.125

####  OPTIONAL Fields ###
# These fields may be necessary depending on the BladeCenter configuration.
# This is a mandatory field that specifies the username for the
# BladeCenter Management Module.
mmuser=UX2

# This is an optional field that contains the password of the specified
# username for the BladeCenter Management Module.  If not specified, an
# empty password will be supplied to the Management Module.
mmpass=nIKH7P!,
```

```
# This field is mandatory if you intend to update the Management Module.  If
# not overridden, the default paths are used.
mmFilename1=\\server\share\AMMFirmware\BPETXXX.TKT
# mmFilename2=FILE2
# mmFilename3=FILE3
# This is an optional field that disables the update of the BladeCenter
# Management Module.  If not specified, or specified as FALSE, the
# Management Module is updated.
mmdisable=FALSE
# This is an optional field that is used for informational purposes by
# BladeScanner. BladeScanner in scan mode detects the firmware revision of
# the MM and stores it in this field. BladeScanner in edit mode reads the MM
# firmware revision from this field and displays it on the UI.
# The update scripts ignore this field.
mmMainAppFirmwareRevision=BRET86L
mmMainAppRevisionNum=16
#mmBootRomFirmwareRevision=
#mmBootRomRevisionNum=
#mmRemoteControlFirmwareRevision=
#mmRemoteRevisionNum=
mmPS2toUSBFirmwareRevision=BREZ15
mmMMtoUSBFirmwareRevision=BRPI33
mmName=MM00096BCA2328
```

4. From a command-line prompt, change to the disk drive that contains the UpdateXpress for BladeCenter utilities.
5. Type the following command to run the ChassisUpdate utility:

   `chassisupdate.py -r` *file*

   where, *file* is the fully qualified file name of the response file that you want to use. The ChassisUpdate utility reads the parameter from the response file and updates the applicable systems.

Results

BladeScanner and ChassisUpdate record the transactions that they perform in a single log file. The log file is created in the following directories:

Table 3. BladeScanner and ChassisUpdate log file locations

Windows	Linux
%TEMP%\uxbc.log where %TEMP% is the temporary directory for the Windows operating system.	$HOME/uxbc.log

Information is appended to the uxbc.log file each time you run BladeScanner or ChassisUpdate. As a best practice, you should periodically delete this file.

Steps to update firmware without an OS

About this task

The use of UXSPs requires that you have an OS running on the blade. If you do not, you can follow these steps to upgrade your firmware.

Steps to update blade BMC firmware

Procedure

1. Download the latest BMC firmware boot image (BMC update diskette) from http://www.ibm.com/support/fixcentral/systemx/groupView?query.productGroup=ibm%2FBladeCenter and select your blade type from the list. This action directs you to a page for your blade type. Click **Baseboard Management Controller**, which takes you to the Baseboard

Management Controller section of the page. You can then select from a list of available boot images. The boot image (BMC update diskette) has a file extension of `img`.

2. Update the firmware by either creating a diskette from the image or using the remote drive feature of the AMM.
3. Follow the directions to update the BMC firmware.

Steps to update blade BIOS

Procedure

1. Download the latest BIOS update boot image from http://www.ibm.com/support/fixcentral/systemx/groupView?query.productGroup=ibm%2FBladeCenter and select your blade type from the list. This action directs you to a page for your blade type. Click **BIOS**, which takes you to the BIOS section of the page. You can then select from a list of available boot images. The BIOS has a file extension of `img`.
2. Update the blade BIOS by either creating a diskette from the image or using the remote drive feature of the AMM.
3. Follow the directions to update the BIOS.

Steps to update Emulex HBA firmware for x86 architecture

Procedure

1. Download the latest version of the Emulex HBA firmware from http://www.ibm.com/support/fixcentral/systemx/groupView?query.productGroup=ibm%2FBladeCenter and select your blade type from the list. This action directs you to a page for your blade type. Click **Fibre Channel**, which takes you to the Fibre Channel section of the page. You can then select from a list of available Emulex HBA firmware updates.
2. Create a bootable DOS diskette image containing the doslpcfg.exe flash tool and the <flash image name>.prg flash file.
3. Update the firmware by either creating a diskette from the image or using the remote drive feature of the AMM.
4. Type the following commands:

```
> doslpcfg download n=1 i=<flash image name>.prg
> doslpcfg download n=2 i=<flash image name>.prg
```

Steps to update QLogic firmware for x86 architecture

Procedure

1. Download the latest version of the QLogic HBA firmware from http://www.ibm.com/support/fixcentral/systemx/groupView?query.productGroup=ibm%2FBladeCenter and select your blade type from the list. This action directs you to a page for your blade type. Click **Fibre Channel**, which takes you to the Fibre Channel section of the page. You can then select from a list of available QLogic HBA firmware updates.
2. Create a bootable DOS diskette image containing the flashutil.exe flash tool and the <flash image name>.bin flash file.
3. Type the following command:

```
> flashutil /f /o<flash image name>.bin
```

Steps to update Emulex or QLogic HBA firmware for POWER PC architecture

Procedure

1. Pre-OS installations on POWER PC architecture systems can only be accomplished with the IBM Standalone Diagnostics CD-ROM. You can order

the CD-ROM from http://www.ibm.com/support/entry/portal/docdisplay?brandind=5000008&lndocid=SERV-DSA. In the search field, type `pSeries standalone`.

2. Obtain the latest firmware for Emulex or QLogic HBA from http://www.ibm.com/supportportal. Select **JS22** or **JS12** blades in the **Product family** field. Refine the results by selecting **Fibre Channel firmware**, then select from a list of available Emulex and QLogic firmware updates.
3. Create an ISO image CD using the acquired image. **Note:** Some external Windows or AIX-based workstations must be used in this step to create the ISO image.
4. Load the Standalone Diagnostics CD with the blade that requires the firmware update. Use the SoL interface on the JS blade to access the Standalone Diagnostics CD. Follow the documentation included with the Standalone Diagnostics CD-ROM to download firmware to the Emulex or QLogic HBA. After starting the Standalone Diagnostics CD-ROM, the Diagnostics CD must be removed and replaced with the CD you created in the previous steps. The Standalone Diagnostics utility uses this new CD as the source of the firmware download.

Setting up boot from SAN

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

Before you begin

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

Chapter 4. Basic BOFM

This topic describes how to install, configure, and use Basic BOFM.

AMM Web interface

Some functions require you to access the management-module Web interface.

For detailed information related to the AMM Web interface, see the *BladeCenter Management Module User's Guide*. The most recent versions of all BladeCenter documentation are at http://www.ibm.com/supportportal.

Installing Basic BOFM

The use of Basic BOFM does not require any installation because Basic BOFM capabilities are accessible through the AMM software. However, there are prerequisite tasks that must be satisfied before you can begin using Basic BOFM.

Ensure you have completed the steps outlined in Chapter 3, "Preparing for BOFM," on page 15.

Session and credentials

The AMM displays an error page when another user attempts to login with the same credentials.

For most of the Basic BOFM operations, the AMM needs to interact with other chassis. By default, it uses the user name and password that you used to login to the current AMM. If the AMM cannot login to other chassis, it prompts you to provide an alternative user name and password. The alternative user name and password are stored for the local session and are not cleared until you log out. Thus, while you are using Basic BOFM, another user cannot. If another user tries to open the Basic BOFM page while it is in use by you, the Web interface displays the Open Fabric Manager is in Use By Another Session page. If the new user clicks **Continue**, your operation is canceled.

Note: This page is displayed only if a new user starts Basic BOFM while a Basic BOFM operation is in progress, but is not yet complete. If you complete your last operation, this page is not displayed and the credentials are cleared automatically.

Configuring Basic BOFM

Configuring Basic BOFM involves a number of steps that include the creation of your configuration file and applying the new configuration.

Important:

1. To use Basic BOFM you must obtain a Basic BOFM license, which is available from http://www.ibm.com/systems/bladecenter/hardware/openfabric/openfabricmanager.html.
2. Changes in the Basic BOFM take effect when you restart the server. See the documentation that comes with your blade server for further instructions on how to turn off and turn on your blade server.

Consider the following conditions before using and installing BladeCenter HS23 Type 7875 and Emulex 10GbE VFA (option part number 81Y3120 and 90Y9332):

Table 4. BOFM configurations with BladeCenter HS23 and Emulex 10GbE VFA

	pNIC[1]	**IBM Virtual Fabric Mode**	**Switch Independent Mode**
Port 1	1 Gb LOM[2]	1 Gb LOM[2]	1 Gb LOM[2]
Port 2	1 Gb LOM[2]	1 Gb LOM[2]	1 Gb LOM[2]
Port 3			
Port 4			
Port 5	10 Gb LOM[2]	10 Gb LOM[2]	10 Gb LOM[2]
Port 6	Emulex 10 GbE VFA		
Port 7	10 Gb LOM[2]	10 Gb LOM[2]	10 Gb LOM[2]
Port 8	Emulex 10 GbE VFA		

Table notes:

1. Multichannel disabled
2. LAN on motherboard (LOM)
3. BOFM supports LOM whether the multichannel is enabled or disabled, but the VFA is only supported when the multichannel is disabled.
4. When FCoE personality is enabled, the World Wide Node Name (WWNN) port matches the Ethernet port.
5. When storage personalities (iSCSI or FCoE) are enabled, the storage ports obtain their MAC address from the MAC_2 field of the physical ports.
6. When the multichannel is enabled, the Ethernet information for the virtual ports is obtained from the virtual Ethernet data. If storage personalities (iSCSI or FCoE) are also enabled, Ethernet data for Virtual Port (vPort) 3 and 4 are ignored.
7. When the multichannel is enabled on BladeCenter HS23 10 Gb LOM ports, Ethernet data for Virtual Port (vPort) 5 and 6 are ignored. For 1Gb LOM ports, the Ethernet data is from the MAC address of Ethernet port 1 and 2.
8. You can manually edit the .CSV file to configure VLAN columns in IBM virtual fabric mode and switch independent mode. You can also configure minBand and maxBand in the switch independent mode.
9. Install the 10Gb interposer card to enable virtual ports for port 5 and 7.

Note: You may consider the above-mentioned conditions when installing and using Emulex 10GbE Virtual Fabric Adapter (option part number 49Y4235) and Emulex 10GbE Virtual Fabric Adapter II (CFFh) (option part number 90Y3550).

Creating a configuration file automatically

When using Basic BOFM for the first time, you must create a configuration file in which you assign virtual addresses to each slot in each chassis.

About this task

The following example outlines the steps you might follow when creating a configuration file automatically. It does not apply to all BladeCenter environments. These example steps assume that you have a single domain (no addresses are duplicated).

Procedure

1. Log in to the AMM Web interface and select **Open Fabric Manager** in the left pane, under **Blade Tasks**. The Open Fabric Manager Configuration Management page opens in the right pane.
2. Click **Create an Initial Configuration**. This opens the Specify Virtual Addresses page in the right pane.
3. For the **Ethernet Address Type**, use the pull-down under **Vendor** and select **IBM**.

   Note: Another option for **Vendor** is **User Defined**.
4. For the **FC Address Type**, use the pull-down under **Vendor** and select **Emulex** or **QLogic**.
5. For the **SAS Address Type**, use the pull-down under **Vendor** and select **LSI** or **IBM** range.
6. Click **Advanced option** and check the box next to **Generate an FC target place holder** or **SAS target place holder**.
7. In the **WWN** field, enter the storage system WWPN.

   Note: Optionally, you can also specify a value in the **LUN** field.
8. Click **Next**. This opens the Chassis to include page in the right pane.
9. Click **Next**. You can optionally add to an existing BOFM configuration. You can specify an existing BOFM configuration file (CSV file) using the **Browse** button. This file is prepended to the newly generated BOFM configuration file that contains addresses that follow those in the existing specified file. This extends the existing BOFM domain. If you do not want the new BOFM configuration prepended to an existing configuration, do not specify any file name. Instead, click **Next**.
10. On the Chassis to include page, there are two methods for providing the list of chassis to be included in the configuration file.

    You can either create a file with the list of AMM IP addresses or use the chassis that were discovered by the AMM via SLP. Before you click the **Use AMM IP Addresses that were discovered on the AMM management network** button, first use the Remote Chassis page with the SLP method to verify that all chassis on the page are those you want to configure BOFM. Otherwise, specify the chassis address list in a file as described below.

    If you elect to use an explicit list of AMM IP addresses instead, create a text file in which each line contains a single IP address or the hostname of a single chassis. If you use hostnames in this file, enable DNS and define at least one DNS server on the AMM Web interface Network Protocols page. When the text file is complete, you can then select the **Use AMM IP Addresses in a file that I specify** option on the Chassis to include page. Click **Browse** to locate the file that you created.

    Note: You can also use a valid existing BOFM configuration file to define the list of chassis.
11. Click **Next**. The AMM generates the configuration file and displays The Configuration File Has Been Created page.
12. The browser launches the File Save window allowing you to save the generated configuration file. If the File Save window does not appear, click **Download the configuration file manually** on The Configuration File Has Been Created page.

What to do next

It is best practice to store the configuration file locally, and validate the new configuration. It is also important to store the configuration file in a safe location because this is your original copy of the BOFM configuration. If an AMM has a hardware failure and you don't have a standby AMM, this is your single source to reproduce the BOFM configuration.

To apply the configuration directly or to create a Requirements Report, you can do it directly from this page.

When you complete the Specify Virtual Addresses page, consider the following information:

- Some applications check the adapter type and vendor using the address. You can select ranges that meet the type of adapter that you are using. Each vendor has allocated a special range for Basic BOFM outside of their normal range which guarantees that these addresses do not conflict with any previous or future burned-in addresses. Selecting a vendor automatically sets values within that range. You can also set it to **user defined** mode and select any range by editing the **From** and **To** fields.

  The default address ranges are as follows:

  ```
  Ethernet: The range for IBM MAC range is:
  00:1A:64:76:00:00 - 00:1A:64:76:FF:FF.

  FC :
    Qlogic: WWPN odd port range : 21:80:00:E0:8B:0X:XX:XX
    WWPN even port range: 21:81:00:E0:8B:2X:XX:XX
    where : X = 0..F
    WWNN adresses are generated internally by Qlogic from the WWPN.

  Emulex : WWNN odd port range: 2F:FE:00:00:C9:XX:XX:XX
    WWNN even port range: 2F:FF:00:00:C9:XX:XX:XX
    WWPN odd port range: 2F:FC:00:00:C9:XX:XX:XX
    WWPN even port range: 2F:FD:00:00:C9:XX:XX:XX
    where x = 0..F

  SAS:
    IBM range for WWPN: 50:05:07:60:1A:80:00:02 to
    50:05:07:60:1A:BF:FF:FF
    LSI range for WWPN:
    50:00:62:B0:00:11:17:02 to 50:00:62:B0:00:12:16:ff
  ```

- For FC (Fibre Channel), there are two ranges for each vendor: one for odd-numbered ports and one for even-numbered ports. The non-BOFM default is that the system assigns an address from one of the ranges for each port. When generating the file automatically, the system allocates the addresses for the even ports out of the first range and allocates the addresses for the odd ports out of the second range.

  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, and this might appear as two different devices rather then a single device. You can update the file manually to match your specific devices.
- For some vendors (such as QLogic), you do not need to define a WWPN, since it is automatically derived from the WWPN.
- By default, when you choose to assign MAC addresses they are assigned for each of the ports 1 to 8, FC addresses are assigned for each of the ports from 3 to 8, and SAS for ports 3 and 4 only. These configurations match a single slot blade. These are generic configurations, which contain a virtual address for each possible hardware type (Ethernet expansion card, FC expansion card, or SAS expansion card). As a result, when you change the type of blade or expansion

card, you do not need to modify the BOFM configuration. However, this option makes the configuration file bigger and error validation harder. If you want to generate a configuration that assigns an address to a subset of the ports, you can use the advanced options section. In this section, you can select which type of address to assign to each port.

Note: You can not assign FC addresses to ports 1 and 2, because these are the on board Ethernet NICs.

- Some Ethernet expansion cards 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. To set up a range of MAC addresses for a port, click **Advanced option**, then click **Generate range of MAC addresses per port**. You can define the following values for the JS and PS blade requirements:
  - **List of ports to apply to (numbers in the range 1 to 8, comma or space separated)**: The default value is 1.
  - **Range size:** Enter a range size between 2 and 256. The default value is 16.
  - **Ethernet VLAN for the second MAC address:** The default is 0.

  Note: The above default values allow the JS and PS blade onboard HEA Ethernet adapter to use the virtual addresses preassigned by the OS. To avoid conflicts, the MAC Address Step value (range size) must be between 16 and 256.
- For the NetXen 10 Gb Ethernet Expansion Card for IBM BladeCenter (39Y9271), do not click the **Advanced option** button to apply Fibre Channel (FC) addresses to FC ports that exist on the card. This generates errors.
- Click the **Advanced option** button to assign addresses to multi-slot blades. To do this, select the slot offset that you wish to assign addresses to, and, in the table for that offset, select the ports and type of address that you would like to assign. The maximum number of addresses that you can assign to any single blade is 32 addresses for a four-slot blade. For more information, see “Multi-slot blades and the port offset parameter” on page 12.
- Also click the **Advanced option** button to define the increment of the assigned addresses. The default is one (by default addresses are assigned sequentially). You can also define the VLAN tag for host-based VLAN tagging. Some Ethernet cards can have two MAC addresses per port. For these, you can elect to assign two MAC addresses by checking the **Generate range of MAC addresses per port** checkbox with a range of 2 addresses.
- In the advanced options for the FC section, you can also specify the step increment for the WWN and WWPN. In addition, you can select to create templates for the FC targets. After the file is created, you can edit the configuration file and fill in the correct target WWN and LUN for each slot.

Selecting domains

In some complex environments, you might need to create separate configuration files for multiple domains.

A single BOFM configuration corresponds to a single BOFM domain, in which duplicated addresses are not allowed. In general, unless you have a special reason to do so, it is best practice to have one configuration file for the entire domain. This way the AMM verifies that there are no address duplications when you modify the BOFM configuration.

However, in a more complex environment, it may be convenient to have multiple domains, where the same addresses can exist in different domains. In this case, you can generate a separate configuration file for each domain.

Attention: Do not use multiple configurations on a single network, since this overrides the protections against MAC or FC address duplication as discussed in "Avoiding address duplication."

Avoiding address duplication

When creating your BOFM configuration file, it is best practice to avoid address duplication.

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 blade is trying to access the same volume at the same time.

To ignore the duplicated addresses and apply the configuration anyway, click **Ignore**. To avoid the address duplication check, you can also select the **Ignore duplicate virtual addresses in the configuration file** advanced option on the Apply a Configuration window.

To avoid duplicate addresses, the AMM performs the following actions:

1. When a new configuration file is applied, the AMM verifies that it does not contain internal duplicate addresses.
2. Before applying the configuration, the AMM verifies that the blades that are about to be re-configured are powered off. This ensures that no addresses are currently in use.
3. Before writing the new BOFM configuration to the blades, the AMM disables the BOFM configuration on all the blades that are about to be re-configured. As a result, there can be no address duplication even if the operation has not completed.

For flexibility, the user can override these checks and apply the configuration even if the AMM generates warnings that duplicate addresses might exist. In addition, if the user defines the same address, in two different configuration files, for two chassis that are on the same network, then the AMM can not protect against address duplication.

To avoid address duplication, it is best practice to use a single configuration file for a single network domain and not use the options to override the protection that the AMM provides.

Resolving duplicate address errors

An error page results when the configuration file contains duplicate addresses.

If the configuration file contains duplicate addresses, the Open Fabric Manager Configuration Failure window displays in the AMM Web interface. The window contains a table. Each row of the table indicates an address that is duplicated and all of the lines in the configuration file on which the error appears. If you did not intend to have duplicate addresses, you must press **Cancel**, fix the configuration file, and then re-apply it.

Creating a requirements report

It is best practice to create a requirements report before you apply the BOFM configuration.

About this task

The requirements report verifies the firmware level of the blades BMC, BIOS, and adapters. It also goes through a dry run of the first part of applying the BOFM configuration and checks to see if there are potential problems.

Creating a requirements report from "The Configuration File Has Been Created" page in the AMM Web interface

Procedure

1. Follow the steps outlined in "Creating a configuration file automatically" on page 22.
2. On The Configuration File Has Been Created page, click **creating a requirements report**.

Creating a requirements report from the main Open Fabric Manager Configuration Management page on the AMM Web interface

Procedure

1. Login to the AMM Web interface.
2. In the left pane, under **Blade Tasks**, select **Open Fabric Manager**. The Open Fabric Manager Configuration Management page opens in the right pane.
3. Select **Create a Requirements Report**. The Create a Requirements Report page opens in the right pane.
4. Click **Browse** to locate the configuration file for which you are creating the requirements report. This would typically be a configuration file you want to use to apply a new BOFM configuration.
5. You can select **Advanced Options** to override certain checks. See "Applying a new configuration" on page 28 for more information.
6. After you locate the configuration file, click **OK**.

What to do next

If no parsing errors are found in the configuration file, the Requirements Report page is shown.

For a description of how to read the requirements report, a list of typical requirements report errors, and how to take action on the errors, see "Error messages" on page 50.

Editing the configuration file manually

After the initial generation of the configuration file, you can edit it to make changes to accommodate the specific needs of your environment.

Applying a new configuration

You can apply a new BOFM configuration from the main Open Fabric Manager page on the AMM Web interface.

Procedure

1. Login to the AMM Web interface.
2. In the left pane, under **Blade Tasks**, select **Open Fabric Manager**. The Open Fabric Manager Configuration Management page opens in the right pane.
3. Select **Apply a Configuration**. The Apply a Configuration page opens in the right pane.
4. Click **Browse** to locate the configuration file you want to apply.
5. You can click **Advanced Options** to override checks that protect against address duplication.
   a. If you select **Ignore duplicate virtual addresses in the configuration file** under **Advanced Options**, the AMM does not check for address duplication.
   b. If you select **Force the configuration to be applied to powered on blades** under **Advanced Options**, the AMM does not check the power state of the blades.

      Note: In general, you should not change the BOFM configuration while the blade is powered on. Changing the BOFM configuration while the blade is powered on can lead to duplicate addresses, and unexpected results.
   c. If you select **Continue on error** under Advanced Options, the AMM continues on most errors. Ignoring some of these errors may lead to address duplication. For example if the AMM is unable to connect to one of the chassis it continues even though that chassis might be using an address that is now assigned to a different chassis.
6. After you locate your configuration file and select advanced options, click **OK**. The AMM prepares to apply the new BOFM configuration and any errors that occur during this process are reported.

   Note: If the new configuration is identical to the current configuration, then a No Configuration Change page displays.

   Before applying the configuration, the AMM displays the Basic BOFM changes. There is a single line displayed for each chassis that has changes. If the Basic BOFM configuration for a given slot is changed, the corresponding cell in the table contains an icon, otherwise the cell is blank. If Basic BOFM is enabled for that slot, the icon is blue. If Basic BOFM is disabled for that slot, the icon is gray.
7. If you approve the changes, click **Continue**.

What to do next

The AMM applies the BOFM configuration. As described in "Avoiding address duplication" on page 26, the first phase is to disable the BOFM configuration for all the slots that are about to be reconfigured. The next phase is to apply the new configuration for all of the slots. Finally, Basic BOFM is re-enabled on the appropriate slots. When the process completes, **The configuration file was applied successfully** page displays in the right pane of the AMM Web interface.

Viewing the configuration in a local chassis

After you change the BOFM configuration, you can view it on any of the chassis.

Procedure

1. Login to the AMM Web interface.
2. In the left pane, under **Blade Tasks**, click **Configuration**. The **Configuration** page opens in the right pane. The Configuration page contains an **Open Fabric Manager Parameters** table. In this table, you can see the Basic BOFM overview displayed under these column headings:
   - **Bay** The location of the blade.
   - **Blade Name** The name of the blade at that bay location.
   - **OFM Mode** Either enabled or disabled, as defined by the BOFM configuration file.
   - **Profile** As defined in the configuration file.
   - **System Mgmt Processor OFM Capable** Displays `Yes` if the BMC (blade systems management processor) supports Basic BOFM and `No` otherwise.
   - **BIOS OFM Capable** Yes if the blade BIOS supports Basic BOFM and No otherwise.

     Note: This value is accurate only after the blade boots for the first time after updating the BIOS firmware.
   - **OFM status** If the BMC (blade systems management processor) is BOFM-capable and the blade BIOS is Basic BOFM-capable, the status is `N/A` (Not Applicable), until the blade is powered on for the first time after the BOFM configuration has been enabled. The status (after blade BIOS boot is completed) is: Normal, Error, or Warning. If this blade Basic BOFM mode is disabled or one of the above Basic BOFM capabilities is missing, then the status remains N/A, even after powering on the blade.
3. If you click a blade name, you can see the detailed BOFM configuration page for that slot as was defined in the BOFM configuration file.

What to do next

The Configuration page is divided into sections of device address type: Ethernet, FC, or FC target. In addition, this page displays information about whether devices (attached to this slot) support Basic BOFM and if any address type and value was consumed by any of the slot attached devices. If a Basic BOFM address was consumed, then the Address Status column is Used or Error, otherwise it is Not Used.

The Configuration page optionally displays a table of non-BOFM devices, provided there are such devices attached to the blade. This table has 3 columns: Slot offset, Port, and Address Status. If such a device (characterized by <Slot-offset , Port>) is referred to in the BOFM configuration file under this blade, the Address Status column will be flagged as Warning. Otherwise it will be flagged as N/A.

In general, the addresses that you see on the AMM Hardware VPD page are the current actual addresses. After a change to the BOFM configuration, the addresses are not updated until the next power on. To view the new Basic BOFM addresses, click **Reload MAC/Unique IDs** on the hardware VPD page.

Note: If the FCoE or iSCSI is enabled by the installed adapter, the addresses displayed on the AMM Hardware VPD page are the factory MAC addresses for the two storage ports. However, the BOFM MAC addresses will be applied properly.

Retrieving the current configuration

You can retrieve the current BOFM configuration by selecting **Retrieve the Current Configuration** on the main Open Fabric Manager page.

Procedure

1. Login to the AMM Web interface.
2. In the left pane, under **Blade Tasks**, click **Open Fabric Manager**. The Open Fabric Manager Configuration Management page opens in the right pane.
3. Click **Retrieve the Current Configuration**. The Retrieve Current Configuration page opens in the right pane.
4. You can select **Use the IP addresses that were discovered by the AMM** or **Use AMM IP addresses in a file that I specify**. For more information on these two options, see "Creating a configuration file automatically" on page 22.
5. Click **Retrieve**. The AMM starts to retrieve the information.

What to do next

On completion, your browser launches the File Save window allowing you to save the generated configuration file. If the File Save window does not appear, click **Download the configuration file manually**.

Using Basic BOFM

This topic describes how to deploy Basic BOFM, manage the BOFM configuration file, and use the BOFM CLI command.

Initial deployment

Follow these steps for an initial deployment.

Procedure

1. Update the firmware of the AMM, blade service processor, blade BIOSes and adapters. See "Upgrading firmware" on page 15.
2. Create an initial configuration file. See "Creating a configuration file automatically" on page 22.
3. Download and store the new configuration file in a safe location. This file is the source of your BOFM configuration.
4. Update the configuration file, if required, and save the resulting file.
5. Create a requirements report. Validate that you can apply the BOFM configuration without errors. You can apply the configuration successfully even if no blades are present or if the blade's firmware does not support Basic BOFM. In this case, the AMM stores the configuration on the AMM and it pushes it to the blade when it is inserted or when its firmware is updated. See "Creating a requirements report" on page 27.
6. Apply the BOFM configuration. See "Applying a new configuration" on page 28.

Adding a new chassis to the domain

To add a new chassis to the domain, you must add the BOFM configuration to the BOFM configuration file. You can either add it manually or use the generate feature to create a new configuration file. In that case, define the ranges so that they do not contain addresses that are already used by the current configuration.

About this task

Procedure

1. Create a file where each line contains the IP address or hostname of the new chassis that you wish to add to the domain.
2. Create a new configuration file using the list you just created.
3. After creating the new file, you can append it to the current file using a spreadsheet or text editor.
4. Apply the configuration.

What to do next

When you apply the combined file, only the changes to the new chassis are applied assuming that for the other chassis the configuration in the file matches the existing configuration.

Replacing a blade in the same slot

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

Swapping addresses between blades

To swap the addresses of one blade to a different blade in a different slot (potentially a different chassis), you can move the BOFM configuration from the first slot to the second.

Before you begin

Procedure

1. Edit the BOFM configuration and swap the configurations of the two slots.
2. Apply the new configuration. Only the configuration of these two slots are updated.

What to do next

Note:

- You must manually swap the boot sequence of the two slots (if swapping is necessary).
- In cases where slot based configuration has been used on the switches, such as VLAN for Ethernet or Zoning for Fibre Channel, update those configurations, also.

Replacing AMM IP addresses

The BOFM configuration is defined per AMM IP address. If you change the IP of the AMM in a chassis and reapply the same BOFM configuration file, then the

BOFM configuration changes. For example, assume that Chassis-A uses IP-A, and Chassis-B uses IP-B, and you apply a BOFM configuration for these two chassis. If you swap the IPs so that Chassis-A uses IP-B, and Chassis-B uses IP-A, then re-apply the same BOFM configuration file, the BOFM configuration is swapped between the two chassis.

Replacing the AMM in a single AMM environment

You can replace the AMM in a single AMM environment.

About this task

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

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

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

Note: You might have to wait longer if the AMM you insert in the standby slot does not have the same firmware level as the primary. In that case, the standby AMM is flashed first and then the data is synchronized.

CLI command

You can apply a new configuration using the **bofm** CLI command. To use the command, you must have a tftp server available for uploading the configuration file.

Format

bofm -d [on|off] | -i <ip> |-l <file name> | -p [on|off] | -v

Options

-d: check duplicate [on|off]

-i: ip of tftp server

-l: configuration file name

-p: check blade power state [on|off]

-v: verbose mode

Usage

Supply the tftp server IP address in the –i option, and the configuration file name in the –l (similar to the **update** CLI command). Adding the **–d off** option causes BOFM to ignore duplicate addresses in the configuration file. Adding the **–p off** option causes the BOFM to apply the configuration even on powered-on blades. These parameters default to "on".

Chapter 5. Advanced BOFM

This topic describes how to install and use Advanced BOFM.

Installing Advanced BOFM for Windows

To install Advanced BOFM for Windows, complete the following steps.

About this task

Procedure

1. Download the installation file (OFM40L.exe).
2. Using an account with either local or domain **Administrator** authority, log on to the operating system.
3. Run the install program.

What to do next

You must disable any earlier versions of BOFM that you are using.

Installing Advanced BOFM for Linux

To install Advanced BOFM for Linux, complete the following steps.

Procedure

1. Download OFM40.bin.
2. Using an account with **root** authority, log on to the operating system.
3. Run the install program.

What to do next

You must disable any earlier versions of BOFM that you are using.

Importing configuration information into to Advanced BOFM

You can import configuration information from previous releases of BOFM into a new template for Advanced BOFM. Only configuration data can be imported from BOFM V1.0, V2.x, and V3.x to Advanced BOFM V4.x.

To import configuration information from a previous version of BOFM into a new Advanced BOFM V4.x template, complete the following steps:

1. Export the configuration template from the previous version of BOFM.
2. Disable the previous version of BOFM.
3. Install Advanced BOFM V4.x.
4. Import the configuration template to Advanced BOFM V4.x.

Using Advanced BOFM

This topic contains information about using Advanced BOFM, including launching the program, discovering a chassis, creating a standby blade pool template, and applying a failover template.

Important: You must configure AMM to enable Advanced BOFM access. You must set the following network protocols on the AMM Web interface:

File Transfer Protocol (FTP)

1. From the AMM Web interface access the **MM Control** → **Network Protocols** page.
2. Click the **File Transfer Protocol (FTP)** link and make sure that it is set to **Enabled**.

TCP Command Mode Protocol

1. From the AMM Web interface access the **MM Control** → **Network Protocols** page.
2. Click the **TCP Command Mode Protocol** link and make sure that the Command mode is set to 20 connections.

Simple Network Management Protocol (SNMP)

1. From the AMM Web interface access the **MM Control** → **Network Protocols** page.
2. Click the **Simple Network Management Protocol (SNMP)** link and make sure that **SNMP traps** and **SNMPv1 agent** are enabled and configured.

The following table lists the default protocol port numbers used by Advanced BOFM:

Table 5. Default protocol port numbers used by Advanced BOFM

Port number	Protocol	Endpoint
21	FTP	AMM
23	TELNET	Advanced BOFM server
161, 162	SNMP	Advanced BOFM server
50990	SNMP trap	Advanced BOFM server
6090	TCP/IP (command mode)	AMM
Note: You can change the SNMP trap port number by editing `server.prop` in `C:\Program Files\OFM\data\`.		

Starting Advanced BOFM

About this task

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

Procedure

1. Navigate to the program shortcut.
2. Select **Adv BOFM OFM Combined Server-Client** and wait until a console is displayed, which indicates that the server has started.

Adding chassis inventory

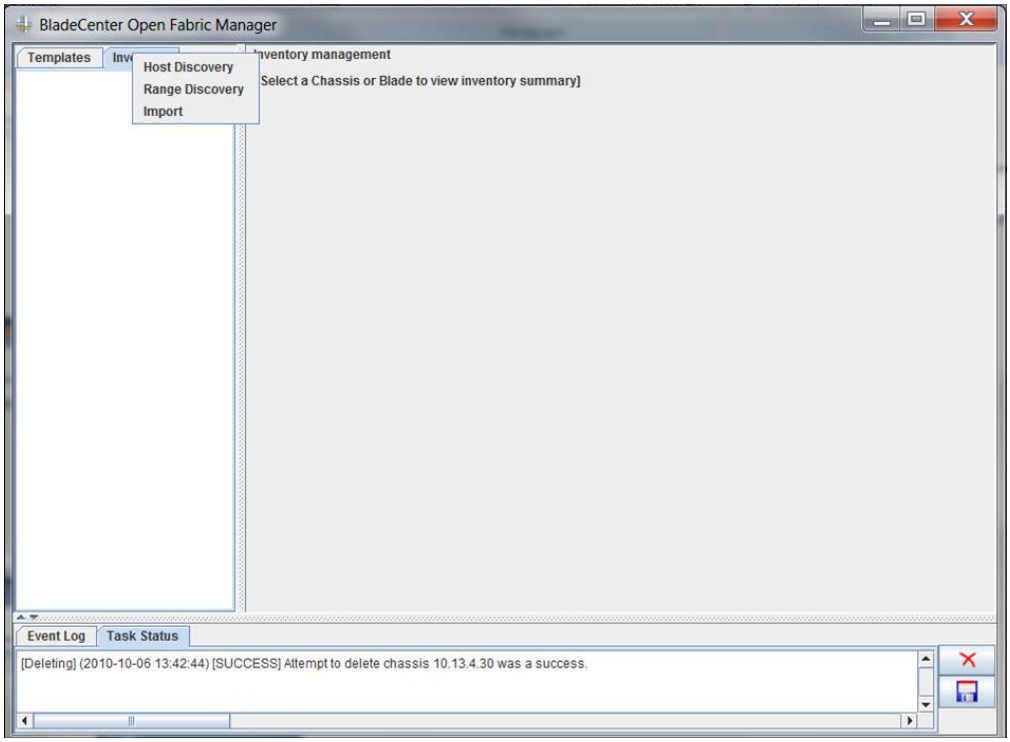
You can add a chassis from a single IP address, add multiple chassis from a range of IP addresses, or import chassis from a file containing IP addresses.

About this task

To add one or more chassis, complete the following steps.

Procedure

Right-click the **Inventory** tab and select a choice to add inventory.



- **Host Discovery**

  Select this choice to add a chassis from a single IP address.
- **Range Discovery**

  Select this choice to add a chassis from a range of IP addresses.
- **Import**

  Select this choice to import IP addresses from a file.

Managing chassis inventory

You can view information about a chassis, enable or disable BOFM on a chassis, and perform other management activities.

About this task

To perform chassis management activities, complete the following steps.

Procedure

1. Select the **Inventory** tab.

2. Select a chassis and view the **Summary** tab, which shows the name, IP address, and other summary information.
   - **Properties**

     Select this choice to view login information for a chassis.
   - **BOFM Status**

     Select this choice to view the status of a chassis. Also, select this choice to enable or disable a blade.
   - Right-click a chassis and select from the following choices:
     - **Login**

       Select this choice to log in to a chassis. When using the login function, consider the following information.
       - The user name and password are defined in the chassis properties.
       - If a chassis is **Undiscovered, Generic**, you must log in to collect the inventory.
     - **Get Inventory**

       Select this choice to collect and refresh all inventory.
     - **Delete**

       Select this choice to remove the chassis and all associated blades from inventory.
     - **Rename**

       Select this choice to create an alias for the chassis.
   - Double-click a chassis to view the blades associated with the chassis.

Managing blade inventory

You can view information about the blades associated with a chassis.

About this task

To view information about the blades associated with a chassis, complete the following steps.

Procedure

1. Select the **Inventory** tab.
2. Double-click a chassis to view the blades associated with the chassis.
3. Select a blade to view the name, slot, status and other general information.

Managing switch inventory

You can view information about the switches associated with a chassis.

About this task

To view information about the switches associated with a chassis, complete the following steps.

Procedure

1. Select the **Inventory** tab.
2. Double-click a chassis to view the inventory associated with the chassis.
3. Select a switch (IO Module) and view the name, IP, slot, UUID, and other general information in the **Summary** tab.

4. Click the **Properties** tab to set the Telnet login information to access the switch. The login information varies depending on the switch.

   Note: You must set the Telnet login information in this screen for the BOFM server to access and configure the switch during a failover.

Creating or importing an address manager template

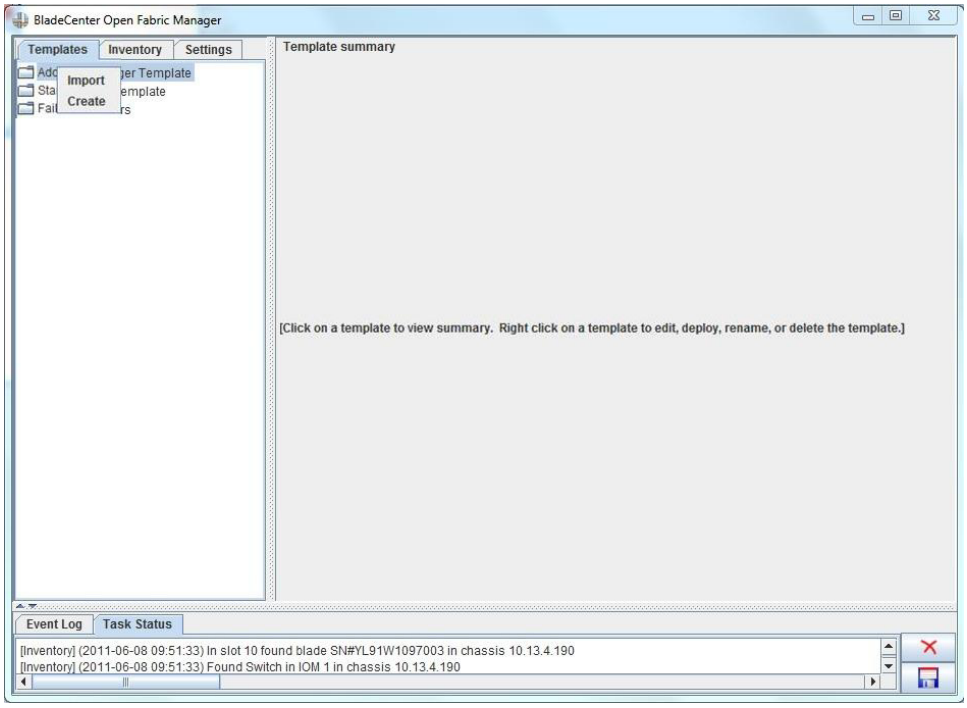
You can create or import an address manager template.

About this task

To create or import an address manager template, complete the following steps.

Procedure

1. Select the **Templates** tab.
2. Right-click **Address Manager Template**.



3. Select the **Import** or **Create** choice:
   - **Import**

     Select this choice to import an existing Blade Address Manager .csv configuration file. Specify a name for the imported file. Use this as a starting point to edit, then create a new configuration file based on the imported configuration.
   - **Create**

     Select this choice to add a chassis to the configuration and specify a name for the template.
4. Select the **Ethernet**, **Fibre Channel**, or **SAS** tab to enter or view the generic configuration information.
   - **Ethernet**

– To assign Ethernet MAC addresses to bays, click the **Enable** check box. Then select **IBM** in the drop down list to automatically assign addresses. Select **User Defined** in the drop down list to edit the MAC address range.

Some Ethernet expansion cards have a range of MAC addresses per port. The range is defined by specifying two MAC addresses per port: MAC A and MAC B. To define a range of MAC addresses for a port, click the **Use a range of MAC addresses** check box. Then, specify a value from 1 to 255 in the **Range** field.

Note: The default values allow the JS22 and JS12 onboard HEA Ethernet adapter to use virtual addresses. A ranging Ethernet address must be applied to port 1 and the minimum value allowed is 16. Even though the 16 MAC range for the onboard HEA adapter is declared via port 1, the actual routing of the 16 MAC range is determined by the operating system configuration.

– Define the generic VLAN ID.

– Define port ranging and applicable ports.

– Select **Use virtual ports** to include virtual ports in the template. Virtual ports allow additional virtualization across physical ports and use the Ethernet address range that is assigned to the physical ports. Each virtual port can have its own associated MAC address or VLAN ID. Physical ports 5 and 7 each have four associated virtual ports that share the bandwidth of the physical ports.

- **Fibre Channel**

  – To assign Fibre Channel WWN addresses to bays, click the **Enable** check box. Select either **Qlogic** or **Emulex** to automatically assign addresses. Select **User Defined** to edit the Fibre Channel address range.

  Valid address range for Qlogic:

  First port: 21:80:00:E0:8B:0X:XX:XX

  Second port: 21:81:00:E0:8B:2X:XX:XX

  Valid address range for Emulex:

  WWNN: 2F:FE:00:00:C9:XX:XX:XX through 2F:FF:00:00:C9:XX:XX:XX

  WWPN: 2F:FC:00:00:C9:XX:XX:XX through 2F:FD:00:00:C9:XX:XX:XX

  – Define WWN stepping.

  – Select and define the boot targets.

- **SAS**

  – To assign storage target WWPN addresses to bays, click the **Enable** check box. Then, select the Vendor type and enter the range of addresses.

  IBM Valid address range: 50:05:07:60:1A:80:00:00h to 50:05:07:60:1A:BF:FF:FFh

  LSI Valid address range: 50:00:62:B0:00:11:17:00h to 50:00:62:B0:00:12:16:FFh

  – Define SAS stepping.

  – Select and define the boot targets.

5. Click **Next** to view Advanced Settings. Use Advanced Settings to change the configuration settings for an individual chassis, blade, or port.
   - Enable or disable individual blades.
   - Define additional blade offsets for multi-wide blade support.
   - Edit settings for individual ports:

     Enable or disable the port

Modify associated addresses

Modify VLAN IDs

- Edit boot targets for individual blades.

Managing an address manager template

You can view information about an address manager template, edit a template, deploy a template, and perform other management activities.

About this task

To perform address manager template activities, complete the following steps.

Procedure

1. Select the **Templates** tab.
2. Select **Address Manager Template**.
3. Select a template and view the summary page.
4. Right-click a template and select from the following choices:
   - **Edit**

     Select this choice to modify the existing template values.
   - **Append**

     Select this choice to add new data to an existing template.
   - **Clone**

     Select this choice to create a duplicate of an existing template.
   - **Rename**

     Select this choice to rename an existing template.
   - **Export**

     Select this choice to save the template to a file.
   - **Deploy**

     Select this choice to send the template to the chassis.
   - **Delete**

     Select this choice to remove the template.

Creating a standby blade pool template

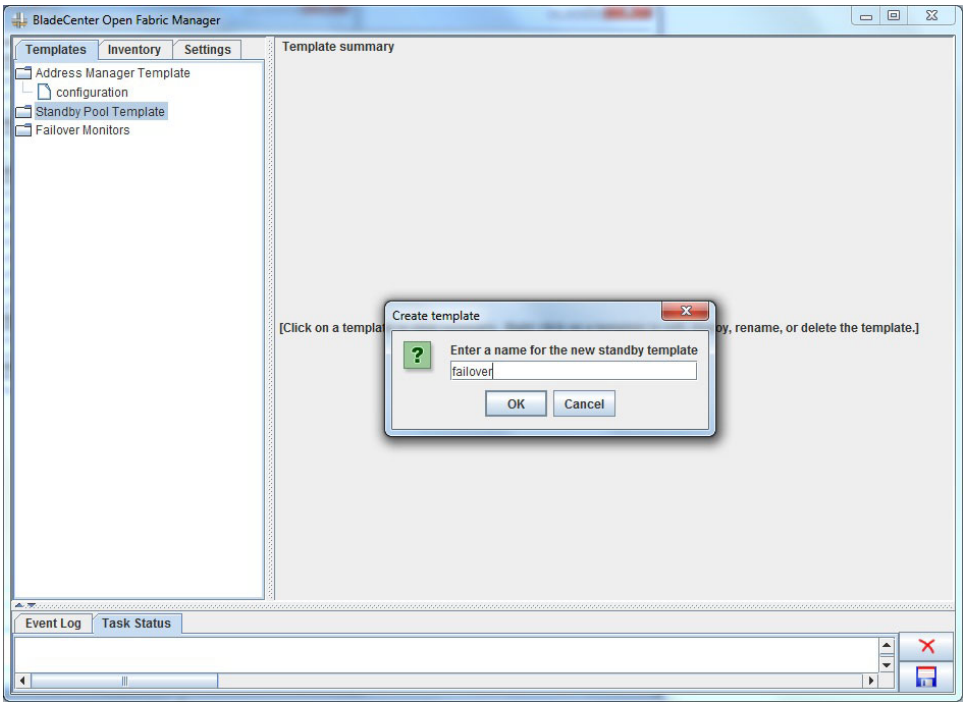
You can create a standby blade pool template using the template wizard.

About this task

To create a standby blade pool template, complete the following steps.

Procedure

1. Select the **Templates** tab.
2. Right-click **Standby Pool Template**.
3. Select **Create**.



4. Define a name for the template and click **OK**.
5. Select the blades to be used for failover in the Available blades window and click **Next**.
6. On the Advanced Settings window, select the failover options to be used by the standby blade pool template, then click **Finish**. When in use, failover attempts to match the criteria you define in the Advanced Settings window. Then, failover is attempted on the blades in the order they appear in the Selected blades window.
7. The Template Summary window shows the settings that you have selected.

Managing a standby blade pool template

You can view a summary of a standby blade pool template, manually enact a failover of a BOFM template, and perform other management activities.

About this task

To perform standby blade pool template management activities, complete the following steps.

Procedure

1. Select the **Templates** tab.
2. Under **Standby Pool Template**, select a chassis and view the Template summary page.
3. Right-click a template and select from the following choices:
   - **Edit**

     Select this choice to modify the existing values.
   - **Clone**

     Select this choice to create a duplicate of an existing template.
   - **Rename**

Select this choice to rename an existing template.

- **Manual failover**

  Select this choice to manually select one or more target blades to use for failover. When you use manual failover, consider the following information:

  – The configuration of the blade you select is sent to one of the standby pool blades.
  – Manual failover selects the first match from the standby pool.
  – You can select multiple blades for manual failover.
  – You cannot failover to a blade that is already enabled.

- **Delete**

  Select this choice to remove the template.

Creating a failover monitor

You can create a failover monitor using the monitor wizard. Failover monitoring allows you to select events for which to monitor and automatically enact blade failover when an event occurs. You also select a standby pool.

Before you begin

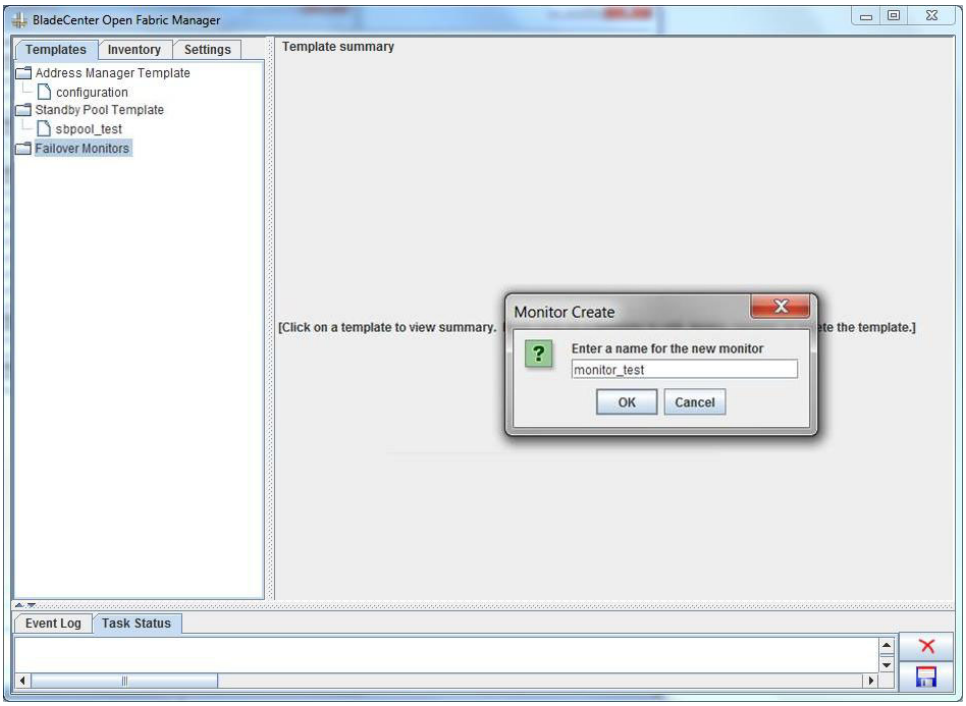
Select to monitor the following events:
- Microprocessor failure
- Blade removal
- Hard disk drive failure
- Blade denied power
- Memory failure
- Voltage warnings
- Predictive failure analysis (PFA) events

About this task

To create a failover monitor, complete the following steps.

Procedure

1. Select the **Templates** tab.
2. Right-click **Failover Monitor**.
3. Select **Create**.



4. Define a name for the monitor template and click **OK**.
5. Select a standby pool and click **Next**.
6. Select the blades and events to monitor and click **Save**.

Managing a failover monitor

You can view a summary of a failover monitor, start or stop monitoring, and edit or delete a failover monitor.

About this task

Note: To avoid a blade automatic restart after failover, you need to stop monitoring a blade, complete the restart, and resume monitoring a blade. See the following steps to stop and resume a failover monitor.

To perform failover monitor management activities, complete the following steps:

Procedure

1. Select the **Templates** tab.
2. Under **Failover Monitor**, select a failover monitor and view the Template summary window.
3. Right-click a failover monitor and select from the following choices:
   - **Stop monitoring**

     Select this choice to stop monitoring using the configuration.
   - **Resume monitoring**

     Select this choice to resume monitoring using the configuration.
   - **Delete**

     Select this choice to remove the failover monitor.

Deploying a standby blade pool configuration template manually

You can deploy a standby blade pool configuration template manually.

Procedure

1. Right-click on the desired standby pool template.
2. Select **Manual Failover**.
3. In the failover wizard, select the active blade to failover.
4. Click **Failover**.

What to do next

When the Standby Blade Pool is being applied to an active blade, the software communicates with the active blade's corresponding chassis management device (the Advanced Management Module) to read the currently assigned addresses associated with that blade. These addresses are applied to the chassis management device associated with the selected standby blade's chassis slot.

When applying the Standby Blade Pool to an active blade, the Ethernet Switch Module's port based VLANs are migrated from the active blade to the standby blade. The software connects to all of the Ethernet switches in the active blade's chassis and reads the VLAN port information associated with the active blade. The software connects to all of the Ethernet Switches in the standby blade's chassis and applies these port based VLANs to the Ethernet switches.

The Advanced BOFM performs the following checks prior to implementing a failover from the source blade to the standby blade:

1. Checks for matching standby blade machine type
2. Check for matching standby blade model type
3. Check for standby blade initial power state to be off
4. Check for blade width
5. Determine whether to migrate the switch settings from the source blade to the switch associated with the standby blade

Backing up Advanced BOFM data

You can create a backup of the Advanced BOFM data.

Procedure

1. Select the **Settings** tab.
2. Click **Data**.
3. Click the **Backup** tab specify the directory information in the fields.
   - **Directory of source data**

     Click **Browse** to locate the source directory from which you want to back up the data.
   - **Location of backup files**

     Click **Browse** to locate the destination directory to which you want to store the backup files. Data is archived in a .jar file.
4. Click **Backup**.

Migrating Advanced BOFM data

You can convert data from Advanced BOFM version 4.0 or later to the data format supported by the current Advanced BOFM version.

Procedure

1. Select the **Settings** tab.
2. Click **Data**.
3. Click the **Migration** tab. specify the directory information in the fields.
4. In the **Directory of source data** field, click **Browse** to locate the directory whose data you want to convert.
5. Click **Migrate**. When you restart the BOFM server, data in the current data directory will be replaced by the converted data.

Chapter 6. Solving problems

This topic provides basic troubleshooting information to help you solve some common problems.

If you cannot locate and correct a problem by using the information in this topic, see “Getting help and technical assistance,” on page 63.

Basic BOFM troubleshooting

This topic describes troubleshooting information for Basic BOFM.

Events

This topic describes some AMM events that you might encounter with Basic BOFM.

- If the BOFM configuration changes for a slot, then an information event is generated for that slot.
- If a slot has BOFM configuration enabled and the system management processor of the blade in that slot does not support BOFM, then a warning event is generated.
- If a slot has BOFM configuration enabled and the blade's BIOS in that slot does not support BOFM, then a warning event is generated.
- If a slot has BOFM configuration enabled and any device in that slot does not support BOFM, thean a warning event is generated.
- If any of the adapters reported a BOFM error, then a warning event is generated.
- If the AMM was unable to apply a BOFM configuration to a blade for which the system management processor supports BOFM, then the blade is not given power permission and an error event is generated for that blade.
- If the AMM cleared the BOFM configuration after moving to a new chassis, then a warning alert is generated.
- If the AMM discovered that a BOFM configuration is in use by a blade that is powered on and it is different from the configuration defined on the AMM, then a warning event is generated.

BOFM address usage

Follow these procedures in the order in which they are presented to diagnose a problem with the BOFM addresses:

1. Check the AMM website:
   a. Select **Blade tasks** -> **Configuration** -> **Open Fabric Manager**.
   b. Click the name of the blade.
   c. Verify that the BOFM configuration is enabled.
   d. Verify that the blade supports BOFM.
   e. Verify that the blade system management processor supports BOFM. If necessary, upgrade the firmware of the Blade System Management processor.
   f. Verify that the blade BIOS supports BOFM. If necessary, upgrade the BIOS firmware.
2. The BOFM status for the blade is `N/A`:

a. If the blade is powered off:
   1) Power it on.
   2) Wait for the OS to reboot.
   3) Check the BOFM status again.
b. If the OS is running:
   1) Reboot the blade.
   2) Check the BOFM status again.

3. Check the address status:
   a. If the address status for the adapter is `Used` and the addresses are not actually used, replace the adapter.
   b. If the address status for the adapter is `Error`, replace the adapter.
   c. If the address status for the adapter is `Not Used`, verify that the address type matches the adapter type.

Configuration failure scenarios

This topic describes some errors that you might encounter when applying your BOFM configuration.

Parsing failures

If the configuration file contains errors while being parsed, the AMM Web interface displays the Open Fabric Manager Configuration Failure page. The page contains a table that shows the line number of each error and a brief description of the error. You must fix all of the errors in the configuration file before continuing.

For a detailed description of these errors, see “Error messages” on page 50.

Connection failures

If the AMM is unable to connect to any of the chassis' that are listed in the configuration file, the Web interface displays the Open Fabric Manager Configuration Failure page. The page contains a table that shows the IP address of the chassis it is unable to connect to. If you want to ignore this chassis and apply the configuration anyway, you can press **Ignore**. Ignoring a chassis might result in duplicate addresses, because the AMM cannot compare the addresses against the ones that are being used by the unreachable chassis. You can also suppress this warning by selecting the **Continue on error** advanced option on the Apply a Configuration page.

Login failures

The AMM uses the user name and password that you used to login to the current AMM to attempt to login to the other AMMs. If the AMM fails to login to the other AMMs using these credentials, the Web interface displays the Open Fabric Manager Authentication Failure page. This page gives you the option to provide an alternate user name and password for the chassis. If you check the **use this user and password for the rest of the AMMs** box, this user name and password combination is attempted on all other chassis to which the AMM fails to connect.

After you fill in the user name and password, click **Retry**. If you wish to ignore this chassis and continue to apply the configuration anyway click **Ignore**. If you wish to ignore all the chassis to which the AMM fails to login click **Ignore All**. Ignoring a chassis might result in duplicate addresses since the AMM cannot

compare the addresses against the ones that are being used by the unreachable chassis. You can also suppress this warning by selecting the **Continue on error** advanced option on the Apply a Configuration page.

Important: You can get a **login failed** message in cases where all the TCP Command Mode connections to the AMM are in use. If you get the login failed message when using a valid user name and password, make sure that the AMM connection limit of the AMM you failed to login to is more than the number of connections in use (if, for example, Director is using one connection). This is controlled through the AMM Web interface on MM Control→Network Protocols→TCP Command Mode Protocol.

Retrieve failure

If the AMM fails to retrieve the BOFM configuration from any of the chassis, the Web interface displays the Open Fabric Manager Retrieve Failure page. Failure to retrieve the BOFM configuration usually occurs when the other chassis' do not support BOFM or if there are communication errors.

If you want to ignore this chassis and apply the configuration anyway, you can press **Ignore**. Ignoring a chassis might result in duplicate addresses, because the AMM cannot compare the addresses against the ones that are being used by the unreachable chassis. You can also suppress this warning by selecting the **Continue on error** advanced option on the **Apply a Configuration** page.

Blade power state failure

Before applying a configuration, the AMM validates that all the blades that are about to be re-configured are powered off. If any of these blades are powered on, the Web interface displays the Open Fabric Manager Configuration Error - Found Powered On Blades page. The page contains a table that shows the blades that are currently powered on (indicated by a red X icon).

You can optionally force the configuration changes to these powered on blades by clicking **Force**. This keeps the blades powered on and causes the configuration to be applied to those blades during their next reboot. Forcing the configuration might result in duplicate addresses. You can also force the configuration changes by selecting the **Force the configuration to be applied to powered on blades** advanced option on the Apply a Configuration page.

Disable BOFM failure

As described in “Avoiding address duplication” on page 26, before applying the new configuration, the AMM disables the BOFM configuration for the slots that are about to be re-configured. If there is a failure disabling the BOFM configuration for any of the blades, the Web interface displays the Open Fabric Manager Configuration Failure page. The page contains a table that shows the blades that could not be disabled (indicated by a red X icon). A green check mark icon indicates blades that were properly disabled.

Important: This is a critical error so you must resolve this issue before continuing. If it is not resolved immediately, blades in your BOFM environment can be disabled when that was not your intent.

Apply BOFM failure

If there is a failure applying the BOFM configuration to any of the slots, the AMM continues to apply the BOFM configuration to all the other slots. After the process completes, the Web interface displays The configuration file could not be successfully applied to one or more blades page. The page contains a table that shows the blades to which the configuration could not be applied (indicated by a red X icon). If you apply the configuration again, the AMM attempts to configure only the slots that it failed to configure on the previous attempt.

Error messages

This topic describes error messages you might encounter when working with Basic BOFM.

Requirements report errors

The following are causes of error messages that you might encounter.

- The following firmware requires updating:
  - AMM firmware
  - Baseboard Management Controller (BMC)
  - Blade BIOS
  - HBA firmware
- Communication error to the blade or user doesn't have permission for BOFM on a blade.

Parsing errors

The following table describes the parsing errors that can be generated when processing the BOFM configuration file.

Table 6. Parsing errors

Error message	Description
Assuming boot type `None`	The “Boot Type” field has been left empty – the system assumes a value of “none” and continue processing the line.
Assuming mode `Ignore`	The “Mode” field has been left empty – the system assumes a value of “Ignore” and continue processing.
Attempt to add multiple boot targets to a blade with the same priority	A single priority value for a target can only be used once for a given slot.
Attempt to redefine slot	There are multiple lines defining a slot. A slot must be defined before it is used and cannot be defined more than once.
Attempt to use a slot that has not yet been defined	A slot must be defined before it used. The BOFM configuration file contains a reference to a slot that has not been defined when referenced.
Attempt to write non-Ethernet data to Ethernet port	The BOFM configuration file includes an attempt to define a non-Ethernet port to an Ethernet-only port number (1 or 2).
Bad boot type	The “Boot type” string cannot be parsed.
Bad entry type	The entry type (One of: BladeCenter, Slot, Eth, FC, FCTarget) was not recognized.

Table 6. Parsing errors (continued)

Error message	Description
Bad IP address	The IP address was incorrectly formed or, in the case of a hostname, the DNS lookup failed.
Bad offset number	Cannot parse the offset number, or the number is out of range. (Offsets must be in the range 0-3)
Bad port number	Cannot parse the port number, or the number is out of range. (Ports must be in the range 1-8 for Ethernet ports or 3-8 for all other types)
Bad slot number	Cannot correctly parse the slot number or it is out of range. The exact range depends on the BladeCenter type (BCH, BCS, BCHT), but is never less than 1 or more than 14. This error can also occur when the slot field does not have a closing comma.
Bad target priority - must be first or second	Cannot parse the target priority, or it was out of range (first/second). Targets can only be set as the first or second priority.
Bad value in mac/wwpn/wnn	The value in the EUI field is correctly formed but contains characters that cannot be interpreted as a hexadecimal number. EUI format is a 16-character hexadecimal value with the leading prefix of *eui*, for example: eui:*0123456790ABCDEF*.
Bad vlan number	Cannot parse the VLAN number (not a number or similar problem).
Could not interpret the LUN value	The LUN value in the FCTarget was not correct.
Failure opening the configuration file	The BOFM configuration file could not be opened: probably a bad file name or path, or a problem with file permissions.
Failure reading the configuration file	The BOFM configuration file could not be read until the end.
Incomplete Line	This line is missing required fields.
Input line is too long	The maximum length for a single line in the BOFM configuration file is 512 characters. Lines longer than this are discarded.
Insufficient addresses in the range for chassis	The range of addresses defined for this BOFM configuration file is not sufficient for the number of chassis required.
Invalid integer	Cannot parse an integer number.
mac or wwnn field is too short or too long	Too few or too many bytes in an EUI field.
Maximum value is 0xfffffffe - for longer values use EUI notation	LUN values can be specified in decimal, hexadecimal or EUI formats. Values above 4294967295 (0xffffffff) must be specified as an EUI.
No closing quote	One of the fields on this line is missing a closing quote. To prevent problems the line is ignored.

Table 6. Parsing errors (continued)

Error message	Description
Profile is too long and has been truncated	The profile string cannot be longer than 32 characters.
Second reference to a specific port or target	A port or target has been reused with the same type (for example, Eth, FC, etc.). Ports and targets can only be defined once for a particular type.
Too many BladeCenters	The maximum number of BladeCenters that can be processed from a single BOFM configuration file is 100.

Advanced BOFM troubleshooting

This topic describes troubleshooting information for Advanced BOFM.

Common problems

This topic describes common problems that might occur when you use Advanced BOFM.

Table 7. Advanced BOFM common problems

Problem	Solution
BOFM tasks not available on AMM.	Make sure that a Basic BOFM license is installed on the AMM.
Unable to download BOFM Advanced software.	Check the product activation code shipped with your order. To download BOFM Advanced, go to http://www.ibm.com/systems/bladecenter/hardware/openfabric/openfabricmanager.html.
An address manager template configuration did not apply.	Power off the blade or select the template power-on override option.
Failover monitor deployment failed.	Check for a mismatch between the template configuration and the hardware configuration.
Failover monitor fails to power on the standby blade.	Make sure that you set the blade OFM mode to **Disable** before applying the template.

Problems when you create or apply a standby blade pool

This topic describes error conditions that might occur when you create a standby blade pool or apply the standby blade pool.

Table 8. Blade address configuration creation and application problems

Problem	Solution
Template failed to be applied.	1. Check that blades are not powered on. 2. Check that you have discovered all of the chassis in the domain. 3. Check that you do not have address duplications in the domain.
No chassis show up in the Available chassis box	Make sure that the chassis have been completely discovered.

Table 9. Standby blade pool creation and application problems

Problem	Solution
No blades show up in the available blades section.	Make sure that the blades and the BladeCenter chassis have been completely detected.
Only the blades from one chassis appear in the available blades section.	When creating a standby pool through a targeted action only the blades from that chassis appear in the available blades section. To see all of the blades that have been detected, start BladeCenter Configuration Manager through an un-targeted action, such as clicking on the task.
Standby Blade Pool failed after manually applying to a blade.	1. Check that the blades in the standby pool have the same model and type as the source blade. 2. Check that the standby blade pool does not contain only the source blade (a failover attempt to the same blade always fails). 3. Check that the blades in the standby blade are powered off. 4. Make sure that the Director plug-in for your network switches has been installed.
Standby Blade Pool failed to be applied after creating an event action plan and applying the event action plan to a blade.	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 blade. 3. Check that the event was sent to the blade object and not just to the BladeCenter chassis.

Chapter 7. BOFM To IBM Fabric Manager Migration

This chapter summarizes the steps necessary to migrate an existing, licensed BOFM Advanced configuration to a licensed IBM Fabric Manager (IFM) configuration.

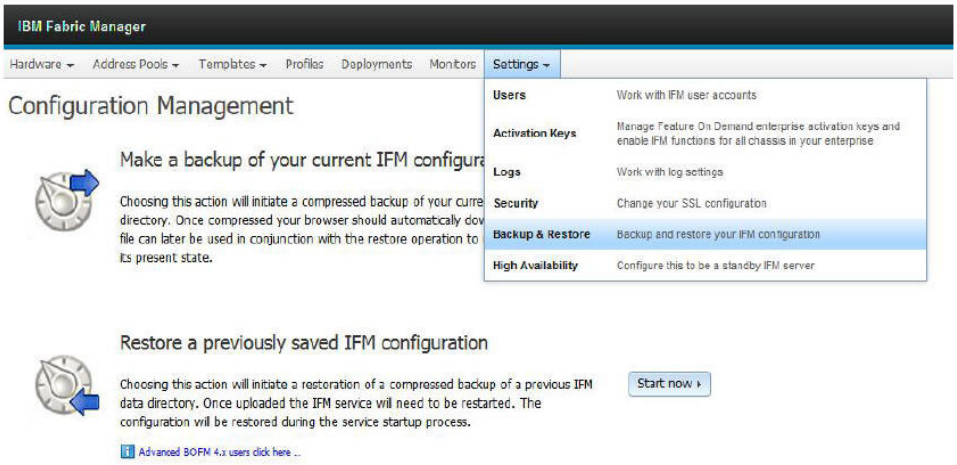
Attention: Starting from version 66E, 66F, and 66K, there will no longer be any support for BOFM. Last supported version is 66G. BOFM will be fully replaced by IFM.

Steps for BOFM to IBM Fabric Manager (IFM) migration

To migrate from BOFM to IFM, complete the following steps.

Procedure

1. Install IFM on your system. Typically this is a desktop or laptop used to configure or manage/monitor your BladeCenter chassis.
2. Start IFM (navigate to the program shortcut "Start IFM Server") and Login.
3. From the web GUI, navigate to "Settings" and then choose "Backup & Restore".



4. Beneath the "Restore a previously saved IFM configuration" click on the "Advanced BOFM 4.x users click here..."

5. Per the instructions -

Process overview
IBM Fabric Manager (IFM) can be used to migrate existing Advanced BOFM 4.x data to IFM via the configuration restore mechanism. The process requires compressing your current BOFM data into an archive file, and then uploading it to the IFM server just as you would any IFM configuration backup file. The steps below describe how to create this archive on both Windows and linux platforms
For Windows GUI users:
Open Windows Explorer
Navigate to the BOFM home directory. This can be changed during installation, but default values are:
For v4.0 **%SYSTEMDRIVE%\Program Files\OFM**
For v4.1 **%SYSTEMDRIVE%\ofm**
Open the data directory
Select all the displayed files
Right click on any of the now highlighted files
Hover over Send to
Click Compressed (zipped) folder
Name the file data.zip.
The new data.zip file is the one that will be uploaded to the IFM restore mechanism.
For linux users:
Open a terminal
Change directory to the BOFM home directory. This can be changed during installation, but the default value is ~/usr/OFM
Change directory to the data directory inside this directory
Run this command: zip -r data.zip *
The new data.zip file is the one that will be uploaded to the IFM restore mechanism.

6. The previous Advanced BOFM CSV files are now loaded into IFM as a deployment and can be pushed to your target HW. Per the IFM instructions –

   "Any deployed profiles in the Deployments page is ready to be pushed. A push allows the deployed profile to be sent to the chassis which in turns sends the info to the bay where the powered off server resides. Before any push action, 'IFM Mode' should be enabled, view the Hardware Devices help topic for more about proper setup for consumption."

7. Manually create failover monitors.
   a. Discover the monitored chassis/blades.
   b. Create hardware pools for active blades and standby blades.
   c. Create failover monitors.

BOFM Basic to IFM Migration Option 1 – Do Nothing

This topic describes BOFM Basic to IFM Migration Option 1.

- When to choose this option.
  - There will be No Hardware Reconfiguration of the BladeCenter.
  - The BOFM Configuration Does Not Need to Change.
- The BOFM Configuration Continues to be Stored on the AMM.
  - BOFM Configuration is Synchronized with Redundant AMM.
- Replacement Blades of same Type etc. will pickup BOFM Configuration from AMM.
  - BOFM Data Block Stored on BladeCenter AMM is compatible with IFM.
- Will Not be Able to Use all IFM Features.
- Will Not be Able to Use All IFM Supported Hardware.

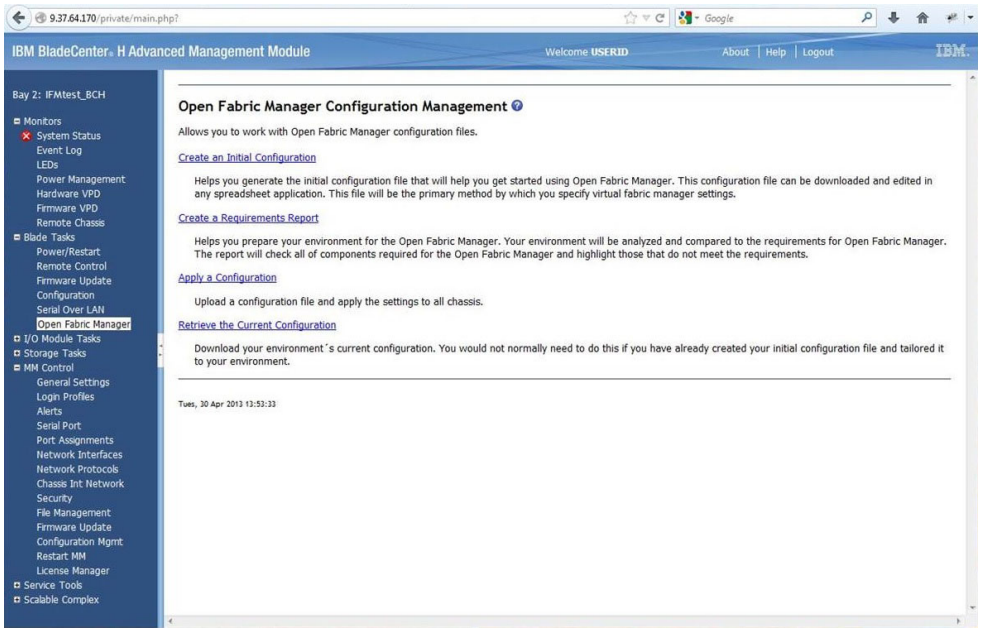
BOFM Basic to IFM Migration Option 2 – Import CSV File

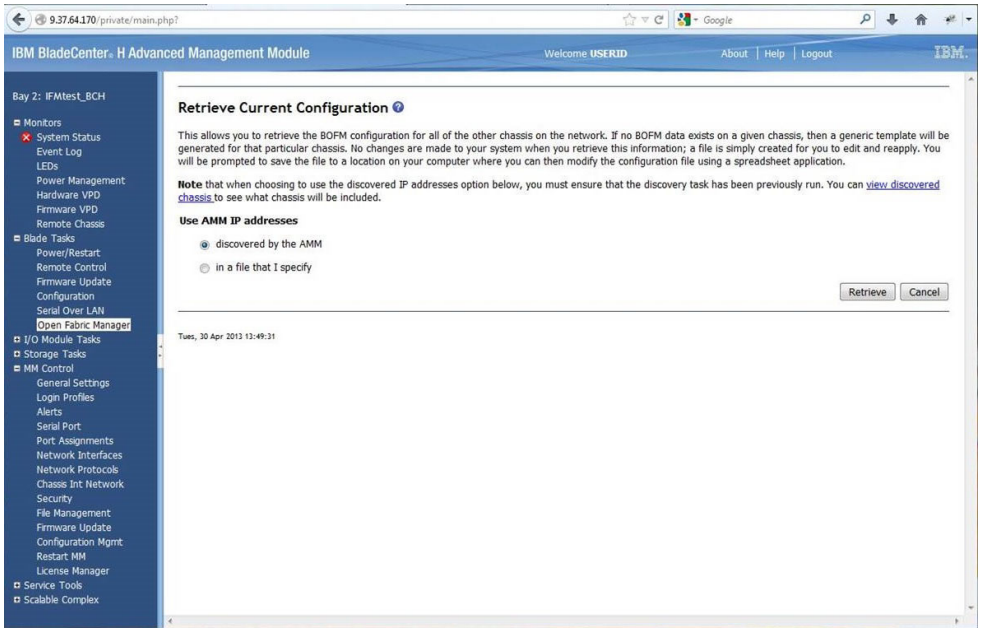
This topic describes BOFM Basic to IFM Migration Option 2.

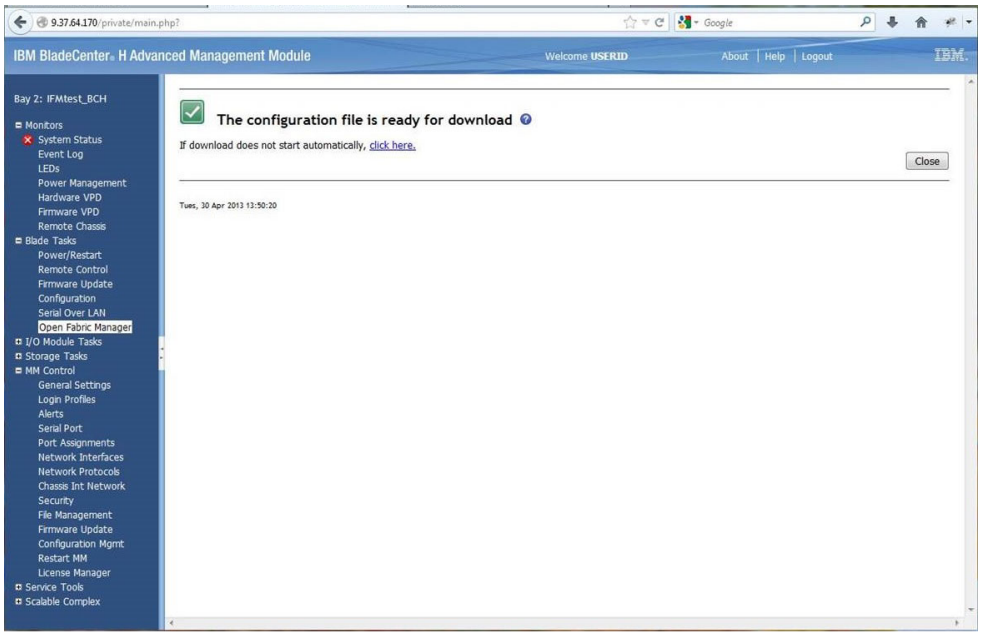
- When to choose this option.
  - BOFM Basic Configuration has been Downloaded from AMM and Stored in CSV File.
  - There will be No Hardware Reconfiguration of the BladeCenter.
- CSV File Imported in IFM.

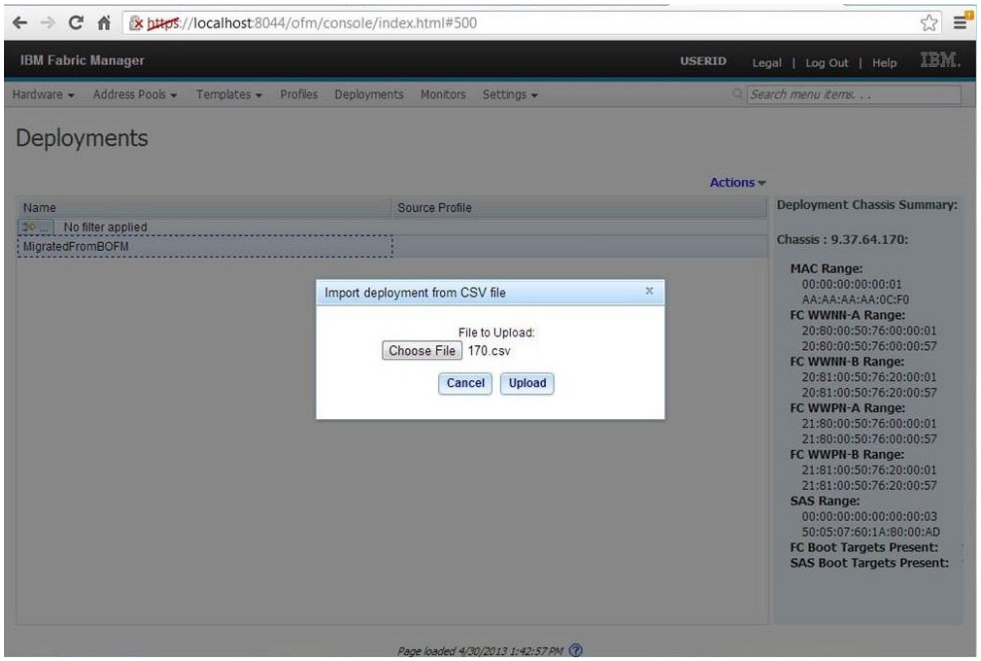
- Addresses can be Edited before Re-Deployment.
- IFM Configuration of Blade Slots can be Enabled/Disabled/Ignored on Deployment.

- Will Not be Able to Use all IFM Features.
- Will Not be Able to Use all IFM Supported Hardware.







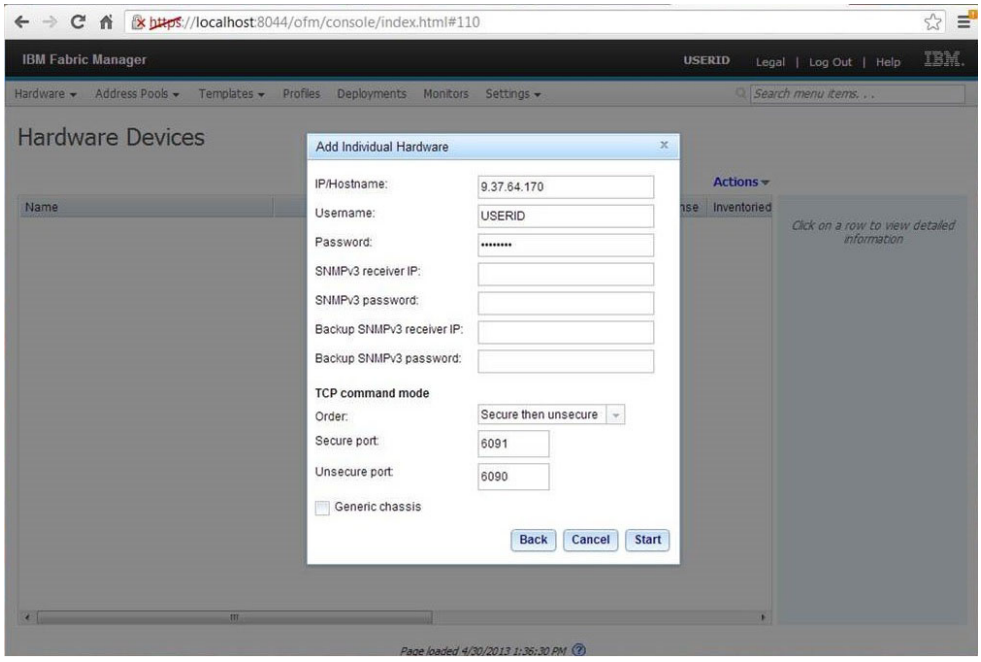


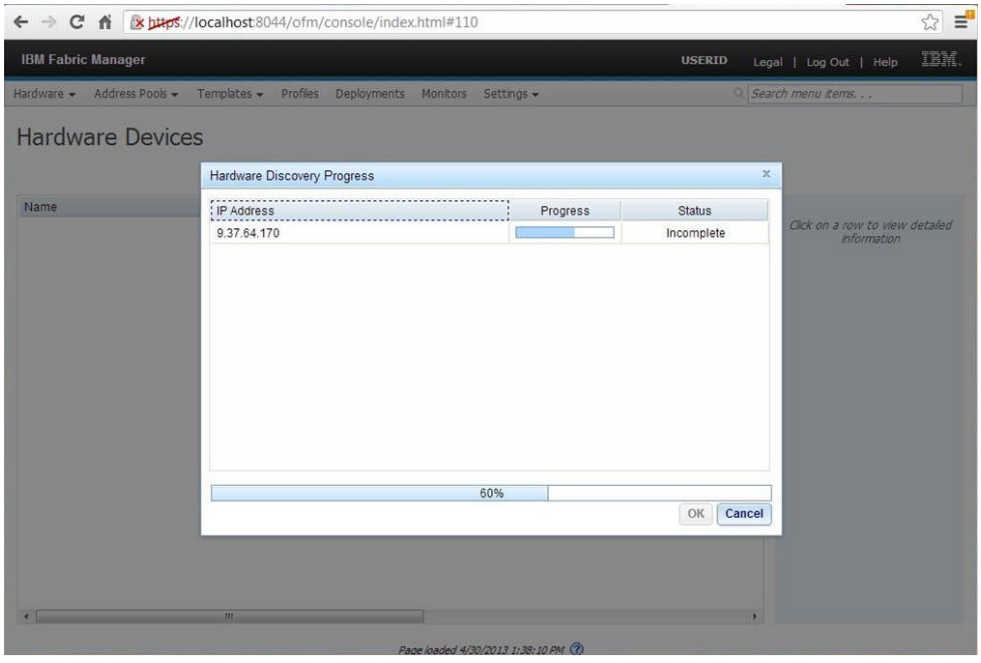
BOFM Basic to IFM Migration Option 3 – Create Deployment by Harvesting from BladeCenter

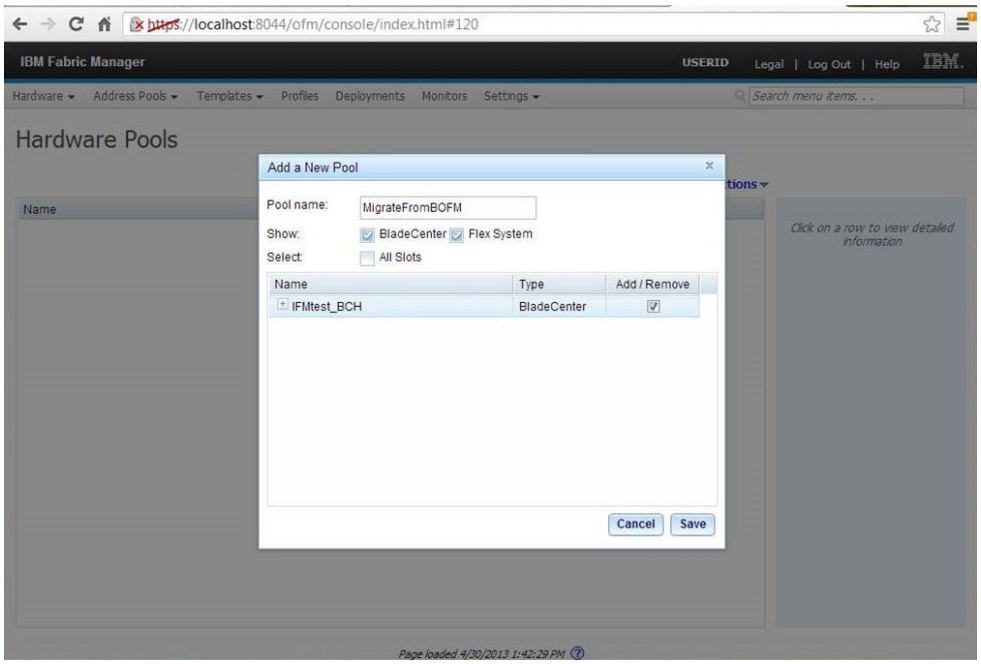
This topic describes BOFM Basic to IFM Migration Option 3.

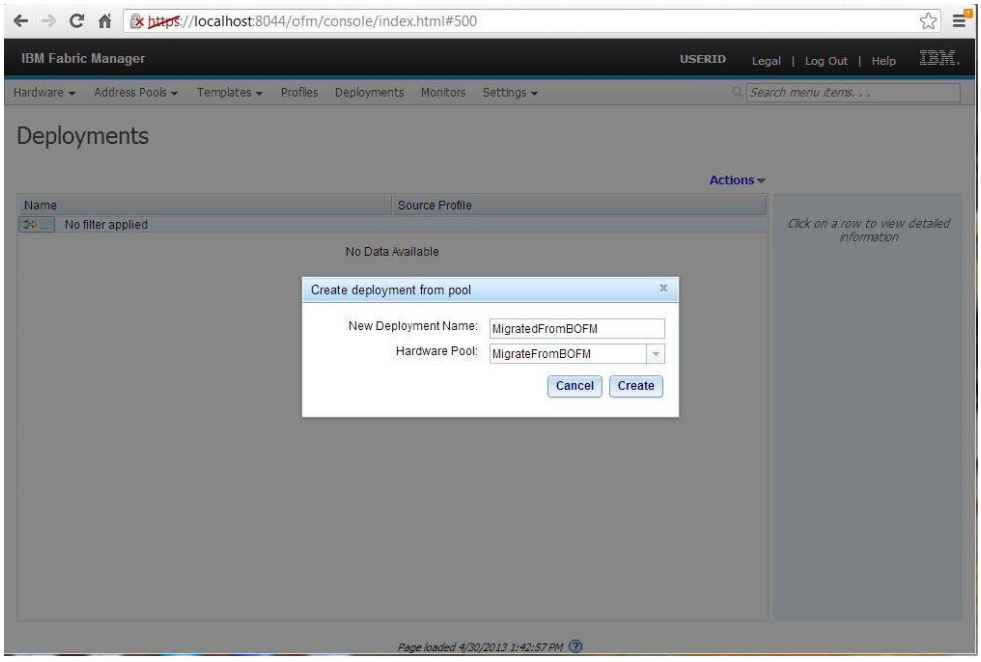
- When to choose this option.
  - The IFM Server has Network Access to the BladeCenter AMM.
  - There will be No Hardware Reconfiguration of the BladeCenter.
- Add BladeCenter Chassis to IFM.
  - Discover BladeCenter AMM.
  - Create Hardware Pool.

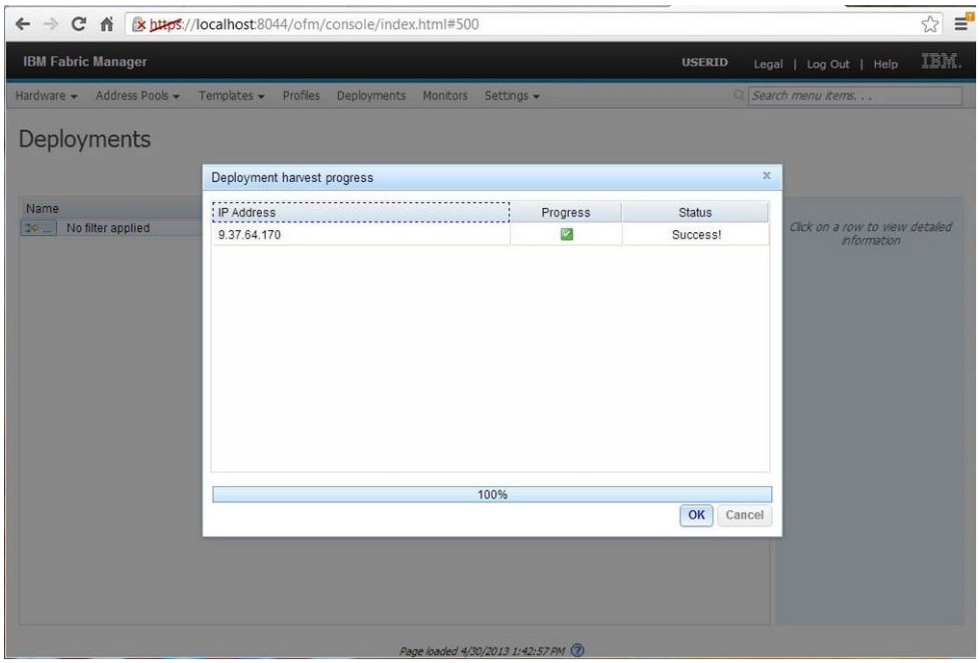
- BOFM Configuration in AMM Harvested into IFM.
  - Addresses can be Edited before Re-Deployment.
  - IFM Configuration of Blade Slots can be Enabled/Disabled/Ignored on Deployment.
- Will Not be Able to Use all IFM Features.
- Will Not be Able to Use all IFM Supported Hardware.

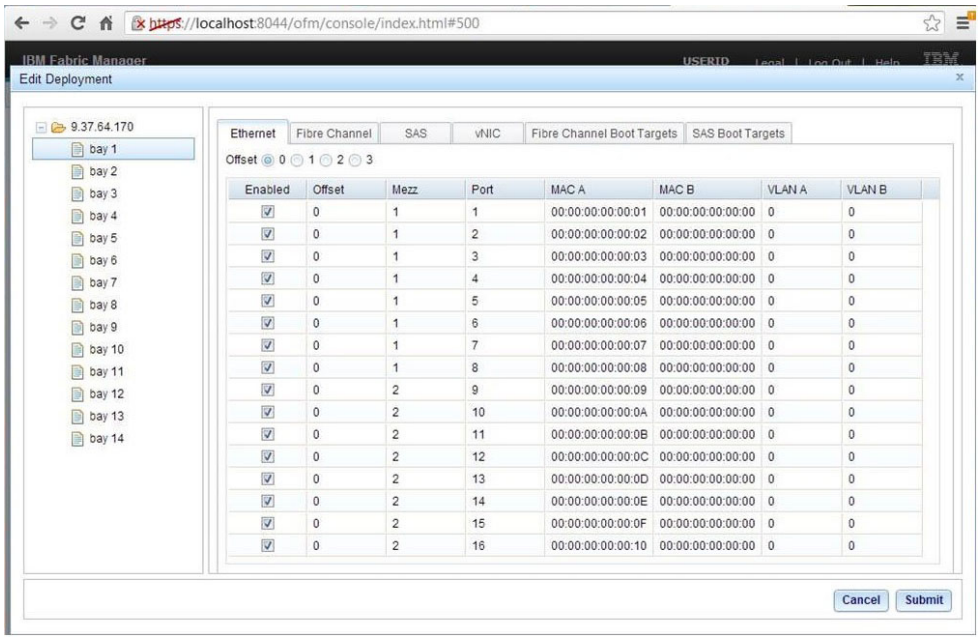





https://localhost:8044/ofm/console/index.html#120
IBM Fabric Manager
USERID
Legal | Log Out | Help
Hardware
Address Pools
Templates
Profiles
Deployments
Monitors
Settings
Search menu items. . .
Hardware Pools
Add a New Pool
Pool name:
MigrateFromBOFM
Show:
BladeCenter
Flex System
Select:
All Slots
Name
Type
Add / Remove
IFMtest_BCH
BladeCenter
Cancel
Save
Click on a row to view detailed information
Page loaded 4/30/2013 1:42:29 PM


https://localhost:8044/ofm/console/index.html#500
IBM Fabric Manager
USERID
Legal | Log Out | Help
Hardware
Address Pools
Templates
Profiles
Deployments
Monitors
Settings
Search menu items. . .
Deployments
Actions
Name
Source Profile
No filter applied
No Data Available
Create deployment from pool
New Deployment Name:
MigratedFromBOFM
Hardware Pool:
MigrateFromBOFM
Cancel
Create
Click on a row to view detailed information
Page loaded 4/30/2013 1:42:57 PM





BOFM Basic to IFM Migration Option 4 – Start Over

This topic describes BOFM Basic to IFM Migration Option 4.

- When to choose this option.
  - You will be Adding Hardware to Your BladeCenter.
  - You wish to take Advantage of Features Not Supported in BOFM.
- Follow Instructions in IFM User's Guide to Start Fresh.
- Add BladeCenter Chassis to IFM.
  - Discover BladeCenter AMM.
  - Create Hardware Pool.

- Build IFM Configuration.
  - Address Pools.
  - VNIC Settings.
  - Boot Targets.
  - Failover Monitors.
- Deploy New IFM Configuration to Discovered BladeCenter AMM.

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 all cables to make sure that they are connected.
- Check the power switches to make sure that the system and any optional devices are turned on.
- 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.
- 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
- 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.

You can solve many problems without outside assistance by following the troubleshooting procedures that IBM provides in the online help or in the documentation that is provided with your IBM product. The documentation that comes with IBM systems also describes the diagnostic tests that you can perform. Most systems, operating systems, and programs come with documentation that contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the documentation for the operating system or program.

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.

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. IBM System x information is at http://www.ibm.com/systems/x. IBM BladeCenter information is at http://www.ibm.com/systems/bladecenter. IBM IntelliStation information is at http://www.ibm.com/systems/intellistation.

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

Creating a personalized support web page

You can create a personalized support web page by identifying IBM products that are of interest to you.

To create a personalized support web page, go to http://www.ibm.com/support/mynotifications. From this personalized page, you can subscribe to weekly email notifications about new technical documents, search for information and downloads, and access various administrative services.

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 **Business Partner Locator**. 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 http://www.ibm.com/legal/us/en/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.

Each solid-state memory cell has an intrinsic, finite number of write cycles that the cell can incur. Therefore, a solid-state device has a maximum number of write cycles that it can be subjected to, expressed as `total bytes written` (TBW). A device that has exceeded this limit might fail to respond to system-generated commands or might be incapable of being written to. IBM is not responsible for replacement of a device that has exceeded its maximum guaranteed number of program/erase cycles, as documented in the Official Published Specifications for the device.

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

Table 10. Limits for particulates and gases (continued)

Contaminant	Limits
[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.

Telecommunication regulatory statement

This product may not be certified in your country for connection by any means whatsoever to interfaces of public telecommunications networks. Further certification may be required by law prior to making any such connection. Contact an IBM representative or reseller for any questions.

Electronic emission notices

When you attach a monitor to the equipment, you must use the designated monitor cable and any interference suppression devices that are supplied with the monitor.

Federal Communications Commission (FCC) statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio

communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that might cause undesired operation.

Industry Canada Class A emission compliance statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Australia and New Zealand Class A statement

Attention: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

European Union EMC Directive conformance statement

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a nonrecommended modification of the product, including the fitting of non-IBM option cards.

Attention: This is an EN 55022 Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Responsible manufacturer:

International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
914-499-1900

European Community contact:

IBM Deutschland GmbH
Technical Regulations, Department M372
IBM-Allee 1, 71139 Ehningen, Germany
Telephone: +49 7032 15 2941
Email: lugi@de.ibm.com

Germany Class A statement

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der IBM gesteckt/eingebaut werden.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden: **Warnung:** Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen.

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG). Dies ist die Umsetzung der EU-Richtlinie 2004/108/EG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2004/108/EG) für Geräte der Klasse A

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:

International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:

IBM Deutschland GmbH
Technical Regulations, Abteilung M372
IBM-Allee 1, 71139 Ehningen, Germany
Telephone: +49 7032 15 2941
Email: lugi@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

Japan VCCI Class A statement

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI-A

This is a Class A product based on the standard of the Voluntary Control Council for Interference (VCCI). If this equipment is used in a domestic environment, radio interference may occur, in which case the user may be required to take corrective actions.

Japan Electronics and Information Technology Industries Association (JEITA) statement

高調波ガイドライン適合品

Japan Electronics and Information Technology Industries Association (JEITA) Confirmed Harmonics Guidelines (products less than or equal to 20 A per phase)

Japan Electronics and Information Technology Industries Association (JEITA) statement

高調波ガイドライン準用品

Japan Electronics and Information Technology Industries Association (JEITA) Confirmed Harmonics Guidelines with Modifications (products greater than 20 A per phase)

Korea Communications Commission (KCC) statement

This is electromagnetic wave compatibility equipment for business (Type A). Sellers and users need to pay attention to it. This is for any areas other than home.

Russia Electromagnetic Interference (EMI) Class A statement

ВНИМАНИЕ! Настоящее изделие относится к классу А.
В жилых помещениях оно может создавать радиопомехи, для снижения которых необходимы дополнительные меры

People's Republic of China Class A electronic emission statement

中华人民共和国“A类”警告声明

声 明

此为A级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。

Taiwan Class A compliance statement

警告使用者:
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Index

R

S

T

U

V

Part Number: 00KC100

Printed in USA

(1P) P/N: 00KC100