IBM Systems

IBM Flex System Manager Management Software Troubleshooting and Support Guide

Version 1.3.2

IBM Systems

IBM Flex System Manager Management Software Troubleshooting and Support Guide

Version 1.3.2

Fourth Edition (December 2014)

Contents

Chapter 1. Overview of the IBM Flex System management node

IBM® Flex System Manager management software is the software stack for managing multiple chassis that comes preinstalled on the Flex System Manager Types 7955, 8731, and 8734 management node. It provides a consistent interface that you can use to efficiently manage more than one chassis.

The Flex System Manager Types 7955, 8731, and 8734 management node is supported in the Flex System Enterprise Chassis only.

The Flex System Manager Types 7955, 8731, and 8734 management node comes with a limited warranty. For information about the terms of the warranty and getting service and assistance, see the *Warranty Information* document on the IBM *Documentation* CD. You can obtain up-to-date information about the management node at http://www.ibm.com/supportportal/.

This documentation might be updated occasionally to include information about new features. Technical updates might also be available to provide additional information that is not included in the documentation.

You can subscribe to information updates that are specific to the management node at http://www.ibm.com/support/mynotifications/.

The model number and serial number are on the ID label that is located next to the power LED on the management node bezel. They are also on a label on the side of the management node that is visible when the management node is not in the Flex System Enterprise Chassis.

Before you begin

Use this background information to learn more about IBM Flex System Manager management software and Flex System Manager Types 7955, 8731, and 8734 accessibility and documentation resources.

Important: This publication contains troubleshooting information about the IBM Flex System Manager management software. For troubleshooting information about the IBM Flex System Manager hardware, or management node, see the *Flex System Manager Types 7955, 8731, and 8734 Installation and Service Guide*.

Related documentation

Use this information to identify and locate related documentation.

This documentation contains troubleshooting information for the IBM Flex System Manager management software. For troubleshooting information for the Flex System Manager Types 7955, 8731, and 8734 hardware, see the *Flex System Manager Types 7955, 8731, and 8734 Installation and Service Guide* document.

IBM Flex System Manager management software documentation

In addition to this document, the following documentation is also available in the IBM Flex System Manager Information Center at http://publib.boulder.ibm.com/infocenter/flexsys/information/index.jsp:

- *IBM Flex System Manager Systems Management Guide*
- *Flex System Manager Types 7955, 8731, and 8734 Installation and Service Guide*
- *IBM Flex System Manager Command Reference Guide*
-
- *IBM Flex System Manager Service and Support Manager (Electronic Service Agent™)*
- *IBM Flex System Manager Network Control*
- *IBM Flex System Manager VMControl*

IBM Flex System Chassis Management Module documentation

- *Chassis Management Module Installation Guide*

  This document explains how to install a Chassis Management Module in an Flex System Enterprise Chassis. See the IBM Flex System Chassis Management Module Installation Guide at http://publib.boulder.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.cmm.doc/dw1ku_cmm_ig_book.pdf for more information.
- *Chassis Management Module Command-Line Interface Reference Guide*

  This document explains how to use the Chassis Management Module command-line interface (CLI) to directly access Flex System Enterprise Chassis management functions. See the IBM Flex System Chassis Management Module User's Guide at http://publib.boulder.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.cmm.doc/dw1kt_cmm_cli_book.pdf for more information.
- *Chassis Management Module Events*

  This section in the information center provides a complete list of all non-device-specific events and recommended actions, sorted by event ID. See http://publib.boulder.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8721.doc/cmm_error_messages.html for more information.
- *Chassis Management Module User's Guide*

  This document provides information about configuring a Chassis Management Module and managing components that are installed in an Flex System Enterprise Chassis. This document explains how to use the Chassis Management Module command-line interface (CLI) to directly access Flex System Enterprise Chassis management functions. See the IBM Flex System Chassis Management Module User's Guide at http://publib.boulder.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.cmm.doc/dw1kt_cmm_ug_pdf.pdf for more information.

Flex System Enterprise Chassis and IBM Flex System compute node documentation

- *Flex System Enterprise Chassis Installation and Service Guide*

  This document explains how to install, configure, and service the Flex System Enterprise Chassis. See the Flex System Enterprise Chassis Installation and Service Guide at http://publib.boulder.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8721.doc/nn1gw_chassis_pdf.pdf for more information.
- *Flex System x240 Compute Node Installation and Service Guide*

The Flex System x240 Compute Node is an X-Architecture compute node that can be managed by management software. This document contains installation and service information about the compute node. See the Flex System x240 Compute Node Installation and Service Guide at http://publib.boulder.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8737.doc/dw1ko_book.pdf for more information.

- *IBM Flex System p260 Compute Node and IBM Flex System p460 Compute Node Installation and Service Guide*

  The Flex System p260 and p460 Compute Nodes can be managed by management software. This document contains installation and service information about the compute node. See the IBM Flex System p260 and p460 Compute Nodes Installation and Service Guide at http://publib.boulder.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.7895.doc/ps7895_pdf.pdf for more information.

To check for updated documentation, go to http://www.ibm.com/supportportal/.

Notices and statements in this document

Use this information to understand the most common documentation notices and statements and how they are used.

The caution and danger statements in this document are also in the multilingual *Safety Information* document, which is on the IBM *Documentation* CD. Each statement is numbered for reference to the corresponding statement in the *Safety Information* 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 possible 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 hazardous to you. A danger statement is placed just before the description of a potentially lethal or hazardous procedure step or situation.

Chapter 2. Troubleshooting the IBM Flex System Manager management software

Use this information to diagnose and fix problems that might occur in your hardware and software.

Important: This publication contains troubleshooting information about the IBM Flex System Manager management software. For troubleshooting information about the IBM Flex System Manager hardware, or management node, see the *Flex System Manager Types 7955, 8731, and 8734 Installation and Service Guide*.

The information in this section describes tools and procedures that can help you resolve software problems yourself.

IBM Service and Support Manager with IBM Electronic Service Agent (ESA), which is integrated with the management software, is a valuable resource for solving problems with managed resources. If configured and activated in the management software, ESA automatically reports hardware problems to IBM Support and collects system service information for monitored systems.

For general information about Service and Support Manager and ESA, see the *IBM Flex System Manager Service and Support Manager (Electronic Service Agent)* document.

Solving problems

In the IBM Flex System Manager management software web interface, use the Chassis Map in Chassis Manager to see events and problems for a device. To see events and problems at a higher, chassis level, use the Active Status or Problems page.

Use the information in this section to relate a problem to a managed resource (and a serviceable part, if applicable) with the Active Status and Problems pages by using the Chassis Manager in the management software web interface.

Important: The management software Service and Support Manager is a key software component for solving problems and getting support for your IBM Flex System hardware and software. Service and Support Manager automatically detects serviceable hardware problems and collects supporting data for serviceable hardware problems that occur on your monitored endpoint systems. The Electronic Service Agent™ tool is integrated with Service and Support Manager and transmits serviceable hardware problems and associated support files to IBM Support. See the *IBM Flex System Manager® Service and Support Manager (Electronic Service Agent)* document for detailed information about Service and Support Manager and Electronic Service Agent.

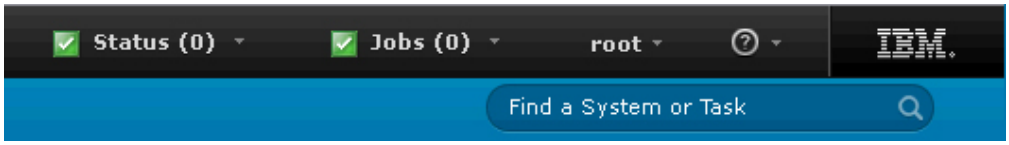
If configured and activated in the management software, IBM Electronic Service Agent (ESA) automatically reports hardware problems to IBM Support and collects system service information for monitored systems. For more information about setting up ESA, see the *IBM Flex System Manager Systems Management Guide* document.

For educational information about getting service and support for management software, see http://publib.boulder.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.common.nav.doc/learning_resource_management.html.

Viewing problems

Use the Chassis Manager and Chassis Map to view problems with chassis, compute nodes, or other resources that are managed by IBM Flex System Manager management software.

Note: This topic describes how to access this task in the IBM Flex System Manager Web user interface. If you are using the IBM FSM Explorer, use the finder at the top of the user interface (shown here) to locate this task:

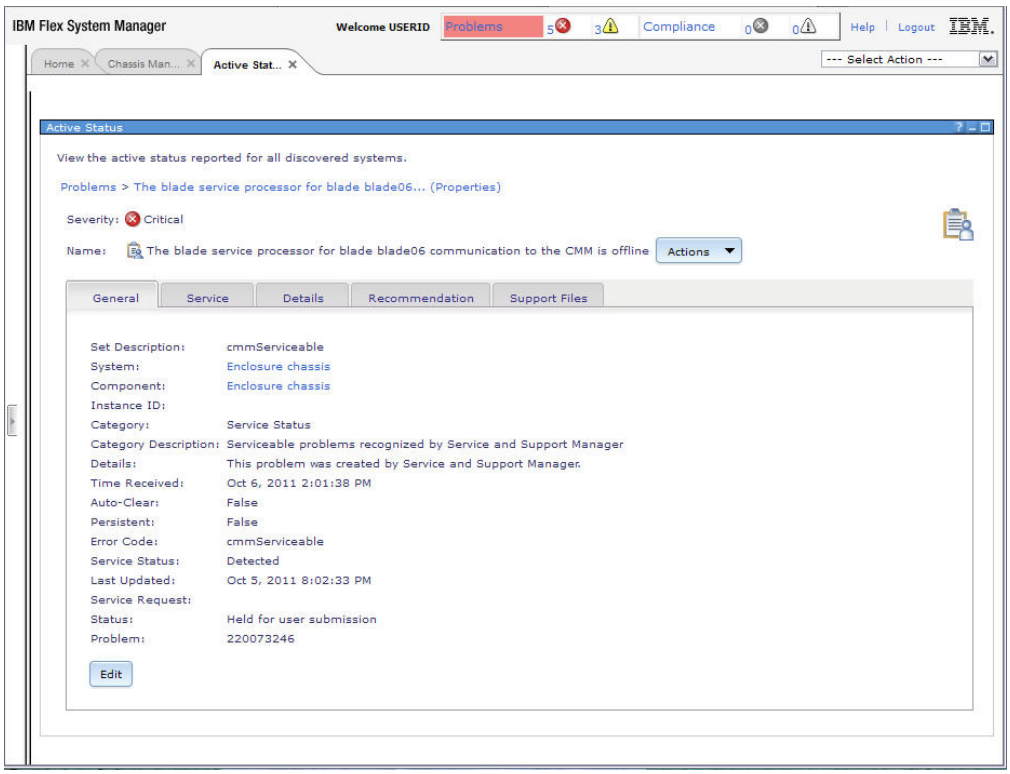


There are three primary ways to view problems by using the management software web interface:

- To view the problems for a chassis, open the Chassis Manager page and click the linked number for the chassis in the Problems column of the table.
- To view the problems for a compute node or other resource, open the Chassis Manager page and click the linked name of the chassis that contains the compute node. After the Chassis Map opens, click the compute node that has the problem that you want to view.
- To view all problems that are detected by management software, click the linked number beside **Problems** in the Scoreboard.

After you click a problem from the Active Status or Problems view, more information about the problem is displayed on one or more pages. The tabs that are displayed are determined by the nature of the problem. One or more of the following tabs might be displayed:

- General (info from Status Manager)
- Service (service transmission summary and service log)
- Details (everything associated with that event and affected resources)
- Recommendation (including a link to problem-related documentation)
- Support Files (submission of support files to IBM)



Note: To view only serviceable problems, use the Service and Support Manager page:

1. From the Home page, click the **Plug-ins** tab.
2. Click **Service and Support Manager**. The Service and Support Manager page opens.
3. In the **Problem Reporting** area, click **Serviceable Problems**. An Active Status page with a table showing serviceable problems opens.

For more information about solving a problem, see "Finding problem-resolution information through the management software web interface" on page 8 or the *IBM Flex System Manager Management Software Troubleshooting Guide* document.

For information about service requests, see "Submitting a service request" on page 10.

Filtering problems

To determine the nature of a problem on the Active Status and Problems pages, filter the Category column in the table view.

The following table shows the category names, which software or hardware component reports the problems in each category, and whether the problem appears on the Active Status page, Problems page, or both.

Table 1. Problem categories on Active Status and Problems pages

Category name	Reporting software or hardware component	Page where problems appear
Hardware Status	Status Manager	Active Status and Problems

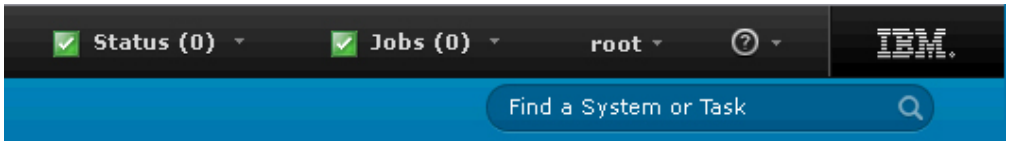
Table 1. Problem categories on Active Status and Problems pages (continued)

Category name	Reporting software or hardware component	Page where problems appear
Service Status	Service and Support Manager	Active Status and Problems
LED Status	LEDs	Active Status
Compliance	Update Manager	Active Status
DPSM Status (System p compute notes only)	Update Manager	Active Status and Problems
Local Health	Problems specific to the Flex System Manager Types 7955, 8731, and 8734	Active Status and Problems
Threshold Status	Status Manager	Active Status and Problems

Finding problem-resolution information through the management software web interface

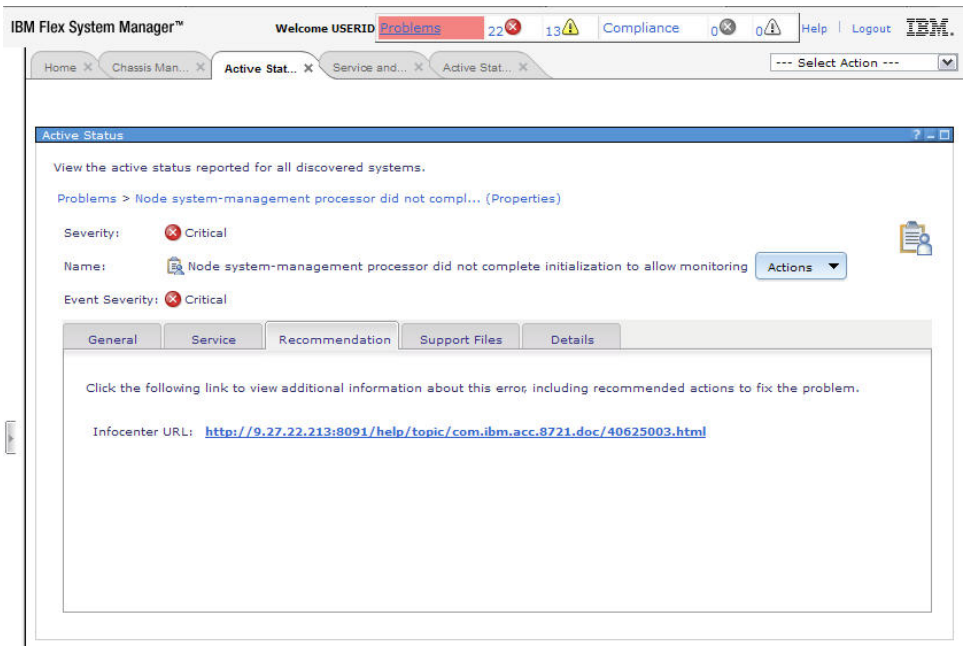
Use the IBM Flex System Manager management software web interface to guide you to problem-resolution recommendations in the IBM Flex System documentation.

Note: This topic describes how to access this task in the IBM Flex System Manager Web user interface. If you are using the IBM FSM Explorer, use the finder at the top of the user interface (shown here) to locate this task:



To find documentation for a problem or error in the management software web interface, complete the following steps:

1. From the Problems (Active Status) view, click the name of the problem. Active status information about the problem is displayed on one or more pages.
2. Click the **Recommendation** tab. If there is a documented description of the problem, a link to the problem in the IBM Flex System information center is displayed, as shown in the following illustration.



3. Click the link. The information center page for the problem opens in your browser.

Console logging and tracing

You can view and modify the configuration properties of the diagnostic trace service. This information pertains to logs and traces for the IBM Flex System Manager Web interface framework only; it does not pertain to your managed resources. If a problem occurs with the Web interface framework and you must contact your next level of support, your service provider, or an IBM Flex System Manager service representative, your service representative might ask you to adjust these configuration properties.

About this task

To change the settings for console logging and tracing, in the IBM Flex System Manager navigation area, expand **Settings** and click **Console logging and tracing**.

Collecting and submitting support files

You can use IBM Flex System Manager management software to collect and submit support files for a managed resource.

Support files can contain detailed system information used to help diagnose a serviceable hardware problem, dump files collected from a managed resource, event logs, and more. By default, Service and Support Manager automatically collects additional data associated with a serviceable hardware problem, and stores it as a support file. However, you can also collect support file data manually, even when a serviceable hardware problem has not occurred.

To collect and submit support files for a managed resource, complete the following steps:

1. To go to the Service and Support Manager page, click the **Plug-ins** tab on the Home page and click **Service and Support Manager** at the bottom of the plug-in list.

2. From the Service and Support Manager page, click **Manage support files** under Common Tasks. The Manage Support Files page opens.
3. To manually collect additional support files from a managed resource, click **Collect Support Files...**. The Collect Support Files panel opens.
4. Use the Collect Support Files panel to select the managed system and support file types for which you want to collect. If you select a file type of `Resource Dump` and do not specify a resource selector, a non-disruptive system dump will be performed. The resulting file will be a `SYSDUMP` file, rather than `RSCDUMP`.

Note:

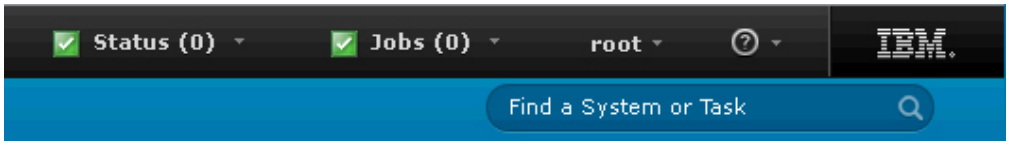
1. You can also collect and submit support files with the **`collectsptfile`** and **`submitsptfile`** commands in the command-line interface. See "collectsptfile" and "submitsptfile" in the *IBM Flex System Manager Service and Support Manager* document for more information.
2. Service and Support Manager requires either `smadmin` or `smmgr` user authority in order to view and manage support files.
3. Support files associated with a problem cannot be submitted unless the problem itself has been submitted to IBM support and is currently in a submitted state. Go to the **Problems** page to see the current status of the problem and ensure that the status is submitted before attempting to submit any associated support files.

Submitting a service request

This topic describes how to submit a service request from Chassis Manager in IBM Flex System Manager management software.

About this task

Note: This topic describes how to access this task in the IBM Flex System Manager Web user interface. If you are using the IBM FSM Explorer, use the finder at the top of the user interface (shown here) to locate this task:



To submit a service request for a managed resource in Chassis Manager, use one of the following methods:

- Click **Submit service request** in the list of common actions for a selected managed resource.
- From the table view, right-click the name of the managed resource. Click **Service and Support** > **Submit service request**.

Submitting service data manually

Use this procedure to submit service data manually.

About this task

To manually submit service data to IBM, complete the following steps.

Note: To submit an ESA event, you must first complete the Getting Started with Electronic Service Agent wizard.

Procedure

1. Click **Resource Explorer**. The Resource Explorer tab opens.
2. In the resource table, click **Service and Support Groups**. A table with the Service and Support groups appears.
3. Click **Monitored Systems**. A table with the monitored systems appears.
4. Select the check box for the monitored system you want and click **Action** > **Service and Support** > **Submit service request**.
5. Type the problem description and details in the applicable fields; then, click **Submit**. The submitted problem will show up in the table on the Problems page. If ESA is configured, the problem is sent to IBM. Otherwise, it is kept in a held state until ESA is configured.

Flex System Manager Types 7955, 8731, and 8734 Software error messages

The following error messages can appear in the event logs for the Flex System Manager Types 7955, 8731, and 8734.

DNZDVM150E There is no value specified for the User ID. You must specify a value for the user ID. Please specify a valid value for the user ID.

Explanation: You must specify a value for the user ID.

DNZDVM151E The format of the specified password is not valid. The password must consist of 7 or more alphnumeric characters. Please specify a valid value for the password.

Explanation: The password must consist of 7 or more alphanumeric characters.

DNZDVM152E You must specify a value for the date. The required format for the date is dd/mm/yyyy. Please specify a valid date in the required format.

Explanation: The required format for the date is dd/mm/yyyy.

DNZDVM153E You must specify a value for the time. The required format for the time is hh:mm:ss AM/PM. Please specify a valid time in the required format.

Explanation: The required format for the time is hh:mm:ss AM/PM.

DNZDVM154E The format of the specified date is not valid. The required format for the date is dd/mm/yyyy. Please specify a valid date in the required format.

Explanation: The required format for the date is dd/mm/yyyy.

DNZDVM155E The format of the specified time is not valid. The required format for the time is hh:mm:ss AM/PM. Please specify a valid time in the required format.

Explanation: The required format for the time is hh:mm:ss AM/PM.

DNZDVM156E The format of the specified domain name is not valid. The required format for the domain name is xxx.xxx.xxx, for example, server1.mycompany.com. Please specify a valid domain name in the required format.

Explanation: The required format for the domain name is xxx.xxx.xxx, for example, server1.mycompany.com.

DNZDVM157E The format of the specified domain name is not valid. The domain name can consist of alphanumeric characters a through z, A through Z, 0 through 9, and the hyphen character, separated by a period. The value must be more than 3, and fewer than 255, characters. The required format for the domain name is xxx.xxx.xxx, for example, server1.mycompany.com. Please specify a valid domain name in the required format.

Explanation: The domain name can consist of alphanumeric characters a through z, A through Z, 0 through 9, and the hyphen character, separated by a period. The value must be more than 3, and fewer than 255, characters. The required format for the domain name is xxx.xxx.xxx, for example, server1.mycompany.com.

DNZDVM158E You must specify a value for the domain name. The required format for the domain name is xxx.xxx.xxx, for example, server1.mycompany.com. The domain name can consist of the alphanumeric characters a through z, A through Z, 0 through 9, and the hyphen character, separated by a period. The value must be more than 3, and fewer than 255, characters. Please specify a valid domain name in the required format.

Explanation: The required format for the domain name is xxx.xxx.xxx, for example, server1.mycompany.com. The domain name can consist of the alphanumeric characters a through z, A through Z, 0 through 9, and the hyphen character, separated by a period. The value must be more than 3, and fewer than 255, characters.

DNZDVM159E The specified domain name is longer than the allowed maximum length. The domain name must consist of fewer than 255, and more than 3, alphanumeric characters, hyphens, and periods. Please specify a valid domain name that meets the length requirements.

Explanation: The domain name must consist of fewer than 255, and more than 3, alphanumeric characters, hyphens, and periods.

DNZDVM160E The specified domain name is shorter than the allowed minimum length. The domain name must consist of more than 3, and fewer than 255, alphanumeric characters, hyphens, and periods. Please specify a valid domain name that meets the length requirements.

Explanation: The domain name must consist of more than 3, and fewer than 255, alphanumeric characters, hyphens, and periods.

DNZDVM161E The format of the specified gateway IP address is not valid. The required gateway IP address format is nnn.nnn.nnn.nnn, where nnn is a number between 0 and 255. Please specify valid gateway IP address in the required format.

Explanation: The required gateway IP address format is nnn.nnn.nnn.nnn, where nnn is a number between 0 and 255.

DNZDVM162E You must specify a value for the gateway address. The required gateway IP address format is nnn.nnn.nnn.nnn, where nnn is a number between 0 and 255. Please specify a valid gateway IP address in the required format.

Explanation: The required gateway IP address format is nnn.nnn.nnn.nnn, where nnn is a number between 0 and 255.

DNZDVM163E The format of the specified gateway address range is not valid. The required gateway IP address format is nnn.nnn.nnn.nnn, where nnn is a number between 0 and 255. Please specify a valid gateway address range in the required format.

Explanation: The required gateway IP address format is nnn.nnn.nnn.nnn, where nnn is a number between 0 and 255.

DNZDVM164E The format of the specified IP address is not valid. The required IP address format is nnn.nnn.nnn.nnn, where nnn is a number between 0 and 255. Please specify a valid IP address in the required format.

Explanation: The required IP address format is nnn.nnn.nnn.nnn, where nnn is a number between 0 and 255.

DNZDVM165E You must specify a value for the IP address. The required IP address format is nnn.nnn.nnn.nnn, where nnn is a number between 0 and 255. Please specify a valid IP address in the required format.

Explanation: The required IP address format is nnn.nnn.nnn.nnn, where nnn is a number between 0 and 255.

DNZDVM166E The format of the specified IP address range is not valid. The required IP address format is nnn.nnn.nnn.nnn, where nnn is a number between 0 and 255. Please specify a valid IP address range in the required format.

Explanation: The required IP address format is nnn.nnn.nnn.nnn, where nnn is a number between 0 and 255.

DNZDVM167E The format of the specified network mask is not valid. The required network mask format is nnn.nnn.nnn.nnn, where nnn is a number between 0 and 255. Please specify a valid network mask in the required format.

Explanation: The required network mask format is nnn.nnn.nnn.nnn, where nnn is a number between 0 and 255.

DNZDVM168E You must specify a value for the network mask. The required format for the network mask is nnn.nnn.nnn.nnn, where nnn is a number between 0 and 255. Please specify a valid network mask in the required format.

Explanation: The required format for the network mask is nnn.nnn.nnn.nnn, where nnn is a number between 0 and 255.

DNZDVM169E The format of the specified netmask range is not valid. The required format for the netmask is nnn.nnn.nnn.nnn, where nnn is a number between 0 and 255. Please specify a valid netmask in the required format.

Explanation: The required format for the netmask is nnn.nnn.nnn.nnn, where nnn is a number between 0 and 255.

DNZDVM170E Unable to find an IP address. You must specify at least one IP address. Please specify at least one valid IP address.

Explanation: You must specify at least one IP address.

DNZDVM171E The format of the specified IP address is not valid. The required format of the IP address is: nnn.nnn.nnn.nnn, where nnn is a number between 0 and 255. Please specify a valid IP address in the required format.

Explanation: The required format of the IP address is: nnn.nnn.nnn.nnn, where nnn is a number between 0 and 255.

DNZDVM172E The specified DNS server has already been added. The specified DNS server is a duplicate entry. Please specify a new DNS server to add, or click Next to continue to the next step.

Explanation: The specified DNS server is a duplicate entry.

DNZDVM173E The specified domain suffix has already been added. The specified domain suffix is a duplicate entry. Please specify a new domain suffix to add, or click Next to continue to the next step.

Explanation: The specified domain suffix is a duplicate entry.

DNZDVM174E The format of the specified IPv6 address is not valid. Abbreviation of IPv6 addresses is not supported. The required format is xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx. Please specify a valid IPv6 address in the required format.

Explanation: Abbreviation of IPv6 addresses is not supported. The required format is xxxx:xxxx:xxxx:xxx:xxxx:xxxx:xxxx:xxxx.

DNZDVM175E The specified IPv6 address is already in the list. The specified IPv6 address is a duplicate entry. Please specify a different IPv6 address, or click Next to continue to the next step.

Explanation: The specified IPv6 address is a duplicate entry.

DNZDVM176E The format of the IPv6 prefix length is not valid. The required format of the prefix length is a number between 1 and 128. Please specify a prefix length in the required format.

Explanation: The required format of the prefix length is a number between 1 and 128.

DNZDVM177E The specified passwords are not identical. Both specified passwords must be the same. Please specify passwords that match.

Explanation: Both specified passwords must be the same.

DNZDVM178E The specified user ID already exists. The specified user ID is a duplicate entry. Please specify a different user ID.

Explanation: The specified user ID is a duplicate entry.

DNZDVM179E You did not accept the license agreement. You must accept the license agreement before you can continue to the next step. Accept the license agreement, then click Next.

Explanation: You must accept the license agreement before you can continue to the next step.

DNZDVM180E The selected application uses IPv6 addresses only. You cannot specify an IPv4 address. Please specify a valid IPv6 address in the required format of xxxx:xxxx:xxxx:xxx:xxxx:xxxx:xxxx:xxxx.

Explanation: You cannot specify an IPv4 address.

DNZDVM181E The selected application uses IPv4 addresses only. You cannot specify an IPv6 address. Please specify a valid IPv4 address in the required format of nnn.nnn.nnn.nnn.

Explanation: You cannot specify an IPv6 address.

DNZDVM182E The specified host already exists. The specified host is a duplicate entry. Please specify a different host.

Explanation: The specified host is a duplicate entry.

DNZDVM183E The IP address or network mask field is not empty. The IP Address or network mask fields contain values that must be used or discarded before you can continue. Please click Add to add the values, or clear the values from the fields.

Explanation: The IP Address or network mask fields contain values that must be used or discarded before you can continue.

DNZDVM184E The DNS or domain suffix field is not empty. The DNS or domain suffix fields contain values that must be used or discard before you can continue. Please click Add to add the values, or clear the values from the fields.

Explanation: The DNS or domain suffix fields contain values that must be used or discard before you can continue.

DNZDVM185E The specified host name is not valid. The specified host name contains characters that are not valid. Please specify a valid host name in the required format.

Explanation: The specified host name contains characters that are not valid.

DNZDVM186E You must specify a value for the host name. A host name is required. Please specify a valid host name.

Explanation: A host name is required.

DNZDVM187E A label in the specified host name is longer than the allowed maximum length. The maximum length for a label is 63 or fewer alphabetic characters. Please specify a host name that meets the length requirements for each label.

Explanation: The maximum length for a label is 63 or fewer alphabetic characters.

DNZDVM188E You must specify a value for the host name. A host name is required. Please specify a valid host name.

Explanation: A host name is required.

DNZDVM189E The specified host name label begins or ends with the hyphen (-) character. A host name label cannot begin or end with the hyphen (-) character. Please specify host name labels in the required format.

Explanation: A host name label cannot begin or end with the hyphen (-) character .

DNZDVM190E The specified host name is longer than the allowed maximum length. The maximum length of the host name is 255 or fewer alphabetic characters. Please specify a host name that meets the length requirements for the host name.

Explanation: The maximum length of the host name is 255 or fewer alphabetic characters.

DNZDVM191E The specified user ID does not begin with an alphabetic character. The user ID must begin with an alphabetic character. Please specify a user ID that begins with an alphabetic character.

Explanation: The user ID must begin with an alphabetic character.

DNZDVM192E The specified user ID contains one or more special characters. The user ID cannot contain special characters. Please specify a value for the user ID that not does contain special characters.

Explanation: The user ID cannot contain special characters.

DNZDVM198E The IP address range 192.168.70.200 - 192.168.70.299 is reserved and cannot be used.

Explanation: The IP address has to be an address that does not belong to the 192.168.70.200 - 192.168.70.299 range

DNZDVM199E Cannot use localhost as the host name for the management server.

Explanation: Cannot use localhost as the host name for the management server.

DNZDVM200E You need to add at least one IPv6 address. Please specify at least one valid IP address.

Explanation: You must specify at least one IP address.

DNZDVM201E Passwords don't match

Explanation: Passwords don't match.

DNZDVM202E The specified password does not comply with the system's password quality rules. To view a list of these rules, click on the help link below.

Explanation: Password does not comply with the system's password quality rules.

DNZDVM203E The specified password is invalid.

Explanation: The specified password is invalid.

DNZDVM204E We have detected both network adapters being on the same subnet, which is not supported. IP Address *VALUE_0* and IP Address *VALUE_1* are on the same subnet. You can fix this by specifying different subnets or using just one network adapter (eth0).

Explanation:

DNZDVM205E The format of the specified IP address is not valid. The required IP address format is nnn.nnn.nnn.nnn, where nnn is a number between 0 and 255. Please specify a valid IP address in the required format.

Explanation: The required IP address format is nnn.nnn.nnn.nnn, where nnn is a number between 0 and 255.

DNZDVM206E The format of the specified IP address range is not valid. The required IP address format is nnn.nnn.nnn.nnn, where nnn is a number between 0 and 255. Please specify a valid IP address range in the required format.

Explanation: The required IP address format is nnn.nnn.nnn.nnn, where nnn is a number between 0 and 255.

DNZDVM207E You must specify a value for the IP address. The required IP address format is nnn.nnn.nnn.nnn, where nnn is a number between 0 and 255. Please specify a valid IP address in the required format.

Explanation: The required IP address format is nnn.nnn.nnn.nnn, where nnn is a number between 0 and 255.

DNZDVM208E The User ID you specified contains an invalid character. Please pick a different User ID.

Explanation:

DNZDVM209E The User ID you specified is reserved. Please pick a different User ID.

Explanation:

DNZDVM210E The User ID cannot start with a number. Please pick a different User ID.

Explanation:

DNZDVM255E The static IPv4 address and the DHCPv6 client cannot both be selected at the same time.

Explanation:

DNZDVM256E The DHCPv4 client and the static IPv6 address cannot both be selected at the same time.

Explanation:

DNZDVM271E The specified time is before the system build time: *VALUE_0*. This will result in failure to start system. Please specify a time after the system build time, then retry the operation.

Explanation:

DNZDVM272E The specified time is more than an hour before current time, Verify the time is set correctly.

Explanation:

DNZDVM273E The specified time is more than an hour after current time, Verify the time is set correctly.

Explanation:

DNZDVM300E The specified IP address already exists in the network. To prevent an address conflict, please specify a different IP address.

Explanation:

DNZFM0001E Unable to obtain resource. (GUID: *VALUE_0*). Contact Support.

DNZFM0002E Unable to get local computerSystem resource. (GUID: *VALUE_0*). Contact Support.

DNZFM0003E A Resource caching exception occurred. See the next log entry for more information.

DNZFM0004E Unable to find resource. (GUID: *VALUE_0*). Contact Support.

DNZFM0005E Found multiple resources when only one was expected. Contact Support.

DNZFM0006E The root group cannot be found. Contact Support.

DNZFM0007E An unexpected class type was encountered. Expected class type: *VALUE_0*. Contact Support.

DNZFM0103I The ITME Sample Task is running.

DNZFM0112E Task *VALUE_0* must be invoked with one or more targets.

Explanation: A task must be invoked with at least one ITME as target.

DNZFM0201E The check for ITMEs task has finished with errors.

DNZFM0400E Exception occurred in Sample Command *VALUE_0*

DNZFM0510E Unable to generate security certificate because of an internal error (command failure). Make sure that your user ID is assigned to a role of SMAdministrator (smadmin group) and attempt the generate the certificate again. If the problem persists, contact Support.

DNZFM0511E Internal error occurred (command interrupt). Contact Support.

DNZFM0515E Internal error occurred (no host information). Contact Support.

DNZFM0516E Internal error occurred while initializing the user registry. Check the logs for more detailed information and contact Support.

DNZFM0517E Internal error occurred while resetting the user registry. Check the logs for more detailed information and contact Support.

DNZFM0518E Internal error occurred while initializing the user registry. The chkconfig command failed. Contact Support.

DNZFM0519E Internal error occurred while initializing the user registry. The chmod script failed updating of the /etc/init.d/ldap script. Contact Support.

DNZFM0520E Internal error occurred while initializing the user registry. The System Administrator ID could not be found. Contact Support.

DNZFM0521E Internal error occurred while initializing the user registry. The password for the System Administrator passed down to the LDAP initialization component. Contact Support.

DNZFM0522E Internal error occurred while getting the UUID of the FSM. rc = {0}. Contact Support.

DNZFM0523E An internal error occurred while processing a security policy. Error: {0} occurred in method: {1}. Contact Support.

DNZFM0524E Invalid NTP version 3 authentication key value.

Explanation: The NTP version 3 authentication key is a printable ASCII string.

DNZFM0525E Invalid NTP version 3 authentication key index.

Explanation: The NTP version 3 authentication key index is a number between 1 and 65535 inclusive.

DNZFM0526I The operation is successful.

DNZFM0527E The password entered does not meet the criteria for a secure password for reason {0}. Reason 1: Password must contain three of the following combinations: one lowercase alphabetic character, one uppercase alphabetic character, one numeric character, one special character. Reason 2: Password must contain no more than three of the same characters used consecutively. Reason 3: Password must not be a repeat or reverse of the associated user ID. Reason 4: Password must have at least 2 characters that are different from the previous password.

DNZFM0528E The new password must have at least 8 characters.

DNZFM0529E Internal error occurred while upgrading the user registry. The upgrade failed. Check the logs for more detailed information and contact Support.

DNZFM0530E The LDAP version was not able to be updated while upgrading the user registry. The upgrade failed. Check the logs for more detailed information and contact Support.

DNZFM0531E The LDAP schema was not able to be updated while upgrading the user registry. The upgrade failed. Check the logs for more detailed information and contact Support.

DNZFM0532E An internal error occurred while attempting to retrieve the password policy for the FSM. Contact Support.

DNZFM1000E The specified name already exists.

Explanation: User names must be unique within the user registry.

DNZFM1001I User *VALUE* has been created.

Explanation:

DNZFM1002I User(s) deleted successfully.

Explanation:

DNZFM1003I Password for user *VALUE* has been changed.

Explanation:

DNZFM1005I User Groups have been added for user *VALUE*.

Explanation:

DNZFM1006E The passwords do not match.

Explanation:

DNZFM1009E Unexpected error occurred. Contact Support.

Explanation:

DNZFM1011E Operating system(s) *VALUE* must have completed inventory to continue.

Explanation: The selected operating system(s) must have completed software inventory in order to continue.

DNZFM1012E Operating system(s) *VALUE* must be online and unlocked to continue.

Explanation: The selected operating system(s) need to to be online and unlocked in order to send agents to the system.

DNZFM1013E The systems hosting the following operating systems must have access to continue: *VALUE*.

Explanation: The systems hosting the selected operating systems need to have access in order to send the agents to the system.

DNZFM1014I Role *VALUE* has been created.

Explanation:

DNZFM1017E No target for moving chassis management was selected.

Explanation: When moving chassis management, select a target FSM.

DNZFM1019E The specified role information is not valid.

Explanation:

DNZFM1020E No resource was specified.

Explanation: You must specify at least one resource to which the role will be applied.

DNZFM1021E No scope entry was specified.

Explanation: You must specify at least one scope entry from the scope list.

DNZFM1022E The description is not valid.

Explanation: The description cannot start with the reserved mm, imm or frm characters.

DNZFM1023E The data management service is not available.

Explanation: One of the services required by the Flex System Manager is not available.

DNZFM1024W Information is still being collected about the Flex System Manager and its managed chassis. The information displayed on this panel may not be complete. Please log out, wait two minutes, and log back in. If this message persists, contact IBM support.

Explanation: One of the services required by the Flex System Manager is not initialized.

DNZFM1025I The password policy has been configured.

Explanation:

DNZFM1028I Role *VALUE* was deleted.

Explanation:

DNZFM1029I Role *VALUE* was modified.

Explanation:

DNZFM1030I Roles *VALUE* were deleted.

Explanation:

DNZFM1032W The Flex System Manager is about to shut down. This Web connection will be ended.

Explanation: While the Flex System Manager is shut down, a connection to the Flex System Manager Web interface is not available.

DNZFM1033E Unable to establish a connection to the user registry.

Explanation: A connection to the host on which the user registry resides could not be established because the host is not reachable.

DNZFM1034E The password is not valid.

Explanation: A valid password is required.

DNZFM1035E Unable to establish a connection to the user registry.

Explanation: A connection to the host on which the user registry resides could not be established because the user registry host name is blank.

DNZFM1036E Unable to establish a connection to the user registry.

Explanation: A connection to the host on which the user registry resides could not be established. This can occur because the host is not operational or because one or more of the specified settings is not correct.

DNZFM1037E The value specified for the user registry port is blank.

Explanation: The value specified for the user registry port must be between 1 and 65535.

DNZFM1038E The value specified for the user registry port is not valid.

Explanation: The value specified for the user registry port must be between 1 and 65535.

DNZFM1039E No permissions were selected for this role.

Explanation: At least one permission must be selected for the role.

DNZFM1040E No resource was specified.

Explanation: You must specify at least one resource to which the role will be applied.

DNZFM1041I User *VALUE* has been locked.

Explanation:

DNZFM1042I User *VALUE* has been unlocked.

Explanation:

DNZFM1043I The backup process has started.

Explanation:

DNZFM1044I The restore process has started. The Web connection will be ending.

Explanation: While the system is being restored, the user interface will not be available.

DNZFM1045E No backup file was selected.

Explanation: To restore the system, a backup file must be selected.

DNZFM1046E The specified maximum number of CMM sessions is not valid. The value in the maximum number of CMM sessions field must be a whole number between *VALUE_0* and *VALUE_1*.

Explanation:

DNZFM1047E The name is already in use.

Explanation: A user group with this name already exists.

DNZFM1048I User Group *VALUE* created successfully.

Explanation:

DNZFM1049I User group(s) deleted successfully.

Explanation:

DNZFM1050E The new passwords do not match. Reenter the new password and confirm the new password.

Explanation:

DNZFM1051W The Flex System Manager is about to restart. This Web connection will be ended.

Explanation:

DNZFM1052E When the Flex System Manager security level is set to Secure, the server must be enabled to check for password quality and cannot accept the password if unable to check it.

Explanation:

DNZFM1053E When the Flex System Manager security level is set to Secure, users must change the password at first logon.

Explanation:

DNZFM1054E When the Flex System Manager security level is set to Secure, the server must enable account lockout.

Explanation:

DNZFM1055E Cannot create the user because the user name is not valid. The user name must begin with an alphabetic character, must contain only a-z,A-Z,0-9, - or _. It must be no longer than 32 characters. Enter a valid name and create the user again. If the problem persists, contact Support.

Explanation:

DNZFM1056E A security policy level has not been selected. Please select a valid level to change the security policy level.

Explanation:

DNZFM1057E The following syslog server configurations could not be removed: *VALUE*.

Explanation: The syslog server configuration(s) were not removed from the system.

DNZFM1058E A syslog server configuration with these values already exists.

Explanation: The syslog server configuration was not added.

DNZFM1059E The syslog server configuration was not modified. Verify the entered values are correct and attempt the operation again.

Explanation: The syslog server configuration was not modified.

DNZFM1060E The syslog server configuration was not added. Verify the entered values are correct and attempt the operation again.

Explanation: The syslog server configuration was not added.

DNZFM1061E There was a problem uploading the encryption files. Verify the files are valid and attempt the operation again.

Explanation: The FSM could not upload one or more of the files.

DNZFM1062E One or more of the encryption files specified do not have a .pem extension. Verify the files are valid and attempt the operation again.

Explanation: One or more encryption file did not have the correct extension.

DNZFM1063E One or more chassis need to be selected to proceed.

Explanation: No chassis selected.

DNZFM1064E Syslog server encryption configuration could not be modified. Verify the files are valid and attempt the operation again.

Explanation: There was an error modifying the encryption configuration.

DNZFM1065E A valid host name or IP address must be entered for the remote syslog configuration.

Explanation: The value in the host name or IP address field was not valid.

DNZFM1066E A value was not specified for the SFTP user or password field.

Explanation: A user id and password are required to restore from a file on an SFTP server.

DNZFM1067W The security level in the backup file (*VALUE_0*) and the current security level (*VALUE_1*) are different. Select Allow restore with a different security level if you would like to continue with this restore and try again.

Explanation:

DNZFM1068E The FSM security policy level must be set to legacy to configure unencrypted remote syslog configurations.

Explanation: The remote syslog configuration was not created because the FSM security policy level must be set to legacy.

DNZFM1069E The value in the SSH timeout field must be a whole number between *VALUE_0* and *VALUE_1*.

Explanation:

DNZFM1070I The selected CMM is being restarted.

Explanation: A restart of the selected CMM has been requested.

DNZFM1071I The selected $$IO_MODULE$$ has been restored to factory defaults.

Explanation: A restore of the selected $$IO_MODULE$$ to factory defaults succeeded.

DNZFM1072E The selected $$IO_MODULE$$ could not be restored to factory defaults.

Explanation: A restore of the selected $$IO_MODULE$$ to factory defaults has failed.

DNZFM1073I The new roles for *VALUE* were assigned successfully.

Explanation:

DNZFM1074E Please select one or more IMMs to configure.

Explanation: One or more IMMs must be selected in order to continue with the wizard.

DNZFM1075E IMMs *VALUE* must be online and unlocked in order to continue with the wizard.

Explanation: The selected IMMs need to to be online and unlocked in order to configure the network settings.

DNZFM1076E The following IMMs were not successfully configured: *VALUE*.

Explanation: The listed IMMs failed to have the networking settings configured.

DNZFM1077I The network configuration for the following IMMs were successfully configured: *VALUE*.

Explanation: The listed IMMs were successfully configured.

DNZFM1078E Role and Resource Group selection is already selected.

Explanation: The Specific Role and Resource Group selection already selected. The selection should be unique.

DNZFM1079E Redundant Resource group and Role selection.

Explanation: For the same role already some resource groups have been assigned. Now you are trying to assign new resource groups which are redundant. If All Groups selected then all the other resource groups selected for the same role will be ignored.

DNZFM1080E No unique identifier was available for selected chassis: *VALUE*.

Explanation: A unique identifier is required in order to manage a chassis.

DNZFM1081E No unique identifier was available for the FSM.

Explanation: A unique identifier is required in order to manage a chassis.

DNZFM1082E User *VALUE* cannot be edited.

Explanation: This is a system defined user.

DNZFM1083E User Group *VALUE* cannot be edited.

Explanation: This is a system defined user group.

DNZFM1084I The backup process has completed.

Explanation:

DNZFM1085I The restore process has completed.

Explanation:

DNZFM1086E The selected CMM could not be restarted.

Explanation: A request to restart the selected CMM failed.

DNZFM1087E The value specified for the certificate file path is not valid.

Explanation: The value specified for the certificate file path is required when the Flex System Manager is operating at the current security policy level.

DNZFM1088W The following users could not be deleted: *VALUE*.

Explanation:

DNZFM1089E The following IMMs were not able to return network configuration data: *VALUE*.

Explanation: The IMMs did not return network configuration data.

DNZFM1090W One or more chassis is already managed by another Flex System Manager. Managing a chassis will remove it from the other Flex System Manager.

Explanation: A chassis can only be managed by one Flex System Manager.

DNZFM1091W The Features on Demand chassis key limit purchased is *VALUE* chassis. Managing the indicated chassis will exceed this limit.

Explanation: The number of chassis being managed by the Flex System Manager will exceed the Features on Demand chassis key limit purchased.

DNZFM1092I The graphical view was closed because the shown chassis began the unmanage process.

Explanation:

DNZFM1093W The graphical view was unable to retrieve necessary data.

Explanation: Data for the graphical view was not complete, however the table view is still available and is shown.

DNZFM1094E Please select one or more $$IO_MODULES_UPPER_CASE$$ to configure.

Explanation: One or more $$IO_MODULES_UPPER_CASE$$ must be selected in order to continue with the wizard.

DNZFM1095E $$IO_MODULES_UPPER_CASE$$ *VALUE* must be online and unlocked in order to continue with the wizard.

Explanation: The selected $$IO_MODULES_UPPER_CASE$$ need to to be online and unlocked in order to configure the network settings.

DNZFM1096E The following $$IO_MODULES_UPPER_CASE$$ were not successfully configured: *VALUE*.

Explanation: The listed $$IO_MODULES_UPPER_CASE$$ failed to have the networking settings configured.

DNZFM1097I The network configuration for the following $$IO_MODULES_UPPER_CASE$$ were successfully configured: *VALUE*.

Explanation: The listed $$IO_MODULES_UPPER_CASE$$ were successfully configured.

DNZFM1098E User *VALUE* cannot be added to any group.

Explanation: The user cannot be selected to be added to any group.

DNZFM1099E Users belonging to the FSM *VALUE_0* role must be in the *VALUE_1* user group.

Explanation:

DNZFM1100E The *VALUE* user group must be specified for the user. All users must be a member of *VALUE* user group.

Explanation:

DNZFM1101E User group $$ROOT_USER_GROUP$$ is not a valid selection for this user.

Explanation: Membership in user group $$ROOT_USER_GROUP$$ cannot be modified. This user group is for internal use and cannot be changed using this wizard.

DNZFM1102E The discovery process is complete. No chassis were found for this management domain.

Explanation: No chassis can be found to manage.

DNZFM1103I The chassis you are trying to manage: *VALUE_1* is already being managed from the following IP addresses: *VALUE*. When a chassis is managed, an event subscription is created for the managing entity on the CMM. Having multiple subscriptions can have an effect on performance. If the other managing entity is a FSM, you can try to remove the subscription by unmanaging. If that is not possible, you can remove the subscription by clicking the 'Manage Subscriptions' button to manually unsubscribe each event subscription. Then, attempt to manage the chassis from this FSM again.

Explanation:

DNZFM1104E A default role and resource group combination can not be removed for the user.

Explanation: A default role with All Resource Group combination can not be removed for the user. Please select a non-default role and resource group combination to be removed.

DNZFM1105E When the Flex System Manager security level is set to Secure, the account lockout duration can not be less than 60 minutes or different than 0.

Explanation:

DNZFM1106I The chassis *VALUE* being unmanaged has lost access. Without access the FSM can not remove CIM indications or remove the configurations that was done during the management of this chassis. It is recommended that the No Access link on the FSM Management Domain page be used to request access to the chassis before unmanaging it.

Explanation:

DNZFM1107I The chassis *VALUE* you are attempting to unmanage has related resources (managed endpoints) that will not be automatically removed if you continue with the unmanage process. This is generally due to Operating System resources, Virtual Machines and other managed endpoints that are associated with the Compute Node resources in the management domain. Unmanaging the chassis without removing these related resources from the management domain can cause problems if these resources are re-managed. It is recommended that you manually remove these resources from the management domain before continuing with the unmanage operation. For more information about how to identify and remove these resources, see Unmanaging a chassis in the online FSM Information Center.

Explanation:

DNZFM1108E The *PRODUCT_NAME_SHORT* does not have Platform agent update files imported that support the operating system types running on the following systems: *VALUE*.

Explanation: The FSM does not have any Platform agent update files imported that are applicable to the systems. Platform agent files for x86 architecture Windows and Linux systems are included as part of the image and can be re-imported. To import Platform agents for other operating systems, use the Import Updates task.

DNZFM1109E The CIM server encountered a error. Please try again.

Explanation: Try again. If the problem persists, contact Support.

DNZFM1110E The provided IPv6 prefix is not valid.

Explanation: IPv6 prefixes must be specified in hexadecimal, using the symbols 0-9 or a-f.

DNZFM1111E The IBM FSM User ID and/or Password is not valid. (Click the Edit Credentials button)

Explanation: Centrally managing a chassis requires a valid User ID and Password on the IBM FSM.

DNZFM1112E The User ID is not a supervisor on the IBM FSM or the password for the user is expired. (Click the Edit Credentials button) Please verify the user credentials and retry the action.

Explanation: Centrally managing a chassis requires a valid User ID that is a supervisor on the IBM FSM.

DNZFM1113W Selecting to automatically set an IPv6 unique address on each chassis component will overwrite any existing static IPv6 addresses.

Explanation:

DNZFM1114I Initial inventory is still being collected for components in *VALUE*. As components are inventoried, the number of components discovered and accessed will be updated.

Explanation:

DNZFM1115E Connecting to user registry server *VALUE* failed. Make sure you have specified the correct port and that the server is available.

Explanation:

DNZFM1116E Authentication failed connecting to external user registry server *VALUE*.

Explanation:

DNZFM1117E Connecting to user registry server *VALUE* failed. Check to make sure you have a valid configuration.

Explanation:

DNZFM1118W The network interface for the management network is configured to use DHCP, which means that the management interface IP address can change when the DHCP lease expires. If the address does change you will be required to unmanage all chassis and then manage them all again. Alternatively, you can change the management interface to a static IP address, you can make sure that the DCHP server configuration is set so that the DHCP IP address is based on a MAC address, or you can make sure that the DHCP server configuration is set to prevent the DHCP lease from expiring.

Explanation:

DNZFM1119E Using the Recovery User ID to manage a chassis is not allowed. Please specify a different User ID.

Explanation:

DNZFM1120E The recovery password is invalid. Please enter a different password.

Explanation:

DNZFM1121E The recovery passwords do not match. Please type in the password again.

Explanation:

DNZFM1122I You have selected remote chassis *VALUE***. Centralized management and automatic assignment of IPv6 Unique Local Addresses (ULAs) are not supported options for remote chassis. To include these options for local chassis, please manage remote and local chassis as separate operations.**

Explanation:

DNZFM1123E Connecting to user registry server *VALUE* **failed. Check to make sure you have a valid configuration.**

Explanation: Could not connect because there is no route to host. Please verify host name, port, and connection configurations.

DNZFM1124I The Secure Policy for FSM is set to Legacy, but you have chosen to enable SSL, please verify the port number specified is correct.

Explanation: The default port number for Legacy mode is 389, while for Secure it's 636. The port number may need to be updated from the defaulted value.

DNZFM1125E Anonymous bind is not supported on user registry server.

Explanation: Anonymous bind is not set up on the server. Verify anonymous is supported and retry operation.

DNZFM1126E The Default base Distinguished Name is invalid.

Explanation: The Default base Distinguished Name (DN) the server is expecting is invalid. Verify the DN entered is correct and try the operation again.

DNZFM1127E Invalid Distinguished Name (DN).

Explanation: The Distinguished Name (DN) the server is expecting is invalid. Verify the DN entered is correct and try the operation again.

DNZFM1500E Internal error attempting to get LDAP client configuration data for CMM {0}. Contact support.

DNZFM1501E Internal error. CMM OID: {0} passed to method is invalid. Contact support.

DNZFM1502E Internal error retrieving CMM configuration block with OID: {0} and PLUGIN: {1}. Contact support.

DNZFM1503E Error attempting to set the chassis user registry password.

DNZFM1504E Internal error applying CMM configuration block with OID: {0} and PLUGIN: {1}. Exception is: {2}. Contact support.

DNZFM1505E Internal error applying or retrieving configuration block, Configuration Manager service is null. Contact support.

DNZFM1506E Internal error retrieving credentials for CMM with OID: {0}.

DNZFM1507E An internal error occurred attempting to reset CMM: {0}. The LDAP client configuration was not reset.

DNZFM1701I Command completed successfully.

DNZFM1702E Command failed.

DNZFM2001W The specified chassis could not be unmanaged because is not currently managed by the FSM. Validate that you are specifying the correct FSM and chassis on the command.

DNZFM2002W The specified chassis is already managed by the FSM. Validate that you are specifying the correct FSM and chassis on the command.

DNZFM2003W The specified chassis cannot be managed. If the problem persists, contact Support.

DNZFM2004W The specified chassis could not be unmanaged. If the problem persists, contact Support.

DNZFM2005W The chassis with the following IP address cannot be found: *VALUE_0*. Verify that the specified IP address is valid.

DNZFM2006W The specified IP address does not match any known chassis IP address. Specify a valid chassis IP address and run the command again.

DNZFM2007W The FSM is not managing Call Home notifications for the specified chassis with host name: *VALUE_0*. Call Home is currently being managed by host name: *VALUE_1*.

DNZFM2008W The FSM is not receiving alert notifications for chassis with host name: *VALUE_0*. ***Note: Action depends on CMM functionality.

DNZFM2009E Unable to obtain the chassis managed endpoint. Contact Support.

DNZFM2010E The FSM cannot determine the IP address of the specified chassis. Attempt to rediscover the chassis, if the problem persists, contact Support.

DNZFM2011E The specified FSM cannot be resolved from the specified IP address. Make sure that the FSM IP address is valid and attempt to run the command again.

DNZFM2012E The FSM that is managing the chassis is not the FSM that is expected to be managing the chassis. Make sure that the specified FSM is the FSM managing the chassis and run the command again.

DNZFM2013E An exception occurred while running inventory. Attempt to run inventory again. If the problem persists, contact Support.

DNZFM2014E A Service Location Protocol (SLP) exception occurred. Contact Support.

DNZFM2015E An internal error occurred (data management) during initialization. Contact Support

DNZFM2016E An internal error occurred (data management) during parsing. Contact Support.

DNZFM2017E The FSM cannot reach the chassis using its available IP addresses. You must define an external address for the chassis that has the same type (IPV4 or IPV6) that the management interface (eth0) of the FSM is using. Verify the chassis IP address by refreshing the view. Then try again. If the problem persists, contact Support.

DNZFM2018E The FSM cannot discover the chassis using the IP addresses that are available. You must define an external address for the chassis that has the same type (IPV4 or IPV6) that the management interface (eth0) of the FSM is using. .

DNZFM2019E The FSM cannot unmanage the chassis without leaving behind manageable elements. You may unmanage with the force option if you wish to manually clean up the elements that were left behind.

DNZFM2020E The number of chassis that will be managed will exceed the chassis management license currently in place. You should upgrade the license to support the management of additional chassis.

DNZFM2021E The network interface for the management network is currently configured to use DHCP. The management interface IP address can change when the DHCP lease expires. If the address does change you will be required to unmanage the chassis and remange the chassis. To prevent problems either change the management interface to a static IP address, or insure that the DCHP server configuration is set so that the DHCP address is based on a MAC address or that the DHCP lease does not expire. If your DHCP server is configured to base DHCP address on the MAC address or the DHCP lease does not expire, you may manage with the force option to override this message.

DNZFM2023E A resource caching exception occurred. Contact Support.

DNZFM2025E The discovery service is not available. Restart the FSM and attempt to manage the chassis. If the problem persists, contact Support.

DNZFM2026E The chassis Discovery process did not complete. Refresh the chassis list by clicking the Discover New Chassis button and attempt to manage the chassis again. If the problem persists, contact Support.

DNZFM2027E The operating system discovery process did not complete. Make sure that the operating system is reachable from the same network on which the FSM is attached. Then, perform the operation again. If the problem persists, contact Support.

DNZFM2028E Unable to move the management of the chassis to the specified FSM. Make sure that the FSM is functioning and that you can log in to the FSM. Then, attempt to move the chassis again.

DNZFM2029E The operating system discovery process did not complete successfully. A timeout was reached while waiting for the operating system discovery to complete. This does not mean that the discovery failed. However, the operating system will not be accessible automatically. From the Chassis Manager, right-click on the node and select Security -> Configure access. Enter the correct authentication credentials to gain access. If the problem persists, contact Support.

DNZFM2030E An error was encountered while trying to remanage chassis after rebooting the FSM. Make sure that the chassis is running correctly and that there is a working network connection between the chassis and the FSM. Then manage the chassis again (You do not need to unmanage first). If the problem persists, contact support.

DNZFM2031E Internal error (problem reading properties file). Make sure that the user account has proper permissions to read files on the FSM. If the problem persists, contact Support.

DNZFM2032E Invalid command usage: run *VALUE_0* **-? for information about running this command.**

DNZFM2033E The chassis you are trying to manage is already being managed from the following IP addresses: *VALUE_0***. When a chassis is managed, an event subscription is created for the managing entity on the CMM. Having multiple subscriptions can have an effect on performance. If the other managing entity is a FSM, you can remove the subscription using the unmanage command. If the other managing entity is another application, run the command: smcli lschassisind to manually remove event subscriptions. Then, attempt to manage the chassis from this FSM again.**

DNZFM2035E Failed to add object to database (Internal Error). Contact Support.

DNZFM2036E No chassis specified on command. Run the command again, specifying a valid chassis.

DNZFM2100E Could not get the localhost IP address for the FSM. Contact Support.

DNZFM2200E The group service is not available. Restart the FSM and attempt to manage the chassis. If the problem persists, contact Support.

DNZFM2201E Unable to request access to the Operating System with host name: *VALUE_0*. From the Chassis Manager, right-click on the node and select Security -> Configure access. Enter the correct authentication credentials to gain access. If the problem persists, contact Support.

DNZFM2203E The chassis with the IP address: *VALUE_0* is in the process of being managed. Therefore, it cannot be deleted. Wait until the management process completes; then, attempt to delete the chassis again.

DNZFM2204E Unable to request access to the chassis with host name: *VALUE_0*. From the user interface, use the link to Fix Access Error and enter correct authentication credentials. From the command line, verify that you are entering a userID and password that can authenticate with the chassis and run the command again. Additionally you can verify that a valid root CA certificate for the chassis with host name: *VALUE_0* exists on the FSM by using FSM Resource Explorer and viewing the \"All Systems\" group. If the chassis is \"Not Trusted\" you will need to accept the CA certificate to successfully manage this chassis. If the problem persists, contact Support.

DNZFM2205E Unable to revoke access to the chassis with host name: *VALUE_0*.

DNZFM2206E An exception was returned while configuring the chassis user registry (LDAP). Make sure that the CMM in the chassis is functional and connected to the network. Attempt to log in to the CMM with the same credentials that you used to manage the chassis. If successful, attempt to manage the chassis again. Otherwise, attempt to manage the chassis using CMM credentials that can be used to access the CMM directly. If the problem persists, contact Support.

DNZFM2207E The manageable element for the chassis with IP address: *VALUE_0* was deleted unexpectedly. Attempt to discover and manage the chassis again.

DNZFM2208E The FSM cannot manage the specified chassis with host name *VALUE_0* because FSM management of that type of chassis is not supported. Specify a supported chassis and try again.

DNZFM2209E Internal error occurred (data management). Contact Support.

DNZFM2210E The FSM for the IP address: *VALUE_0* is unknown to this FSM. Validate that the IP address was specified correctly, and make sure that a chassis with the specified IP address is functioning and connected to the network. Then, perform the operation again.

DNZFM2211E The chassis with the IP address: *VALUE_0* is unknown to this FSM. Validate that the IP address was specified correctly, and make sure that a chassis with the specified IP address is functioning and connected to the network. Then, perform the operation again.

DNZFM2212E The user ID and password provided for the chassis were incorrect. Use the link to Fix Access Error and enter the correct user ID and password.

DNZFM2213E The request access process for the chassis returned a Not Accessible error.

DNZFM2214E The request access process for the chassis returned a Not Supported error.

DNZFM2215E Unable to request access to the chassis with host name: *VALUE_0*. The authentication credentials have expired. Use the link to Change Password and enter a new password. If you are using an external User Registry with your chassis, connect to either the chassis or the external User Registry to restore the expired credentials.

DNZFM2216E Request access failed on chassis with host name: *VALUE_0*. Use the link to Fix Access Error and enter valid user ID and password.

DNZFM2217E Revoke access failed with status of 'result not available'. The chassis with host name: *VALUE_0* is unavailable. Make sure that the chassis is running and that there is a working network connection between the chassis and the FSM. Then, attempt to revoke access again.

DNZFM2218E The user ID and password provided for the FSM were incorrect. Specify a valid user ID and password.

DNZFM2219E The specified FSM is unknown to this FSM. Validate that the specified FSM is functioning and connected to the network. Then, perform the operation again.

DNZFM2220E The specified chassis is unknown to this FSM. Validate that the specified chassis is functioning and connected to the network. Then, perform the operation again.

DNZFM2221E An exception was returned while resetting the chassis user registry (LDAP) during an unmanage operation. The unmanage was successful but the chassis user registry was not reset. Make sure the chassis is functioning and connected to the network. Then, log in to the chassis command-line interface using the RECOVERY_ID user account. Verify that user registry authentication is set to local authentication (CMM command: accseccfg -am local -T mm[p]), verify that the SSL client is disabled (CMM command: sslcfg -client disabled -tc1 remove -T mm[p]), and verify that the CMM local accounts are not disabled (CMM command: fsmcm -off -T mm[p]). Once you have manually reset the chassis user registry using the commands listed, it can be managed again. If the problem persists, contact Support.

DNZFM2222E The unmanage of the chassis failed because some contained hardware elements were not removed. They will have to be deleted manually in order to manage the chassis again.

DNZFM2223E The unmanage of the chassis failed because the removal of contained hardware elements could not be monitored. If any hardware elements are not deleted after a few minutes, they might have to be deleted manually in order to manage the chassis again.

DNZFM2224E The unmanage of the chassis failed because the managed endpoint of the chassis was not removed. Wait a few minutes then try again. If the problem persists, contact Support.

DNZFM2225E The user ID and password provided for the chassis were incorrect. Specify a valid user ID and password.

DNZFM2226E The remote FSM for the IP address: *VALUE_0* is unknown to this FSM. Validate that the IP address was specified correctly, and make sure that a FSM with the specified IP address is functioning and connected to the network. Then, perform the operation again.

DNZFM2227E **Unable to change expired password on chassis with host name:** *VALUE_0*. **Login to chassis web GUI to change the password, then attempt the manage again.**

DNZFM2228E **The chassis user account is locked on host:** *VALUE_0*. **You can attempt to manage the chassis again using a different set of credentials. In addition, you can attempt to manage the chassis using the currently specified credential after the account lock-out period (typically 1 hour), or you can log in to the CMM Web interface using a CMM user account with Supervisor permissions to unlock the account.**

DNZFM2229E **The chassis** *VALUE_0* **has exceeded the number of available connections. Wait for a connection to become available or, if necessary, restart the chassis or the FSM.**

DNZFM2250E **A core service is initializing. Wait a few minutes and try again. If the problem persists, contact Support.**

DNZFM2251E **The chassis you are trying to manage is already sending alerts to the following IP Addresses:** *VALUE_0*. **Follow the link to managing FSM and unmanage the chassis. If you cannot unmanaged the chassis, run the smcli command lschassisind --clear**

DNZFM2252E **Either the user ID or password is invalid. Enter the correct user ID and password and try again.**

DNZFM2253E **The following exception was thrown while trying to run the command.**

DNZFM2254E **The following exception was received:** *VALUE_0*

DNZFM2260E **Validating that the V7000 storage node with address:** *VALUE_0* **has been discovered already and can be deleted.**

DNZFM2261E **The specified V7000 storage node is not currently being managed, so it cannot be unmanaged.**

DNZFM2262I **The V7000 storage node is in the process of being deleted from the list of managed resources.**

DNZFM2263I **Command to remove the data source:** *VALUE_0*

DNZFM2264E **The removal of the data source failed with message:** *VALUE_0* **Attempt to remove the data source again. If the problem persists, contact Support.**

DNZFM2265E **No fibre channel switch was found at address:** *VALUE_0* **Check that you are specifying a valid address and that the fibre channel switch is accessible from the FSM. Then, try the command again.**

DNZFM2266E **Connection was refused to the V7000 storage node. Error code:** *VALUE_0*

DNZFM2267I **Removing the SSH key from** *VALUE_0* **on the V7000:** *VALUE_1*

DNZFM2268I **Pushing the SSH public key for admin to the V7000 storage node using the command:** *VALUE_0*

DNZFM2269E **The V7000 storage node with the management address:** *VALUE_0* **was not unmanaged.**

DNZFM2269I **The V7000 storage node with the management address:** *VALUE_0* **was unmanaged succesfully.**

DNZFM2270E **V7000 with management address:** *VALUE_0* **was not managed.**

DNZFM2270I **V7000 with management address:** *VALUE_0* **was managed succesfully.**

DNZFM2271E **The V7000 storage node has been discovered already.**

DNZFM2272E **User** *VALUE_0* **has a public key defined on the V7000 storage node, which means that the storage node is managed already. Remove the key from** *VALUE_1* **on the storage node. Optionally, run smcli unmanageV700 from the FSM that is currently managing the V7000 storage node.**

DNZFM2273I Generating SSH keys for admin using command: *VALUE_0*

DNZFM2274E SSH public key for admin failed to be generated.

DNZFM2275I SSH public key for admin was generated successfully

DNZFM2276I SSH public key for admin was not pushed to the V7000 storage node.

DNZFM2277I SSH public key for admin was pushed to the V7000 storage node successfully.

DNZFM2278I Assigned SSH public key file to admin.

DNZFM2279I Issue *VALUE_0* **command:** *VALUE_1*

DNZFM2280E The *VALUE_0* **command did not complete successfully.**

DNZFM2281I The *VALUE_0* **command was successful.**

DNZFM2282I No farm resource was found.

DNZFM2283I Collecting inventory of the farm resource.

DNZFM2284I Waiting for storage device managed endpoint to be created.

DNZFM2285I The V7000 storage node with the management address: *VALUE_0* **was not managed succesfully. You might need to wait for the inventory of the storage farm to complete.**

DNZFM2286E Enabling the manufacturing mode on the V7000 storage node was unsuccessful.

DNZFM2287E Superuser was not created on the V7000 storage node.

DNZFM2288E Could not generate SSH key for superuser on the V7000.

DNZFM2294E The backup of the FSM was not successful. Click view log for more details. If the problem persists, contact Support.

DNZFM2295E Restore of the FSM failed. Check the log and make sure that the backup you are trying to restore from completed successfully. If the problem persists, contact support.

DNZFM2296E Restore of the FSM failed. Make sure that the FTP server is on the network and is reachable from the FSM, the credentials for the server are correct, and contains the specified restore image, then try again. If the problem persists, contact support.

DNZFM2297E The restoration of the FSM was not successful. Make sure the USB device contains the specified restore image, and attempt to restore the FSM again. If the problem persists, contact Support.

DNZFM2298E The backup of the FSM was not successful. Make sure that the FTP server is on the network and is reachable from the FSM, the credentials for the server are correct, and that there is enough storage space on the server. Attempt to back up the FSM again. View log for more details. If the problem persists, contact Support.

DNZFM2299E The backup of the FSM was not successful. Make sure that the USB device has sufficient space available and attempt to back the FSM again. View log for more details. If the problem persists, contact Support.

DNZFM2300E An I/O error occurred while attempting to run a backup/restore operation. Make sure that the user account being used to run the operation has permission to perform the operation. Then, attempt to perform the operation again. If the problem persists, contact Support

DNZFM2301E Internal error occurred (command interrupt). Contact Support.

DNZFM2302E Internal error occurred (file not found). Contact Support.

DNZFM2303E An error occurred while trying to assign the NTP server to the managed chassis.

DNZFM2330E The USB device could not be mounted. Multiple USB devices might be installed, or the USB device might be already mounted under a different user. Make sure that only one USB device is connected, and that the USB device is not already mounted by a different user. Attempt to mount the USB device again. If the problem persists, contact Support.

DNZFM2331E The USB device could not be mounted because there is no USB device connected to the FSM. Make sure only one USB device is connected to the FSM, and attempt to mount the USB device. If the problem persists, contact Support.

DNZFM2332I Command: *VALUE_0* was successful.

DNZFM2333E Command: *VALUE_0* was not successful.

DNZFM2400E An error occurred while attempting to update the configuration for the specified node. From the Chassis Manager, make sure that the node is functioning and that there is a working network connection between the FSM and the node. Attempt to update the configuration again. If the problem persists, contact Support.

DNZFM2401E An error occurred while attempting to retrieve the configuration for the specified node. From the Chassis Manager, make sure that the node is functioning and that there is a working network connection between the FSM and the node. Attempt to retrieve the configuration again. If the problem persists, contact Support.

DNZFM2402E An error occurred while trying to determine if the chassis is currently being managed by the FSM. Attempt to run the command again, if the problem persists, contact Support.

DNZFM2403E An error occurred while trying to determine if the chassis can be centrally managed by the FSM. Attempt to run the command again. If the problem persists, contact Support.

DNZFM2404E The chassis you are trying to manage is already centrally managed.

DNZFM2405E The chassis you are trying to manage does not support centralized management. Update the chassis firmware to a level that supports centralized management. Then attempt the command again. If the problem persists, contact Support.

DNZFM2406E A specified parameter is not valid or is missing. When you specify to update the chassis to be centrally managed, you must provide the following information for the CMM: user ID, password, and valid host name or IP address. Attempt to run the command again specifying all required parameters.

DNZFM2407I Updating chassis: *VALUE_0* to be managed centrally. This command can take up to 4 minutes to complete. The -c, --Uc, --Cu, --Cp and --Rp parameters are the only valid parameters for the update function, all others will be ignored.

DNZFM2408E The chassis: *VALUE_0* is now centrally managed.

DNZFM2409E An attempt to centrally manage chassis: *VALUE_0* failed. Check for other messages related to this issue and resolve them. Attempt to run the command again. If the problem persists, contact Support.

DNZFM2410E The chassis: *VALUE_0* cannot be centrally managed because it is not currently being managed by the FSM. Run the smcli command manageChassis to manage the chassis, specifying that it be centrally managed. The --UpdateToCentralized option is intended to be used on chassis that are already managed non-centrally.

DNZFM2411E An error occurred while checking the FSM credentials. Attempt to run the command again, if the problem persists, contact Support.

DNZFM2412E User ID: {0} does not have supervisor authority. Attempt to run the command again using a user ID with supervisor authority.

DNZFM2413E Could not point the chassis user registry to the FSM. Attempt to run the command again with the generate ULA option specified, or use the assignULA CLI command before centrally managing the chassis again. If the problem persists, contact Support.

DNZFM2414E Could not update FSM user registry with chassis data. Attempt to run the command again, if the problem persists, contact Support.

DNZFM2415E Could not update FSM property to centralized. Attempt to run the command again, if the problem persists, contact Support.

DNZFM2416E An error occurred checking the chassis recovery password. Attempt to run the command again, if the problem persists, contact Support.

DNZFM2417E The FSM is using an external user registry therefore the chassis cannot be centrally managed.

DNZFM2418I Attempting to manage chassis: *VALUE_0* centrally. This command can take up to five minutes to complete. Specify the -W parameter to determine how the manage process is progressing. Otherwise, you can check the Chassis Manager in the user interface to determine if the manage process completed successfully.

DNZFM2419E An error occurred while centrally managing the chassis. The Flex System Manager could not reach the chassis component with resource type *VALUE_0*, IPV6 address *VALUE_1*, IPV4 address *VALUE_2*, bay *VALUE_3*. Make sure at least one IP address assigned to this component can be reached by the FSM. Alternatively, you can choose the option to generate a unique local address (ULA) when managing the chassis. Ensure that the chassis component has an IP address that can be reached by the Flex System Manager or select the generate ULA option and attempt to manage the chassis again.

DNZFM2420W The chassis *VALUE_0* is centrally managing the node user accounts for IPMI and SNMP. If *VALUE_0* is centrally managed by FSM the management of these SNMPv3 and IPMI accounts will be controlled by the managed endpoints (IMMv2). The current accounts will be preserved, but you will not be able to manage them from the CMM. To successfully manage *VALUE_0* use the force option when using a CLI command or select the OK button to continue when using the web interface.

DNZFM3000E The feature key file could not be imported. Make sure that the feature key is being imported to the FSM for which it was purchased. Then, attempt to import the feature key again.

DNZFM3001E The specified feature key file (*VALUE_0*) could not be opened. Make sure that you specify the full path to a valid key and that the key file is in the specified location. Then attempt to import the key again.

DNZFM3002I The feature key was imported successfully. You need to restart the FSM to begin using the feature.

DNZFM3003E An internal error occurred while importing the key. Contact Support.

DNZFM3004E The feature key file could not be imported. The serial number in the key does not match this system.

DNZFM3005E The feature key file could not be imported. Feature {0} is not supported on the FSM.

DNZFM3006E The feature key file could not be imported. The file is not a valid key file and may have been corrupted.

DNZFM3007E The feature key file could not be imported. Validation of the signature failed. The file has been modified after it was created. Get a new copy of the file and try again.

DNZFM3008E An internal error occured. Try again or contact Support.

DNZFM4001E Certificate not found.

Explanation: Contact IBM support.

DNZFM5002E Unable to access the user registry. Verify that you are using the correct password.

DNZFM5003E A communication failure occurred accessing the user registry. Wait a few seconds and attempt the request again. If the problem persists, contact Support.

DNZFM5004E An error occurred during user registry initialization. If the problem persists, contact Support.

DNZFM5005E Cannot search for the specified entry because the search criteria are not valid. Verify that the search criteria is complete and valid. Then, attempt to search again.

DNZFM5006E Cannot create the specified user because one or more parameters are not valid. Verify that all parameters are valid and attempt to create the user again. If the problem persists, contact Support.

DNZFM5007E Cannot create or delete the specified role because one or more parameters are not valid. Verify that all parameters are valid and attempt to add or delete the role again. If the problem persists, contact Support.

DNZFM5008E Cannot create the specified role because the role information is not complete. Role name, type, and permissions are required. Verify that the role information is complete and valid. Then attempt to create the role again.

DNZFM5009E Unable to obtain roles from the user registry because FSM could not communicate with the user registry. If the problem persists, contact Support.

DNZFM5010E Predefined roles cannot be modified. Select a different role to be changed.

DNZFM5011E The specified role type *VALUE_0* is not valid. Specify a valid role type, such as CMM, IMM or FSM.

DNZFM5012E The specified user {0} exists. Choose a different user name and try the request again.

DNZFM5013E The specified role {0} type {1} exists. Choose a different role name and try the request again.

DNZFM5015E An exception occurred while modifying a role. No changes have been made to the role. Verify that the role has at least one set of permissions associated with it. If the role is associated with a chassis, make sure that the chassis is available and being managed by the FSM. Then, attempt to modify the role again.

DNZFM5017E The user group {0} cannot be changed because it does not exist.

DNZFM5018E The user group {0} cannot be deleted because it does not exist.

DNZFM5019E A FSM internal error occurred in the user management component. Contact Support.

DNZFM5020E A FSM internal error (null parameter) occurred in the user management component. If the problem persists, contact Support.

DNZFM5021E The selected chassis is already managed by FSM. Select a different chassis to manage.

DNZFM5022E An internal error occurred while attempting to put a chassis under management. This might be a network communication error, a problem with the user registry on the CMM, or the CMM might not be available. Attempt to put the chassis under management again. If the problem persists, contact Support.

DNZFM5023E An internal error occurred while attempting to put a chassis under management. This might be a problem with the user registry on the FSM. If the problem persists, contact Support.

DNZFM5024E An internal error occurred while adding a new element to the user registry. If the problem persists, contact Support.

DNZFM5025W An attempt was made to remove a chassis from FSM management, but the chassis was not found in the list of managed chassis.

DNZFM5026E An error occurred while attempting to locate branch {0} in the user registry. The branch does not exist. Verify that the chassis is under FSM management and try the request again. If the problem persists, contact Support.

DNZFM5027E An internal error occurred while attempting to put a chassis under management. The FSM could not create a new branch: {0} in the user registry. Attempt to put the chassis under management again. If the problem persists, contact Support.

DNZFM5028E An internal error occurred while attempting to change the internal system-defined user registry configuration. If the problem persists, contact Support.

DNZFM5029E One or more errors occurred while updating the system password. The system will be restarted now. For more information, contact Support.

DNZFM5030E An attempt was made to place this FSM under management, which is not allowed. Make sure that you are using the IP address or host name for a CMM in a chassis that has connectivity to the FSM. If the problem persists, contact Support.

DNZFM5031E The IP address for the user registry on the CMM is not valid. If the problem persists, contact Support.

DNZFM5032E A user with the specified user group name {0} exists. Choose a different user group name and try the request again.

DNZFM5033E A user group with the specified user name {0} exists. Choose a different user name and try the request again.

DNZFM5034E A specified permission is not valid for role type {0}. Specify a valid permission.

DNZFM5035E User {0} could not be created. Verify that the group to which the user belongs is valid and that the user roles and resources exist. Then attempt to create the user again. If the problem persists, contact Support.

DNZFM5036E An internal error occurred while attempting to access the password policy for the FSM. Contact Support.

DNZFM5037E An internal error occurred while attempting to put a chassis under management. The FSM could not create one of the required objects: {0} in the user registry. Attempt to put the chassis under management again. If the problem persists, contact Support.

DNZFM5038E The specified {0} role {1} does not exist. Choose a different role and try the request again.

DNZFM5039E The user has insufficient permissions to perform the requested action.

DNZFM5040E An internal error occurred while attempting to update the identifier of a chassis that is under management. The chassis with identifier {0} was not found in the list of managed chassis maintained by the user management component. If the problem persists, contact Support.

DNZFM5041E An error occurred while attempting to retrieve the FSM authentication mode (remote or local). Run the resetToLocal command to recover. Then, run the remote user registry setup wizard if you want to use an external user registry. If the problem persists, contact Support.

DNZFM5042E The password provided is incorrect. Re-enter the current system password.

DNZFM5043E User {0} is a FSM required user and cannot be deleted.

DNZFM5044E The syntax for the role resources or role scope is not correct. Verify that the command contains at least one compute node bay or I/O bay. When adding a user to an IMM type role, be sure to include a centrally managed chassis as well.

DNZFM5046E An internal error occurred while attempting to retrieve the password policy information for the FSM. Contact support.

DNZFM5047E Unable to update the LDAP attribute. The schema policy does not allow the requested action.

DNZFM5048E The user {0} cannot be changed because it does not exist.

DNZFM5049E The user {0} cannot be deleted because it does not exist.

DNZFM5050E The role {0} cannot be changed because it does not exist.

DNZFM5051E The role {0} cannot be deleted because it does not exist.

DNZFM5052E The user {0} cannot be created because user group {1} does not exist in the user registry.

DNZFM5053E The user {0} cannot be created because role {1} does not exist.

DNZFM5054E The user {0} cannot be modified because user group {1} does not exist in the user registry.

DNZFM5055E The user {0} cannot be modified because {1} role {2} does not exist.

DNZFM5056E The specified user group {0} exists. Choose a different user group name and try the request again.

DNZFM5057E The user group {0} cannot be created because user {1} does not exist.

DNZFM5058E The user group {0} cannot be created because {1} role {2} does not exist.

DNZFM5059E The user group {0} cannot be modified because user {1} does not exist.

DNZFM5060E The user group {0} cannot be modified because {1} role {2} does not exist.

DNZFM5061E The user name *VALUE_0* is not valid. The name must begin with an alphabetic character, and it must contain only a-z,A-Z,0-9, - or _. It must be no longer than 32 characters. Enter a valid user name.

DNZFM5062E The user group name *VALUE_0* is not valid. The name cannot contain certain non-alphabetic characters, such as ! # $ & ( ) + = | ; ' < > , . ? / . Enter a valid user group name.

DNZFM5063E The role name *VALUE_0* is not valid. The name cannot contain certain non-alphabetic characters such as ! # $ & ( ) + = | ; ' < > , . ? / . Enter a valid role name.

DNZFM5065E User group {0} is a required user group and cannot be deleted.

DNZFM5066E An error occurred while updating the user's password on the local file system. If the problem persists, contact Support.

DNZFM5067E User {0} is a required user and cannot be disabled.

DNZFM5068E The specified password for user {0} is not correct. Enter the correct password.

DNZFM5069E The new password does not meet the password policy criteria. Re-enter a different password.

DNZFM5070E The specified new password has been used recently. The password policy in effect for the FSM controls the number of previously used passwords that cannot be used. Specify a different password.

DNZFM5071E The password cannot be changed because it was modified recently. The password policy in effect for the FSM controls how often passwords can be changed. Wait the required time interval and attempt to change the password again.

DNZFM5072E User {0} is a required user and cannot be modified.

DNZFM5073E User group {0} is a required user group and cannot be modified.

DNZFM5074E User group {0} is a required user group and its roles cannot be modified.

DNZFM5075E User {0} is a FSM required user and its membership cannot be modified.

DNZFM5076E The new password must have at least {0} characters.

DNZFM5077E To change or reset the password for the user root, select the Change System Password task under the Administration tab or use the chFsmSysPwd command.

DNZFM5078E Changing the password for user {0} is not supported.

DNZFM5079I Users {0} were deleted. Users {1} were not deleted. Users that are not deleted do not exist or are in use.

DNZFM5080I User groups {0} were deleted. User groups {1} were not deleted. User groups that are not deleted do not exist.

DNZFM5081E The specified password does not meet the criteria for a secure password for reason {0}. Reason 1: Password must contain at least three of the following characters in any combination: one lowercase alphabetic character, one uppercase alphabetic character, one numeric character, one special character. Reason 2: Password must contain no more than three of the same characters used consecutively. Reason 3: Password must not be a repeat or reverse of the associated user ID. Reason 4: Password must contain at least 2 characters that are different from the previous password.

DNZFM5082E User group {0} cannot be removed. All users must be a member of this user group.

DNZFM5083E The {0} user group must be specified for the user. All users must be a member of {0} user group.

DNZFM5084E Users belonging to the FSM {0} role must be in the {1} user group.

DNZFM5085E The security policy level for the FSM is set to secure. The password policy settings do not meet the criteria for the secure policy level. Use the setFsmSecPolicy command to set the FSM security policy level.

DNZFM5086E User {0} is a FSM user and cannot be specified.

DNZFM5087E The account for user {0} is locked. See the system administrator for help.

DNZFM5088E The password provided is incorrect. Retry the command using the correct system password.

DNZFM5089E An error occurred while importing the certificate during external user registry setup. Check the file path of the certificate to make sure it is correct.

DNZFM5200I Command completed successfully.

DNZFM5201I Resetting the user registry configuration.

DNZFM5202E Role {0} already exists. Choose a different role name.

DNZFM5203E Role {0} type {1} does not exist.

DNZFM5204E User {0} does not exist.

DNZFM5205E Command failed.

DNZFM5206E Cannot create entry {0} because one or more parameters set for the object are not valid. Verify that all parameters are valid and attempt to create the entry again. If the problem persists, contact Support.

DNZFM5207E Usage error: the *VALUE_0* can only be used if the *VALUE_1* option is also specified.

DNZFM5208E No options were specified when invoking the command.

DNZFM5209E The command terminated due to an unexpected internal error. If the problem persists, contact Support.

DNZFM5210E The *VALUE_0* option requires a value. Run the command again, specifying a value for the option. See the command help for the correct usage.

DNZFM5211E The value {0} is not valid for the specified option. See the command help for the correct usage.

DNZFM5213E The FSM is using an external user registry therefore the chassis cannot be centrally managed. Do not select the chassis to be centrally managed and try the request again.

DNZFM5214I There are no centrally managed chassis.

DNZFM5215E The CLI command lsCentrallyManagedChassis failed for this reason: {0}.

DNZFM5216E The CLI command rmCentrallyManagedChassis failed for this reason: {0} If the problem persists, contact Support.

DNZFM5217I Chassis with UUID: {0} was removed from centralized management successfully. You must now reaquire access with credentials for the chassis.

DNZFM5218E The UUID (parameter -u | --uuid) is required. Attempt to run the command again, specifying a valid UUID.

DNZFM5219E User name error: *VALUE_0* is not a valid user name. The user name must begin with an alphabetic character, must contain only a-z,A-Z,0-9, - or _, and must be no longer than 32 characters.

DNZFM5220E Chassis error: *VALUE_0* is not a centrally managed chassis. Use the lsCentrallyManagedChassis CLI command to find all centrally managed chassis.

DNZFM5221E Role error: *VALUE_0* is not a valid role entry. The role must have the format role-type:role-name[:role-target].

DNZFM5222E Extending and removing roles cannot be specified together. Choose to extend or to remove roles.

DNZFM5223E Extending and removing groups cannot be specified together. Choose to add or to remove groups.

DNZFM5224E SSH time out value must be non-negative and less than 2147483647. Enter a valid value for SSH time out.

DNZFM5225E Role {0} that is type {1} must contain at least one chassis.

DNZFM5226E Cannot change, delete, add, or remove user group {0} because it does not exist.

DNZFM5227I You will need to restart the FSM to activate this change.

DNZFM5228I User {0} created successfully.

DNZFM5229E Both user and password must be specified.

DNZFM5230I User group {0} created successfully.

DNZFM5231I User group {0} changed successfully.

DNZFM5232I User {0} changed successfully.

DNZFM5233I Role {0} created successfully.

DNZFM5234I Role {0} changed successfully.

DNZFM5235E An internal error occurred attempting to manage the CMM: {0}. If the problem persists, contact Support.

DNZFM5236E Specify Supervisor or Operator for the FSM role but not both.

DNZFM5237E Supervisor or Operator cannot be specified as the FSM type role for a user group.

DNZFM5238E Extending and removing permissions cannot be specified together. Choose to extend or to remove permissions.

DNZFM5239E Extending and removing scope entries cannot be specified together. Choose to extend or to remove scope entries.

DNZFM5240E All permissions cannot be removed from a role. A role must have at least one permission.

DNZFM5241E All scope entries cannot be removed from a role. A role must have at least one scope entry.

DNZFM5242E The *VALUE_0* option is not a valid option for an IMM role. See the command help for the correct usage.

DNZFM5243E Role name does not have the correct syntax. Specify roleType:roleName.

DNZFM5244I User {0} was removed successfully.

DNZFM5245I User groups were removed successfully.

DNZFM5246I Role {0} type {1} was removed successfully.

DNZFM5247I There are no CMM custom roles.

DNZFM5248I There are no IMM custom roles.

DNZFM5249E *VALUE_0* is not a valid user group name. A user group name cannot contain certain non-alphabetic characters such as ! # $ & ( ) + = | ; ' < > , . ? / .

DNZFM5250E *VALUE_0* is not a valid role name. A role name cannot contain certain non-alphabetic characters such as ! # $ & ( ) + = | ; ' < > , . ? / .

DNZFM5251E Resource group {0} does not exist.

DNZFM5252I The user {0} is locked = {1}.

DNZFM5253I The user {0} has been locked successfully.

DNZFM5254I The user {0} has been unlocked successfully.

DNZFM5255E User, old, and new passwords are required parameters.

DNZFM5256E Password for user {0} was changed successfully.

DNZFM5257E User name must be specified.

DNZFM5258E The password for user {0} was reset successfully.

DNZFM5259I The password for user {0} has expired.

DNZFM5260I The password for user {0} has not expired.

DNZFM5261I Temporary password: {0}

DNZFM5262E The following file could not be loaded: {0}

DNZFM5263E Usage error: Old and new password cannot be the same.

DNZFM5264I The password for user {0} is expired: {1}.

DNZFM5265I The password and verification password entered for user {0} do not match.

DNZFM5266I The user {0} is not locked.

DNZFM5267E The user {0} is in use and cannot be deleted.

DNZFM5268E Usage error: At least one value listed for the scope is not valid.

DNZFM5269I This command is not supported on the Flex System Manager.

DNZFM5270I User group {0} could not be created.

DNZFM5271I User {0} could not be created.

DNZFM5272E Extending and removing users cannot be specified together. Choose to add or to remove users.

DNZFM5273I Some settings for user {0} could not be changed. See the previous errors for specific issues with those settings.

DNZFM5274I Some settings for user group {0} could not be changed. See the previous errors for specific issues with those settings.

DNZFM5275E Old and new passwords are required parameters.

DNZFM5276I The system password was changed successfully. System is being restarted for the change to take effect.

DNZFM5277I Are you sure that you want to change the system password and restart the Flex System Manager? (Y,N)

DNZFM5278I You entered {0}. The system will be restarted after the password is changed.

DNZFM5279I You entered {0}. The command is canceled.

DNZFM5280E Userid: {0} or password: {1} is incorrect. If a valid userid is given, that account may become locked if too many attempts are made with an incorrect password. Try the request again with caution.

DNZFM5281E An internal error occurred attempting to unmanage the CMM: {0}. The LDAP client configuration was not reset.

DNZFM5282E The *VALUE_0* option is limited to {1} characters. Run the command again, specifying a different value.

DNZFM5283E Usage error: At least one value listed for the scope is not valid. Specify c1 for a chassis, bay 1 to 10, or iobay 1 to {0}.

DNZFM5284E The specified UUID: {0} is not valid. Try the command again specifying a valid UUID. Run the CLI command lsCentrallyManagedChassis and select the appropriate UUID from the output.

DNZFM5285E The attempt to remove chassis with UUID: {0} from centralized management was partially successful. The Flex System Manager now recognizes the CMM as decentralized, however some operations failed while decentralizing the chassis. Make sure the chassis is functioning and connected to the network. Then, log in to the chassis command-line interface using the RECOVERY_ID user account. Verify that user registry authentication is set to local authentication (CMM command: accseccfg -am local -T mm[p]), verify that the SSL client is disabled (CMM command: sslcfg -client disabled -tc1 remove -T mm[p]) and verify that the CMM local accounts are not disabled (CMM command: fsmcm -off -T mm[p]). If the problem persists, contact Support.

DNZFM5300E This Flex System Manager is configured to use an external registry. This command is not supported for use with an external registry. Instead, you must use the commands that are available with the external registry.

DNZFM5301E The name *VALUE_0* is not a valid name for this command. Review the command help then try the command again.

DNZFM5302E The Flex System Manager Operating System and user registry passwords are not synchronized. Run this command again using a new password that meets the Password policies set on this Flex System Manager.

DNZFM5303E This Flex System Manager is configured to use the internal registry. This command is not supported for use with an internal registry. Instead, you must use the commands that are available with the internal registry.

DNZFM8750E A valid operating system image file in an ISO format must be specified.

DNZFM8751E Only one operating system image file may be specified at a time.

DNZFM8752E The specified operating system image does not exist.

DNZFM8753E An internal error occurred while importing the image. Attempt the command again. If the problem persists, contact Support.

DNZFM8754E The deployment service encountered a problem while importing the image. Restart the FSM and attempt the command again. If the problem persists, contact Support.

DNZFM8755E The specified operating system image is not valid. Attempt the command again, specifying a supported operating system image.

DNZFM8756W An expected return code was returned while importing the image. Return code: {0}.

DNZFM8757I The image was imported sucessfully.

DNZFM8758I The import operation will continue to run in the background.

DNZFM8759E The imported operating systems could not be retrieved.

DNZFM8760W Information is still being collected about the FSM and its managed chassis.

Explanation: One of the services required by the FSM is not initialized.

DNZFM8761E Invalid task activation context is passed. Retry the operation with valid activation context.

DNZFM8762E At least one compute node must be specified for deploying image. Retry the operation with valid compute node.

Explanation: No compute nodes provided for deploying image.

DNZFM8763E The number of image deployments in progress (*VALUE_0*) and the newly requested image deployments (*VALUE_1*) exceeds the maximum number of images that can be deployed concurrently. You can deploy a maximum of *VALUE_2*) images concurrently.

DNZFM8764E Required image deployment data is missing in the task activation context.

DNZFM8765E The *VALUE_0* service is not available.

Explanation: One of the services required by the Flex System Manager is not available.

DNZFM8766E An internal error occurred while the FSM was attempting to activate the image deployment process (invalid image deployment data *VALUE_0*).

DNZFM8767E An internal error occurred while attempting to deploy an operating system image (*ERROR_MSG*).

DNZFM8768E The image for compute node *VALUE_0* cannot be deployed. An internal error (missing image deployment data) occurred while attempting to deploy the operating system image for the compute node.

DNZFM8769E An internal error occurred while attempting to deploy an operating system image.

DNZFM8770E The operating system deployment process did not complete for compute node *VALUE_0*. The image deployment process for this compute node did not complete because another image deployment is already in progress for this compute node.

DNZFM8771E The operating system deployment process did not complete for compute node *VALUE_0*. The image deployment process for this compute node did not complete because it is not a server resource.

DNZFM8772E The operating system deployment process did not complete for compute node *VALUE_0* (*VALUE_1*). The image deployment process for this compute node did not complete because the FSM cannot identify the MAC address for this compute node. Collect inventory of this compute node and attempt to deploy the image again.

DNZFM8773E The operating system deployment process did not complete for compute node *VALUE_0* (*VALUE_1*). The image deployment process for this compute node did not complete because this compute node is not unlocked. From the FSM, request access to the compute node and attempt to deploy the image again.

DNZFM8774E The operating system deployment process did not complete for compute node *VALUE_0* (*VALUE_1*). The image deployment process for this compute node did not complete because this compute node is offline. Make sure the compute node is functioning and that there is a working network connection between the FSM and the compute node. Perform verify connection to the compute node and attempt to deploy the image again.

DNZFM8775E The operating system deployment process did not complete for compute node *VALUE_0* (*VALUE_1*). The image deployment process for this compute node did not complete because this compute node does not have an associated restart or power-on task. Make sure the compute node is functioning and that there is a working network connection between the FSM and the compute node. Perform verify connection to the compute node and attempt to deploy the image again.

DNZFM8776E The operating system deployment process did not complete for compute node *VALUE_0* (*VALUE_1*). The image deployment process for this compute node did not complete because the FSM cannot determine which chassis is managing this compute node. Collect inventory on the chassis managing this compute node and attempt to deploy the image again.

DNZFM8777E The operating system deployment process did not complete for compute node *VALUE_0* (*VALUE_1*). The image deployment process for this compute node did not complete because the chassis *VALUE_2* (*VALUE_3*) managing this compute node is not unlocked. Perform request access to the chassis and attempt to deploy the image again.

DNZFM8778E The operating system deployment process did not complete for compute node *VALUE_0* (*VALUE_1*). The image deployment process for this compute node did not complete because the chassis *VALUE_2* (*VALUE_3*) managing this compute node is offline. Make sure that the chassis is functioning and that there is a working network connection between the FSM and the chassis. Perform verify connection to the chassis and attempt to deploy the image again.

DNZFM8779I Image deployment lock acquired for compute node *VALUE_0* (*VALUE_1*).

DNZFM8780E An exception occured while acquiring an image deployment lock for compute node *VALUE_0*. The associated error is *ERROR_MSG*.

DNZFM8781I Pre-deployment validation completed sucessfully for all specified compute nodes.

DNZFM8782E The operating system deployment process did not complete for compute node *VALUE_0* (*VALUE_1*). The image deployment process for this compute node has timed out while preparing for image deployment at *VALUE_2*. Make sure the compute node is functioning and that there is a working network connection between the FSM and the compute node.

DNZFM8783I All valid targeted compute nodes preparation for image deployement has completed sucessfully.

DNZFM8784I Started monitoring *VALUE_0* image deployments for compute nodes *VALUE_1*.

DNZFM8785E The operating system deployment process did not complete for compute node *VALUE_0* (*VALUE_1*). The image deployment process for this compute node has timed out because its status has not been updated from *VALUE_2* in the last *VALUE_3* minutes. Make sure the compute node is functioning and that there is a working network connection between the FSM and the compute node.

DNZFM8786I Image deployment has completed successfully on the compute node *VALUE_0* (*VALUE_1*).

DNZFM8787I Image deployment has completed successfully for all specified compute nodes.

DNZFM8788E The operating system deployment process did not complete for the compute node. The image deployment process did not complete because the Flex System Manager could not create a node profile for this compute node.

DNZFM8789E The operating system deployment process did not complete for compute node *VALUE_0* (*VALUE_1*). The image deployment process for this compute node did not complete because an internal exception occured while creating a node profile for this compute node.

DNZFM8790E The operating system deployment process did not complete for the compute node. The image deployment process did not complete because the Flex System Manager could not get node profile information for this compute node.

DNZFM8791E The operating system deployment process did not complete for compute node *VALUE_0* (*VALUE_1*). The image deployment process for this compute node did not complete because an node profile was not found for this compute node.

DNZFM8792W Failed to get node profile infromation for the compute node.

DNZFM8793E The operating system deployment process did not complete for the compute node. The image deployment process did not complete because the Flex System Manager could not create a bootable ISO image for this compute node.

DNZFM8794E The operating system deployment process did not complete for compute node *VALUE_0* (*VALUE_1*). The image deployment process did not complete because the Flex System Manager could not create a bootable ISO image for this compute node.

DNZFM8795E The operating system deployment process did not complete for the compute node. The image deployment process did not complete because the Flex System Manager could not mount the remote media to this compute node. Make sure the compute node is functioning and that there is a working network connection between the FSM and the compute node.

DNZFM8796E The operating system deployment process did not complete for compute node *VALUE_0* (*VALUE_1*). The image deployment process did not complete because the Flex System Manager could not mount the remote media *VALUE_2* to this compute node. Make sure the compute node is functioning and that there is a working network connection between the FSM and the compute node.

DNZFM8797E The operating system deployment process did not complete for compute node *VALUE_0* (*VALUE_1*). The image deployment process did not complete because the Flex System Manager could not mount the remote media *VALUE_2* to this compute node (error code of *VALUE_3*). Make sure the compute node is functioning and that there is a working network connection between the FSM and the compute node.

DNZFM8798E Failed to unmount bootable ISO due to missing information about the compute node.

DNZFM8799E Could not unmount remote media *VALUE_0* from compute node *VALUE_1* (*VALUE_2*).

DNZFM8800E An *VALUE_0* error occured during the unmount of remote media *VALUE_1* from compute node *VALUE_2* (*VALUE_3*).

DNZFM8801E The operating system deployment process did not complete for the compute node. The image deployment process did not complete because the Flex System Manager could not modify the UEFI boot sequence for this compute node. Make sure the compute node is functioning and that there is a working network connection between the FSM and the compute node.

DNZFM8802E The operating system deployment process did not complete for compute node *VALUE_0* (*VALUE_1*). The image deployment process did not complete because the Flex System Manager could not modify the UEFI boot sequence for this compute node. Make sure the compute node is functioning and that there is a working network connection between the FSM and the compute node.

DNZFM8803E The operating system deployment process did not complete for compute node *VALUE_0* (*VALUE_1*). The image deployment process did not complete because this compute node did not restart.

DNZFM8804E The operating system deployment process did not complete for compute node *VALUE_0* (*VALUE_1*). The image deployment process did not complete because the Flex System Manager cannot restart or power on this compute node. Make sure the compute node is functioning and that there is a working network connection between the FSM and the compute node.

DNZFM8805E Unable to determine FSM system administrator user ID for the remote media mount operation.

DNZFM8806E Unable to determine FSM password for the system administrator user account *VALUE_0*.

DNZFM8807E An internal error occurred due to an invalid or missing value for *VALUE_0* property in FlexCat.properties file.

DNZFM8808E An internal error occurred (JSON response *VALUE_0*)

DNZFM8809E REST method *VALUE_0* is not supported.

DNZFM8810I Image deployment status for compute node *VALUE_0* (*VALUE_1*) updated to *VALUE_2*.

DNZFM8811E Invalid image deployment status *VALUE_0* reported for image deployment *VALUE_1*.

DNZFM8812W Image deployment for compute node *VALUE_0* is not in progress.

DNZFM8813I A node profile for image deployment was created successfully for compute node *VALUE_0* (*VALUE_1*) using node profile name of *VALUE_2*.

DNZFM8814I Bootable ISO image was created successfully for compute node *VALUE_0* (*VALUE_1*) and image name *VALUE_2*.

DNZFM8815I Bootable ISO image *VALUE_0* has been mounted successfully to compute node *VALUE_1* (*VALUE_2*).

DNZFM8816I The UEFI boot order sequence has been modified successfully for compute node *VALUE_0* (*VALUE_1*).

DNZFM8817I Restarting compute node *VALUE_0* (*VALUE_1*) to boot from the mounted iso image *VALUE_2*.

DNZFM8818I Image deployment preparation completed successfully for compute node *VALUE_0* (*VALUE_1*).

DNZFM8819E The operating system deployment process did not complete for compute node *VALUE_0* (*VALUE_1*). An error occurred while trying to restart the compute node. Wait several minutes and verify that the image was successfully deployed on the compute node by attempting to discover the operating system through the IBM Flex System Manager.

DNZFM8820E The operating system deployment process did not complete for compute node *VALUE_0* (*VALUE_1*). The image deployment process for this compute node has timed out because its status has not been updated from *VALUE_2* in the last *VALUE_3* minutes. Make sure the compute node is functioning and that there is a working network connection between the FSM and the compute node.

DNZFM8821I Discovering the newly installed operating system *VALUE_0* running on compute node *VALUE_1* (*VALUE_2*).

DNZFM8822E The newly installed operating system *VALUE_0* running on compute node *VALUE_1* (*VALUE_2*) could not be discovered.

Explanation: The operating system was deployed but the IBM Flex System Manager is not able to discover it.

DNZFM8823I Image deployment completed successfully for compute node *VALUE_0* (*VALUE_1*).

DNZFM8824I Image deployment completed with errors. Errors occurred while attempting to deploy the operating system to the compute nodes. Check previous messages in this job log for information about the errors.

DNZFM8825E Global settings have not been applied. The IP assignments mode for image deployments cannot be changed while there are images currently being deployed. Wait until all images have been deployed and retry the operation.

DNZFM8826E The operating system cannot be deployed for compute node *VALUE_0* (*VALUE_1*). The installed IMM firmware version *VALUE_2* is not at or above required minimum version of *VALUE_3*. Update the firmware for this compute node and attempt to deploy the operating system image again.

DNZFM8827E The operating system cannot be deployed for compute node *VALUE_0* (*VALUE_1*). The installed UEFI firmware version *VALUE_2* is not at or above required minimum version of *VALUE_3*. Update the firmware for this compute node and attempt to deploy the operating system image again.

DNZFM8828E The operating system cannot be deployed for compute node *VALUE_0* (*VALUE_1*). The IBM Flex System Manager cannot deploy the operating system to the compute node because there is not enough free storage space in *VALUE_2* on IBM Flex System Manager for hosting the bootable ISO image.

DNZFM8829E The specified operating system image name was not found in IBM Flex System Manager inventory.

DNZFM8830E One or more required parameters is missing. For more information about the required options, see the help that is available for the command.

DNZFM8831E One or more parameters are not valid. For more information about the options, see the help that is available for the command.

DNZFM8832E The xCat server restart operation completed with an error. Return code: {0}.

DNZFM8833I No operating system images to display.

DNZFM8834I The specified operating system image name was found in IBM Flex System Manager inventory.

DNZFM8835E The specified operating system profile cannot be deleted.

DNZFM8836E The specified operating system profile cannot be deleted. An internal error occurred (REST call) while attempting to delete the operating system profile.

DNZFM8837E No operating system image was specified to be deleted.

DNZFM8838E Only one operating system image at a time can be specified for deletion.

DNZFM8839I The import operation has started.

DNZFM8840E The maximum number of imported operating systems has been reached. IBM Flex System Manager supports a maximum of *VALUE_0* imported operating system images. Delete an operating system image, using smcli deleteosimage, and attempt the import operation again.

DNZFM8841I Command: *VALUE_0* was successful.

DNZFM8842E The image deployment service is disabled.

DNZFM8843E The default operating system credential have not been changed. The default opreating system credential cannot be changed while there are images currently being deployed. Wait until all images have been deployed and retry the operation.

DNZFM8844E The default operating system credential have not been changed. An error occured while updating the default opreating system credential for key *VALUE_0*.

DNZFM8845E Failed to get the default credentials to be used during operating system deployment.

DNZFM8846I Discovery of ESXi operating system using IPv6 address is not supported. The newly installed operating system running on compute node *VALUE_0* (*VALUE_1*) cannot be auto discovered. Manually discover this operating system using IPv4 address.

Explanation: The operating system was deployed but the IBM Flex System Manager does not support discovering ESXi using IPv6 address.

DNZFM8847E The operating system image *VALUE_0* cannot be imported. The IBM Flex System Manager image repository directory *VALUE_1* does not have enough free space to import the given operating system image of size *VALUE_2*. Delete unused operating system image, using smcli deleteosimage, and attempt the import operation again.

DNZFM9001E Unable to generate security certificate because of an internal error (command failure). Make sure that your user ID is assigned to a role of SMAdministrator (smadmin group) and attempt to generate the certificate again. If the problem persists, contact Support.

DNZFM9002E Internal error occurred (command interrupt). Contact Support.

DNZFM9003E Unable to regenerate user registry certificates. Make sure that the specified user ID has sufficient permissions to regenerate a certificate. Then attempt to regenerate the certificate again. If the problem persists, contact Support.

DNZFM9004E Unable to generate user registry certificates. Make sure that the specified user ID has sufficient permissions to generate a certificate. Then attempt to generate the certificate again. If the problem persists, contact Support.

DNZFM9005E An internal error occurred (exception) while generating user registry certificates during centralized management setup. Contact Support.

DNZFM9006E An internal error occurred (failed return code) while generating user registry certificates during centralized management setup. Contact Support.

DNZFM9007E An internal error occurred while processing a security policy. Error: {0} occurred in method: {1}. Contact Support.

DNZFM9008E An internal error occurred while attempting to get the FSM security policy level. Contact Support.

DNZFM9009E The object identifier (parameter -o | --oid) value {0} is not valid. It must be the object identifier for a CMM that is currently managed by the FSM. Attempt to run the command again, specifying a valid object identifier.

DNZFM9010E The security level (parameter -l | --level) value {0} is not supported. Attempt to run the command again, specifying legacy or secure for the security level.

DNZFM9011E The security level (parameter -l | --level) is required. Attempt to run the command again, specifying a valid security level.

DNZFM9012E The object identifier (parameter -o | --oid) is required. Attempt to run the command again, specifying a valid object identifier.

DNZFM9013E Command failed with exception: {0}. Contact Support.

DNZFM9014E The specified security policy for CMM: {0} failed with return code: {1}.

DNZFM9015E The specified security policy for the FSM failed with return code: {0}.

DNZFM9016I The security policy for CMM: {0} was successfully set to: {1}.

DNZFM9017I The security policy for the FSM was successfully set to: {0}.

DNZFM9018E The security policy level for the FSM must be set to legacy to change legacy protocols.

DNZFM9019E A required parameter was not specified. Attempt to run the command again, specifying either the enable or disable parameter (-E|--enable or -D|--disable).

DNZFM9020E The specified protocol {0} is not a supported protocol. Run the command again, specifying a valid protocol.

DNZFM9021I The {0} protocol has been disabled successfully.

DNZFM9022E Unable to disable {0} protocol. Attempt to run the command again. If the problem persists, contact Support.

DNZFM9023I The {0} protocol has been enabled successfully.

DNZFM9024E Unable to enable {0} protocol. Attempt to run the command again. If the problem persists, contact Support.

DNZFM9025E An internal error occurred while importing a certificate during external user registry setup. Refer to previous messages in the log for specific details. If no earlier messages exist, contact Support.

DNZFM9026W While removing a certificate the following exception occurred: {0}. This may occur in normal processing. If there are no other issues, ignore this warning.

DNZFM9027W The security policy is already at the requested level. Try the request again, specifying a different level.

DNZFM9028W FSM security policy level was updated to {0}, but any chassis that were centrally managed did not get updated to the new policy. Use the Web interface to check the security policy of the managed chassis and update it if necessary.

DNZFM9029W The following unsecure protocol: {0} is active on the FSM so the security policy level cannot be upgraded to: {1}. Use the chLegacyProtocol CLI command to disable the unsecure protocol, and try the request again.

DNZFM9030E An internal error occurred while attempting to get the chassis security policy level.

DNZFM9031E The following exception occurred while attempting to get or set the chassis security policy. Contact Support. Exception: {0}.

DNZFM9032E An internal error occurred while attempting to get the chassis security policy state. The state {0} is not supported.

DNZFM9040E An error occurred while changing the trust/key store password (internal error). Contact Support.

DNZFM9041E Unable to change the trust/key store password. Make sure that the previous password is correct, and that the new password complies with the current FSM security policy. If the problem persists, contact Support.

DNZFM9042E An error occurred getting the security policy status information for CMM {0}.

DNZFM9043E An internal error occurred (exception) while attempting to set or get a security policy. The exception is: {0}.

DNZFM9044E An internal error occurred while parsing the results from setting or getting the CMM security policy.

DNZFM9045E Security level check for chnetcfg was successful.

DNZFM9046E An error occurred while getting the key store or trust store password (internal error). Contact Support.

DNZFM9047E The TFTP server cannot be started because the required port is already in use. Verify that the Update Manager is not using this FSM as a TFTP server and try again. To verify this, go to the Home page, select the Plug-ins tab and then select Update Manager. From the Common Tasks section, select Configure Settings and make sure that the FSM is not used as a TFTP server.

DNZFM9048E The TFTP server cannot be stopped because it is in use by another process. Verify that the Update Manager is not using this FSM as a TFTP server and try again. To verify this, go to the Home page, select the Plug-ins tab and then select Update Manager. From the Common Tasks section, select Configure Settings and make sure that the FSM is not used as a TFTP server.

DNZFM9100W Security services did not start correctly. Wait a few minutes and try the command again. Then, restart the FSM. If the problem persists, contact Support.

DNZFM9101I This command is not supported on the Flex System Manager.

DNZFM9102W The Flex System Manager is managing one or more chassis. When you change the network interface for the management network, you must unmanage all chassis that are managed by the Flex System Manager and then manage the chassis again.

DNZFM9103W If the network interface for the management network is configured to use DHCP, the management interface IP address can change when the DHCP lease expires. If the address does change you will be required to unmanage all chassis that are managed and then manage all chassis again. Alternatively, you can change the management interface to a static IP address, you can make sure that the DCHP server configuration is set so that the DHCP IP address is based on a MAC address, or you can make sure that the DHCP server configuration is set to prevent the DHCP lease from expiring.

DNZFM9104W The Flex System Manager is managing one or more chassis. When the Flex System Manager LDAP certificate is reset, you must unmanage all chassis that are managed by the Flex System Manager and then manage the chassis again.

DNZPWZ050E The duration to continue checking for updates was not specified.

Explanation: A number greater than zero is required for the duration.

DNZPWZ051E The duration to continue checking for updates was not specified.

Explanation: A number greater than zero is required for the duration.

DNZPWZ052E The specified duration to continue checking for updates is not greater than zero.

Explanation: A number greater than zero is required for the duration.

DNZPWZ053E The specified duration to continue checking for updates is not greater than zero.

Explanation: A number greater than zero is required for the duration.

DNZPWZ055E The specified duration to continue checking for updates is not valid. A number between *VALUE_0* and *VALUE_1* is required for the duration.

Explanation:

DNZPWZ056I A valid duration was entered.

Explanation: The duration that was entered is valid.

DNZPWZ057E The date specified for the repeat until field is not valid.

Explanation: The repeat until date must be at least one week greater than the start date.

DNZPWZ058E The date specified for the repeat until field is not valid.

Explanation: The repeat until date must be at least one month greater than the start date.

DNZPWZ059E The date specified for the repeat until field is not valid.

Explanation: The repeat until date must be at least one year greater than the start date.

DNZPWZ060E No days of the week were specified to check for weekly updates.

Explanation: You must specify at least one day of the week to check for weekly updates.

DNZPWZ804E Unable to generate a job to check for updates.

Explanation: The management server cannot create a job to automatically check for updates.

DNZPWZ805E Unable to delete the job to check for updates.

Explanation: The management server cannot delete the job that automatically checks for updates.

DNZPWZ814I Starting to generate a job to check for updates.

Explanation:

DNZPWZ815I A job to check for updates job has been generated.

Explanation:

DNZPWZ816I Starting to remove the existing job that checks for updates.

Explanation:

DNZPWZ817I The job that checks for updates has been removed.

Explanation:

0000 Process completed successfully.

Explanation: The recovery process finished without error.

Severity: Info

User response: Information only; no action is required.

0002 The called script seems to be missing.

Explanation: The recovery process was unable to continue after attempting to call a required script. The script file might be missing, or named incorrectly.

Severity: Error

User response: Contact Support

0008 Something is wrong with the called script, possibly file corruption.

Explanation: The recovery process was unable to continue after attempting to call a required script. The script file might be corrupted on disk.

Severity: Error

User response: Contact Support

0011 Could not open var file.

Explanation: The recovery process was unable to continue after attempting to open a required file. The file might be misnamed, missing, or corrupted on disk.

Severity: Error

User response: Contact Support

0013 The called script is not executable. Check permissions.

Explanation: The recovery process was unable to continue after attempting to call a required script. The script file might not be set to allow execution.

Severity: Error

User response: Contact Support

0017 Could not find partition.

Explanation: The recovery process was unable to continue after attempting to locate a required disk partition.

Severity: Error

User response: Contact Support

0022 Could not make mount point.

Explanation: The recovery process was unable to continue after attempting to create a required mount point.

Severity: Error

User response: Contact Support

0025 Could not make images directory.

Explanation: The recovery process was unable to continue after attempting to create a directory to hold the dvm files.

Severity: Error

User response: Contact Support

0026 Copy failed; check cp_cmd.log.

Explanation: The recovery process was unable to continue after attempting a copy operation. Further details can be found in the indicated log file.

Severity: Warning

User response: Contact Support

0027 MD5 checksum failed.

Explanation: The recovery process was unable to continue after a checksum verification on the data files failed.

Severity: Error

User response: Complete the following steps until the problem is solved:

1. Clear working directory and re-download the ISOs if not originally obtained from IBM.

2. Re-image the DVDs
3. Contact Support

0040 **Could not mount service partition.**

Explanation: The recovery process was unable to continue after attempting to mount the system recovery partition.

Severity: Error

User response: Contact Support

0071 **Could not open var file.**

Explanation: The recovery process was unable to continue after attempting to open a required file. The file might be misnamed, missing, or corrupted on disk.

Severity: Error

User response: Contact Support

0077 **Could not find USB key. Please insert and try again.**

Explanation: The recovery process was unable to continue after attempting to find a required device.

Severity: Error

User response: Re-insert the USB device and repeat the operation.

0082 **Could not make mount point.**

Explanation: The recovery process was unable to continue after attempting to create a required mount point.

Severity: Error

User response: Contact Support

0099 **Exception raised (possibly CTRL-C or other invalid keyboard input). Check recovery_menu.log.**

Explanation: An invalid keyboard input interrupted the recovery process.

Severity: Warning

User response: Shut down the device and restart.

0100 **Could not mount partition.**

Explanation: The recovery process was unable to continue after attempting to mount a required disk partition.

Severity: Error

User response: Contact Support

0127 **Shell interpreter not found or not executable.**

Explanation: The system command interpreter is missing or is not executable.

Severity: Error

User response: Contact Support

0131 **Could not open var file.**

Explanation: The recovery process was unable to continue after attempting to open a required file. The file might be misnamed, missing, or corrupted on disk.

Severity: Error

User response: Contact Support

0132 **Could not create file.**

Explanation: The recovery process was unable to continue after attempting to create a required file.

Severity: Error

User response: Contact Support

0133 **Could not delete file.**

Explanation: The recovery process was unable to continue after attempting to delete a file.

Severity: Error

User response: Contact Support

0138 **Could not clear/create MBR.**

Explanation: The recovery process was unable to continue after attempting to clear or create the Master Boot Record on the system recovery partition.

Severity: Error

User response: Contact Support

0139 **fdisk operation failed.**

Explanation: The recovery process was unable to continue after an attempted fdisk operation.

Severity: Error

User response: Contact Support

0141 **Could not format partition.**

Explanation: The recovery process was unable to continue after attempting to format a disk partition.

Severity: Error

User response: Contact Support

0142 Could not make mount point.

Explanation: The recovery process was unable to continue after attempting to create a mount point.

Severity: Error

User response: Contact Support

0143 Could not mount partition.

Explanation: The recovery process was unable to continue after attempting to mount a required disk partition.

Severity: Error

User response: Contact Support

0146 Error copying files.

Explanation: The recovery process was unable to continue after attempting a copy operation.

Severity: Error

User response: Contact Support

0156 Could not deactivate the volume group.

Explanation: The recovery process was unable to continue after attempting to deactivate a volume group.

Severity: Error

User response: Contact Support

0171 Could not update one of UUID or bootloader.

Explanation: The recovery process was unable to continue after attempting to update the system recovery partition's UUID.

Severity: Error

User response: Contact Support

0172 Could not install boot loader.

Explanation: The recovery process was unable to continue after attempting to install the boot loader into the system recovery partition.

Severity: Error

User response: Contact Support

0173 Untar failed.

Explanation: The recovery process was unable to continue after attempting to extract the installer archive.

Severity: Error

User response: Complete the following steps until the problem is solved:

1. Restart the process.
2. Contact Support.

0175 Could not get UUID of destination partition.

Explanation: The recovery process was unable to continue after attempting to determine the UUID of the system recovery partition.

Severity: Error

User response: Contact Support

0176 Could not turn off swap.

Explanation: The recovery process was unable to continue after attempting to turn off the system swap volume.

Severity: Error

User response: Contact Support

0189 The hard disk in this system is not set to be the alternate boot device, and is configured as /dev/sda.

Explanation: The hard disk in this system is not set to be the alternate boot device, and is configured as /dev/sda.

Severity: Error

User response: Please review the procedures here to restore the RAID controller configuration to a proper working state: Restore RAID controller

0191 Could not open var file.

Explanation: The recovery process was unable to continue after attempting to open a required file. The file might be misnamed, missing, or corrupted on disk.

Severity: Error

User response: Contact Support

0192 Could not create file.

Explanation: The recovery process was unable to continue after attempting to create a required file.

Severity: Error

User response: Contact Support

0193 Could not delete fdisk temp file.

Explanation: The recovery process was unable to delete a temporary file used by the fdisk process.

Severity: Warning

User response: Contact Support

0199 Could not create/delete partition.

Explanation: The recovery process was unable to continue after attempting to either create or delete a disk partition.

Severity: Error

User response: Contact Support

0201 Could not format partition/logical volume.

Explanation: The recovery process was unable to continue after attempting to format a disk partition or logical volume.

Severity: Error

User response: Contact Support

0203 Could not mount partition/logical volume.

Explanation: The recovery process was unable to continue after attempting to mount a required disk partition or logical volume.

Severity: Error

User response: Contact Support

0204 Could not unmount partition/logical volume.

Explanation: The recovery process was unable to continue after attempting to unmount a required disk partition or logical volume.

Severity: Error

User response: Contact Support

0205 Could not make directory.

Explanation: The recovery process was unable to continue after attempting to create a directory.

Severity: Error

User response: Contact Support

0208 Could not create the logical volume.

Explanation: The recovery process was unable to continue after attempting to create the Data2 logical volume.

Severity: Error

User response: Contact Support

0209 Could not remove the logical volume.

Explanation: The recovery process was unable to continue after attempting to remove the Data2 logical volume.

Severity: Error

User response: Contact Support

0210 Could not activate logical volume.

Explanation: The recovery process was unable to continue after attempting to activate a required logical volume.

Severity: Error

User response: Contact Support

0211 Could not deactivate the logical volume.

Explanation: The recovery process was unable to continue after attempting to deactivate the Data2 logical volume.

Severity: Error

User response: Contact Support

0212 Could not find the logical volume in HostVG.

Explanation: The recovery process was unable to continue after attempting to find the Data logical volume in the Host volume group.

Severity: Error

User response: Contact Support

0213 Could not create the volume group.

Explanation: The recovery process was unable to continue after attempting to create the App volume group.

Severity: Error

User response: Contact Support

0214 Could not remove the volume group.

Explanation: The recovery process was unable to continue after attempting to remove the App volume group

Severity: Error

User response: Contact Support

0215 Could not activate the volume group.

Explanation: The recovery process was unable to continue after attempting to activate the Host volume group.

Severity: Error

User response: Contact Support

0216 Could not deactivate the volume group.

Explanation: The recovery process was unable to continue after attempting to deactivate the App volume group.

Severity: Error

User response: Contact Support

0217 Could not find HostVG.

Explanation: The recovery process was unable to continue after attempting to locate the Host volume group.

Severity: Error

User response: Contact Support

0218 Could not create the physical volume.

Explanation: The recovery process was unable to continue after attempting to create a required physical volume.

Severity: Error

User response: Contact Support

0219 Could not remove the physical volume.

Explanation: The recovery process was unable to continue after attempting to remove a physical volume.

Severity: Error

User response: Contact Support

0233 tar exited with an error.

Explanation: The recovery process was unable to continue after attempting to extract a dvm archive segment.

Severity: Error

User response: Restart the process

0256 Script returned "file not found".

Explanation: The recovery process was unable to continue after attempting to open a required file. The file might be misnamed, missing, or corrupted on disk.

Severity: Error

User response: Contact Support

0512 Unknown exit code.

Explanation: This is a generic error message covering unexpected results from external tasks.

Severity: Error

User response: Contact Support

0997 Task returned an error.

Explanation: This is a generic error message covering unexpected errors in external tasks.

Severity: Error

User response: Contact Support

0998 Task failed to run.

Explanation: This is a generic error message covering unexpected errors in external tasks.

Severity: Error

User response: Contact Support

0999 Unknown error.

Explanation: This is a generic error message covering unexpected errors.

Severity: Error

User response: Contact Support

Troubleshooting the management software

Use this information to solve problems with IBM Flex System Manager management software.

For troubleshooting information about the Flex System Manager Types 7955, 8731, and 8734 management node, see the *Flex System Manager Types 7955, 8731, and 8734 Installation and Service Guide* document.

Access state problems

Use this information to identify the cause of an access state that is problematic (any access state other than *OK*), and configure access for the managed resource to correct the access state.

Resolving problems with access states for managed resources

The Access column in the table view of the IBM Flex System Manager management software web interface displays the access states for managed resources. The access state for a resource is a short description of the connection between the management software and the managed resources (endpoints such as chassis or components installed in chassis). The following table describes problematic access states and corrective procedures for configuring access to managed resources.

Unknown

The access state *Unknown* indicates that the management software cannot determine the access state for the managed resource (for example, the management software might not have attempted to connect to the endpoint).

1. From the table view, select the box for the unknown resource.
2. Click **Actions** > **Security** > **Verify Connection**.
3. If the problem remains, contact your IBM representative.

Offline

The access state *Offline* indicates that all of the management software remote service access points (RSAPs) to the managed resource are not responding, so the management software has no connectivity.

Note: You might be able ping the managed resource from the management node (if you use telnet or SSH to it), but the management software requires a response through the protocols that it is using to manage the resource.
There are many possible reasons for this failure. Make sure that you investigate and, if necessary, address each of the following conditions that might be causing the failure:

- there is no physical connectivity
- firewall configuration for the network is preventing connectivity
- the managed resource is powered off and must be powered on
- the managed resource needs to be restarted

After the problem has been identified and resolved, reestablish a connection by either waiting for the next periodic operational status query (the default is 15 minutes) or complete the following steps:

1. From the table view, select the box for the offline resource.
2. Click **Actions** > **Security** > **Verify Connection**.
3. If the problem remains, contact your IBM representative.

Not trusted

The access state *Not trusted* indicates that the management software has connectivity to the managed resource, but the certificate presented by one or more of the RSAPs is not trusted.

The following list describes scenarios where this access state is common, and the procedures required to establish trusted access:

- **You reset the CMM to factory defaults, replaced the only Chassis Management Module (CMM) in your chassis with a new one, replaced the CA certificate for a CMM or the CMM became untrusted after a CMM fail over.** The CMM certificate is regenerated, and you must complete one of the following procedures, depending on whether your management software certificate policy is Explicit or Implicit. To determine the current policy see Changing the certificate policy.

  If the management software certificate policy is set to Explicit or the FSM version is prior to 1.3.2, you must manually copy the CA certificate from the CMM and save it to management software trust store. To add the certificate to the trust store and establish a connection to the CMM, complete the following steps:

  1. Manually add the certificate to the trust store. See "Certificate policies" in the *IBM Flex System Manager Systems Management Guide* PDF document for more information.
  2. From the table view, select the box for the CMM with the regenerated certificate; then, click **Actions** > **Security** > **Verify Connection**.

     Note: The chassis transitions to a trusted state quickly; however, the chassis components might take several minutes to be trusted.

  If the management software certificate policy is set to Implicit, complete the following steps:

  1. From the table view, select the box for the CMM that was reset.
  2. Click **Actions** > **Security** > **View Certificates**.
  3. Select the box for the new, untrusted certificate; then, click **Accept**. The chassis is now trusted (the compute nodes and network devices in the chassis are still not trusted).
  4. From the table view, select the box for the CMM with the regenerated certificate; then, click **Actions** > **Security** > **Verify Connection**.

     Note: The chassis transitions to a trusted state quickly; however, the chassis components might take several minutes to be trusted.

- **You change the certificate that is used by a managed resource to a certificate that is not signed by the CMM (for example, Verisign).**
- **The management software certificate policy is set to Explicit and a new chassis is discovered by the management software.** To add the new CMM certificate to the trust store and establish a connection to the CMM, complete the following steps:

  1. Manually add the certificate to the trust store. See "Certificate policies" in the *IBM Flex System Manager Systems Management Guide* PDF document for more information.
  2. From the table view, select the box for the new CMM.
  3. Click **Actions** > **Security** > **View Certificates**.
  4. Select the box for the new, untrusted certificate; then, click **Accept**. The chassis is now trusted (the compute nodes and network devices in the chassis are still not trusted).
  5. Revoke access for the new CMM; then, request access to the same CMM to establish trust for all of the managed endpoints in the chassis:

a. Select the box for the CMM; then, click **Actions** > **Security** > **Revoke Access**.
b. Make sure that the box for the CMM is selected; then, click **Actions** > **Security** > **Request Access**.

Note: The chassis transitions to a trusted state quickly; however, the chassis components might take several minutes to be trusted.

- **The endpoint for the management node is *Not trusted*.** If an IBM Flex System Manager management node is not managing the chassis in which it is installed, and the CMM in the chassis fails over, the access state of the management node endpoint might change to *Not trusted*. This is caused by a change to the IMM certificate on the management node.

  To add the changed certificate to the trust store, complete the following steps:

  1. From the table view, select the box for the management node endpoint.
  2. Click **Actions** > **Security** > **View Certificates**.
  3. Select the box for the untrusted certificate; then, click **Accept**. The management node is now trusted.

- **The endpoint for the management node is *Not trusted*.** If an IBM Flex System Manager management node is not managing the chassis in which it is installed, and you update the firmware or install a management software fix pack for that management node, the management node endpoint will have the access state *Not trusted* after the management node restarts. When the integrated management module (IMM) firmware is updated on the management node, the management node will not have the CMM CA certificate that is required to validate the new IMM certificate.

  1. Manually add the CMM CA certificate to the trust store. See .
  2. From the table view, select the box for the CMM with the regenerated certificate; then, click **Actions** > **Security** > **Verify Connection**.

     Note: The chassis changes to a trusted state quickly. However, the chassis components might take several minutes to be trusted.

No Access

The access state *No access* indicates that the management software has connectivity to the managed resource (and the managed resource might not be trusted). However, all of the RSAPs for the resource have no credentials, invalid credentials, or valid credentials with an expired password.

Notes:

- If the managed resource is a compute node in the chassis, the problem might be solved at the chassis level or through direct action to the compute node endpoint. If access to the managed chassis endpoint is unlocked, but access to a compute node endpoint in that chassis is locked, then access problems must be resolved by selecting and configuring access for that compute node.
- If the managed resource is a new compute node or storage node in a chassis that is in centralized user management mode, the problem might be node firmware that is not current. See “Centralized user management problems” on page 61 for more information.

1. Select the box for the resource with no access:
   - If the resource with no access is a chassis or compute node in a chassis with no access, select the box for the CMM.

- If the resource is a compute node with no access in a chassis that does have access, select the box for the compute node.
- If the resource with no access is another hardware component, and not a chassis or compute node, select the box for that resource.

2. Click **Actions** > **Security** > **Request Access**.

   Note: If the password has expired it is indicated in the status, and you must change the password before you request access to the resource. Click **Change Password** to update the password.
3. Click **Request Access**.

If a chassis that was previously managed in centralized user management mode has the access state *No access*, you might need to update the CMM LDAP configuration and import a new management node SSL certificate. This scenario is typical when the management node IP address is changed, but centralized user management mode for the chassis was not temporarily disabled.

If you change the IP address of the management node from the command-line interface or from the web interface, the LDAP SSL certificate is out-of-sync with the centrally-managed chassis, and you cannot access the CMM with IBM Flex System Manager credentials. To solve this problem, complete the following steps:

1. Open a CMM command-line interface session, and log in with the RECOVERY_ID account.

   Note: The password for the RECOVERY_ID account was set when you selected the chassis for management on the Management Domain page.
   If this is the first time that you have used the RECOVERY_ID account to log in to the CMM, you must change the password.
2. If you are prompted, type the new password for the RECOVERY_ID account.
3. Run the following command to identify the IP address of the management node: **ldapcfg -T mm[p]**

   In the output that is generated, note the IP address beside the `i1` parameter; this is the management node IP address in the CMM user registry configuration.

   Note: If the `i1` parameter shows the old management node IP address, run the following command to update the CMM configuration with the new management node IP address:

   ```
   ldapcfg -i1 <new_IP_address> -T mm[p]
   ```

   where *<new_IP_address>* is the new management node IP address.
4. Run the following command to import the management node certificate:

   ```
   sslcfg -tc1 import -u https://<IP_address>/FRMServerCert.der -T mm[p]
   ```

   where *<IP_address>* is the new management node IP address that you identified in the previous step.
5. For each chassis that you want to access, from the Chassis Manager page in the management software web interface, select the chassis; then click **Actions** > **Security** > **Request Access**. The Request Access page opens.
6. Click **OK**.

Partial Access

The access state *Partial access* indicates that the management software has connectivity to the managed resource. However, one or more (but not all) RSAPs have no credentials, invalid credentials, or valid credentials with an expired password.

Note: The following procedure will solve the partial access problem if the problem is caused by one or more of the RSAP credentials for the managed resource. However, there might be other reasons why the access is partial (for example, a firewall might be blocking one of the RSAPs).

1. Select the box for the resource; then, click **Actions** > **Security** > **Configure Access**.
2. Enter the valid credentials as needed.
3. Click **OK**.

If you complete the preceding procedure and the partial access problem remains, investigate and address each of the following conditions as needed:

- there is no physical connectivity
- firewall configuration for the network is preventing connectivity
- the managed resource is powered off and must be powered on
- the managed resource needs to be restarted

Backup and recovery problems

Use this information to solve problems with backup and recovery (or restore) in IBM Flex System Manager management software.

General backup and recovery problems

You cannot initiate a backup or restore of the management software image.

- You must have the proper privileges for your userid role (smadmin) to backup or restore the software. Request that your system administrator give you the authority to backup and restore.
- Only on backup or restore task can be run at a time. Make sure that no other users are backing up or restoring the software image before you start a backup or restore operation.

You cannot backup a sofware image to, or restore a backup image from, a USB device.

Make sure that a USB device is inserted in the management node. From a CLI prompt, you can use the **lsmediadev** command to see if a USB device is installed. See the *IBM Flex System Manager Systems Management Guide* document for more information about backing up or restoring software by using a USB device or a secure FTP server.

You cannot backup a software image to, or restore a backup image from, a secure FTP server (SFTP). A message is displayed.

Make sure that you have access to the remote SFTP server. See the *IBM Flex System Manager Systems Management Guide* document for more information about backing up or restoring software by using a USB device or a secure FTP server.

After you restored an management software image and collected inventory on the storage farm managed endpoint without errors, you experience storage fabric errors and the management software incorrectly displays multiple endpoints for

image repositories and virtual appliances.

To solve the problems, complete the following steps:

1. From the management software web interface, click the Chassis Manager tab and make sure that the chassis status is `Managed`.
2. Click **General Actions** > **Resource Explorer**; then, after the Resource Explorer page opens, click **All Systems**. Make sure that all of the discovered endpoints are displayed with an Access status of `OK` (and not the status `Not Trusted`).
3. Verify your network configuration from the SMIA Configuration Tool:
   a. From the Home page, click the **Applications** tab; then, make sure that the SMIA Configuration Tool is running.

      Note: If you have external versions of the SMIA Configuration Tool, make sure that those are also running and can be pinged from the management node.
   b. From the Applications tab, click **Launch administration console** and log in to the SMIA Configuration Tool.
   c. In the SMIA Configuration Tool, click the **CIMOM** tab and make sure that the CIMOM settings are correct.
   d. Click the **Home** tab; then, click the **Fabric Discovery** link. Make sure that all of the required network switches are discovered, with a green check mark that indicates proper SNMP trap communication.
4. Use the management software command-line interface (CLI) to check data sources, remove an Fabric Data Source object, rediscover the object, and ping the operating system endpoints that host image repositories:
   a. From the management software CLI, use the **`lsdatasource`** command to verify that all of the expected data sources are present, and an OID is listed for each network device.
   b. Use the **`rmdatasource`** to remove the Fabric Data Source object, as shown in the following example:

      ```
      smcli rmdatasource -c fabric -i <IPv6>
      ```

      where the *IPv6* is the address for Fabric Data Source 3.
   c. Use the **`mkdatasource`** to rediscover the Fabric Data Source object, as shown in the following example: `smcli mkdatasource -c fabric -t https <IPv6> -p 25989 -u USERID -w Passw0rd -n /interop`

      where *IPv6* is the address for Fabric Data Source 3, and `USERID` and `Passw0rd` are the management software administrator user name and password.
   d. Use the **`pingsys`** command to ping the each of the operating system endpoints that host image repositories.
5. Use the management software web interface to view operating-system endpoint access states and collect inventory:
   a. Open the Resource Explorer page.
   b. Click **All Systems**; then, make sure that all of the operating system endpoints that host image repositories are displayed with an Access status of `OK`.
   c. Select the operating system and farm endpoints from the Resource Explorer table; then, click **Actions** > **Inventory** > **Collect Inventory**.

6. After inventory has been collected, check the image repositories and virtual appliances in VMControl:
   a. From the VMControl summary page, click the **Virtual Appliances** tab.
   b. Under `Where to deploy:`, click the **<*number*> Image repositories** link, where <*number*> is the number of image repositories in your environment. The Image Repositories page opens.
   c. Select each image repository; then, click **Actions** > **Related Resources** > **Server**. Make sure that the server endpoint that hosts each image repository is displayed with an Access status of `OK`.
   d. With each image repository still selected, click **Actions** > **Related Resources** > **Server**. Make sure that the server endpoint that hosts each image repository is displayed with an Access status of `OK`.

      If you find that the server access for an image repository is OK, but the image container is missing, then an image repository endpoint remains, even though it was deleted after the management software backup was created. The errant image repository endpoint must be deleted manually.

      Attention: Make sure that you do not remove the image repository that still has one or more virtual appliances.
   e. Make sure that each virtual appliance is associated with its captured disk in the storage device.

      Note: You can verify the Captured SCS Virtual Appliances for the storage device from the management software web interface. For example, if your storage device is an IBM Flex System V7000 Storage Node, click **Launch IBM Flex System V7000**, log in to the V7000 Storage Node management GUI, and click **Volumes**. For other storage devices, go to the Plug-ins tab and click **Systems and Volumes** under Storage Management.
   f. From the Virtual Appliances tab, under `What to deploy:`, click the **<*number*> Virtual appliances** link, where <*number*> is the number of virtual appliances in your environment. The Virtual Appliances page opens.
   g. Select each virtual appliance; then, click **Actions** > **Related Resources** > **Software Image**.
   h. Compare the virtual appliance software images with the volumes listed for the storage device. Any virtual appliance that does not have an associated software image must be removed manually; the virtual appliance might have been deleted after the management software backup was created, but still exists in the management software database. After you remove the errant virtual appliance endpoint, the management software reflects the current state of your environment.

USB backup and restore error messages

Table 2. USB backup and recovery errors, and corrective actions

Error message	Corrective action
DNZFM2297E - Image to restore not found.	Make sure that the proper name is specified.

Table 2. USB backup and recovery errors, and corrective actions (continued)

Error message	Corrective action
DNZFN2299E - Not enough space on backup device	From a CLI prompt, use the command **backup -e** to determine the amount of space needed for a backup.
DNZFM2330E - Unable to mount USB device	Make sure that only one USB device is mounted.
DNZFM2331E - No USB device detected	From a CLI prompt, you can use the **lsmediadev** command to see if a USB device is installed.

SFTP backup and restore error messages

Table 3. SFTP backup and recovery errors, and corrective actions

Error message	Corrective action
DNZFN2296E - Restore image not found on SFTP Server	Make sure that the proper backup image name is specified, and that the SFTP server name and credentials are correct.
DNZFM2289E - Unable to backup image	Make sure that there is enough space on the SFTP server, and that the server name and credentials are correct.

Centralized user management problems

Use this information to solve problems with a chassis that is configured in the IBM Flex System Manager management software to use the central management node user registry.

Table 4. Centralized user management problems and corrective actions

Problem description	Corrective action
The IBM Flex System Manager management node fails, and you are not able to manage a chassis because it is configured for centralized user management.	If you want to restore account-management functions on the Chassis Management Module (CMM) until the management node is restored or replaced, complete the following steps: 1. Open a CMM command-line interface session, and log in with the RECOVERY_ID account. **Note:** The password for the RECOVERY_ID account was set when you selected the chassis for management on the Management Domain page.If this is the first time that you have used the RECOVERY_ID account to log in to the CMM, you must change the password. 2. When you are prompted, type the new password for the RECOVERY_ID account. 3. Run the following command: `fsmcm -off` This command disables centralized user account management from the IBM Flex System Manager management software, and allows you to use local CMM user accounts to authenticate to the CMM and any management processor that is installed in the chassis. After you run the command, the RECOVERY_ID account is removed from the CMM user registry. You can now authenticate to the CMM and other chassis components with local CMM credentials.
You cannot log in to the CMM with the RECOVERY_ID account.	The RECOVERY_ID account is only valid when a CMM is configured for centralized user management. If you cannot log in with the RECOVERY_ID account, the CMM must have centralized user management disabled. Use an account in the local CMM user registry to access the CMM and other components in the chassis.

Table 4. Centralized user management problems and corrective actions (continued)

Problem description	Corrective action

After you changed the IP address (in the management network settings) for a management node that is managing one or more chassis in centralized user management mode, all of the chassis that were previously accessed and managed by the IBM Flex System Manager are now inaccessible (you might see the value `No Access` in the chassis Status column in the web interface).
 	
If you change the IP address of the management node from the command-line interface or from the web interface, the LDAP SSL certificate is out-of-sync with the centrally-managed chassis, and you cannot access the CMM with IBM Flex System Manager credentials.
	1. Open a CMM command-line interface session, and log in with the RECOVERY_ID account.
	Note: The password for the RECOVERY_ID account was set when you selected the chassis for management on the Management Domain page.If this is the first time that you have used the RECOVERY_ID account to log in to the CMM, you must change the password.
	2. If you are prompted, type the new password for the RECOVERY_ID account.
	3. Run the following command to identify the IP address of the management node:
	`ldapcfg -T mm[p]`
	In the output that is generated, note the IP address beside the `i1` parameter; this is the management node IP address in the CMM user registry configuration.
	Note: If the `i1` parameter shows the old management node IP address, run the following command to update the CMM configuration with the new management node IP address:
	`ldapcfg -i1 <new_IP_address> -T mm[p]`
	
	where <*new_IP_address*> is the new management node IP address.
	4. Run the following command to import the management node certificate:
	`sslcfg -tc1 import -u https://<IP_address>/FRMServer`
	
	where <*IP_address*> is the new management node IP address that you identified in the previous step.
	5. For each chassis that you want to access, from the Chassis Manager page in the management software web interface, select the chassis; then click **Actions** > **Security** > **Request Access**. The Request Access page opens.
	6. Click **OK**.

Table 4. Centralized user management problems and corrective actions (continued)

Problem description	Corrective action
After you started managing a chassis in centralized user management mode, the default USERID management software user account became locked. This can occur when the management software user account is duplicated on the CMM, and the CMM is put in centralized user management mode.	You can use the *pe* user account to unlock any user account. To unlock the user account, complete the following steps: 1. From the management software command-line interface, log in with the user name pe and the pe account password. **Note:** When you completed the Management Server Setup wizard, the password for the pe account was automatically set to be the same as the password for the system-level user account (the default system-level user account is USERID). 2. Run the following command: `smcli unlockuser -u <user_name>` where *user_name* is the locked user name.
You added a new compute node or storage node to a chassis that is in centralized management mode, but the node has the access state *No access* in the IBM Flex System Manager management software and CMM Chassis Map views. You cannot access the node directly or through the request-access action in the management software.	The problem might be caused by a new compute node firmware is not at the latest level.To fix this problem, complete the following steps: 1. Change the user management mode of the chassis in which the new node is installed to decentralized user management. See "Changing the user management mode of a managed chassis" in the *IBM Flex System Manager Systems Management Guide* document (PDF). 2. Update the compute node firmware. See "Updating systems" in the *IBM Flex System Manager Systems Management Guide* document (PDF). 3. Change the user management mode of the chassis to centralized user management.

Certificate for a managed compute node is not trusted

If a compute node that is under management is displayed in the IBM Flex System Manager management software web interface with the trust state *Not Trusted*, and a certificate for that compute node is in the certificate trust store, you must accept the untrusted certificate for that compute node in the management software certificate trust store.

If a certificate is listed with any status other than *trusted*, communication is not permitted with the associated compute node. All certificates required by the access points on the associated compute node must exist in the certificate trust store as trusted certificates before communication is allowed.

You can use the following information to accept an untrusted certificate or import a certificate to the certificate trust store.

Note: A management software administrator can revoke a certificate, which prevents the associated compute node from communicating with the management software. Any resource that is using a certificate that is revoked will not be trusted.

Accepting a certificate

To accept a compute node certificate that is not trusted by the management software, complete the following steps in the management software web interface:

1. From the Chassis Manager page, click the chassis that contains the compute node with the certificate that is not trusted. The Chassis Map opens.
2. From the Chassis Map graphical view, click the chassis or managed system.
3. In the Details section (under the graphical representation of the chassis), click **Actions** > **Security** > **View Certificates**. The View Certificates page opens, and the certificates for the selected system are displayed.
4. To view the details for the certificate, select the box for the certificate; then, click **View Certificate**.
5. Click the **Certificate Trust Store** link on the View Certificates page. The Certificate Trust Store page opens.
6. If you believe the certificate in question is legitimate, select the box for the certificate and click **Accept**. The certificate is added to the trust store.

Importing a certificate

If you have the certificate for the compute node saved as a local file, you can import the certificate and add it to the trust store.

Note: The certificate must be valid to be added to the certificate trust store; if the certificate is expired, not yet valid, or has been corrupted, it will not be imported and added.

To import a certificate to the management software certificate trust store, complete the following steps in the management software web interface:

1. From the Chassis Manager page, click the chassis that contains the compute node with the certificate that is not trusted. The Chassis Map opens.
2. From the Chassis Map graphical view, click the chassis or managed system.
3. In the Details section (under the graphical representation of the chassis), click **Actions** > **Security** > **Certificate Trust Store**. The Certificate Trust Store page opens, and all of the certificates that are stored by the management software are displayed.
4. From the Certificate Trust Store page, click the **Import** button. A Certificate Import page is opened.
5. From the Certificate Import page, in the file name field, point to the certificate that was exported as a local file. Specify any **Display name** value that helps describe this certificate.
6. Click **OK**.

Certificate is issued for another website address

If your web browser displays an error message related to the security certificate, use this information solve the problem.

Problem

Your browser displays an error message similar to on of the following examples.

Note: The browser error messages might vary slightly from the following examples, depending on the version of the browser that you are using.

For Mozilla Firefox

In the window that is titled *This Connection is Untrusted*, the following message appears:

```
This certificate is only valid for domain_name.
```

For Microsoft Internet Explorer

In the window that is titled *There is a problem with this website's security certificate*, the following message appears:

```
The security certificate presented by this website was issued for a
 different website's address.
```

Explanation and resolution

Consider the following list of possible causes:

1. The certificate presented is a default certificate, and is not intended to contain the correct address.
2. The system that you are attempting to access can be accessed from more than one address, and you used an address that is not in the certificate. For example, the certificate contains only the hostname of the system, but you attempted to connect with the system IP address.
3. If you installed a certificate that contains a valid system address, and you attempt to connect to the system at the address given, then this error might indicate a security threat (for example, a *man-in-the-middle* attack). One possible solution might be to work with the appropriate staff at your organization to determine whether your network security has been compromised.

Chassis Manager Chassis Map problems

Use this information to solve problems with Chassis Manager Chassis Map in the IBM Flex System Manager management software web interface. The Chassis Map in the Chassis Manager provides a graphical view of a managed chassis that you can use to navigate and inspect hardware resources within the chassis.

Table 5. Chassis Manager problems and corrective actions

Problem description	Corrective action
The graphical hardware view is not displayed, or components in the chassis are not displayed. The table view is displayed in the Chassis Map instead of the graphical view.	• Make sure that you are using a supported web browser to use the management software web interface. See *IBM Flex System Manager Systems Management Guide* for more information about browsers that are supported by the management software. • Data retrieval from the management software failed. Close the Chassis Manager page and re-open it. • Restart the management node.

CMM access problems

Use one of these procedures to restore IBM Flex System Manager management software access to a managed Chassis Management Module (CMM) after the CMM account credentials are locked out and the CMM is not accessible.

When you manage a CMM with an IBM Flex System Manager management node, the CMM account credentials are stored in the management node user registry. If you change a CMM password directly, in the CMM web or command-line interface, the management software continues to attempt to access the CMM with the old password. Eventually, unsuccessful access attempts by the management node might cause the CMM account to become locked out.

You can use one of the following procedures to reset the CMM credentials and restore access from the management node to the CMM:

- Wait for the CMM lockout period to expire
- Use a secondary CMM account to unlock the primary CMM account
- Unmanage, reset, and re-manage the CMM

  Attention: When you unmanage a chassis, all of the chassis settings are deleted. You must reconfigure chassis and chassis-component settings after the chassis is re-managed. Use this method only if the previous two procedures do not solve the CMM lockout problem.

Wait for the CMM lockout period to expire

1. Revoke access to the CMM from the IBM Flex System Manager management software web interface:
   a. Log in to the management software web interface.
   b. From the Chassis Map view, right-click the chassis; then, click **Security** > **Revoke Access**.
   c. Click **OK** to confirm the revoke-access action.
2. Wait for the CMM lockout period to expire. By default, the lockout period is one hour. However, if you or another user changed the default setting, the lockout period might be shorter or longer than one hour. In a separate browser window, try to log into the CMM to check if the lockout period has expired.
3. After the lockout period expires, request access to the CMM from the IBM Flex System Manager management software web interface:
   a. From the Configure Access page, click **Request Access**.
   b. Enter the primary CMM user account credentials; then, click **Request Access**.

      Management node access to the CMM is restored.

Use a secondary CMM account to unlock the primary CMM account

This method requires a secondary, backup CMM user account with administrative permissions.

1. Log in to the IBM Flex System Manager management software web interface.
2. From the Chassis Map view, right-click the chassis; then, click **Security** > **Revoke Access**.
3. Click **OK** to confirm the revoke access action.
4. Log in to the CMM using the secondary, backup administrator user account that is not being used by the management node.

5. Click **Mgt Module Management** > **User Accounts**.
6. From the User Accounts page, select the primary user account that is currently locked out; then, click **Unlock**.
7. From the IBM Flex System Manager management software Configure Access page, click **Request Access**.
8. Enter the CMM account credentials; then, click **Request Access**.

   Management node access to the CMM is restored.

Unmanage, reset, and re-manage the CMM

Use this method only if the previous two procedures do not solve the CMM lockout problem.

Attention: When you unmanage a chassis, all of the chassis settings are deleted. You must reconfigure chassis and chassis-component settings after the chassis is re-managed.

1. Unmanage the chassis from the IBM Flex System Manager management software web interface:
   a. Log in to the IBM Flex System Manager management software.
   b. From the Home page, click the **Initial Setup** tab.
   c. Click **Select Chassis to be Managed**. The Management Domain page opens.
   d. Select the chassis with the locked-out CMM; then, click **Unmanage**. The Unmanage Chassis page opens.
   e. Click **Unmanage**. After the unmanage operation is complete, close the Unmanage Chassis page.
2. Reset and reconfigure the CMM from the CMM web interface:
   a. With a straightened paper clip or similar tool, press the reset button for 15 seconds to reset the CMM to manufacturing defaults. For more information about the button and its location, see the IBM Flex System Chassis Management Module User's Guide at http://publib.boulder.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.cmm.doc/dw1kt_cmm_ug_pdf.pdf.
   b. Connect an Ethernet cable from a laptop or workstation directly to the CMM.

      Note: This is necessary to avoid connecting to a different CMM on the same subnet with the default IP address.
   c. Open a browser on the laptop or workstation and navigate to the CMM default IP address: `https://192.168.70.100`.

      Note: You might have to reconfigure your local host to be able to reach the subnet.
   d. Log into the CMM with the default user name `USERID` and password `PASSW0RD`. You are required to change the password immediately.
   e. Configure the CMM with the same settings as before the reset.

      If you saved the CMM configuration before the CMM was locked, you can restore the settings. For more information, see the IBM Flex System Chassis Management Module User's Guide at http://publib.boulder.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.cmm.doc/dw1kt_cmm_ug_pdf.pdf. If you cannot restore the settings from a saved configuration, see the IBM Flex System Chassis Management Module User's

Guide at http://publib.boulder.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.cmm.doc/dw1kt_cmm_ug_pdf.pdf.

f. (Optional) Create a second administrative user account for use in future lockout situations.

3. Manage the CMM from the IBM Flex System Manager management software web interface:
   a. From the Home page, click the **Initial Setup** tab.
   b. Click **Select Chassis to be Managed**. The Management Domain page opens.
   c. Select the chassis that you reset; then, click **Manage**. The Manage Chassis page opens.
   d. Select the authentication and IPv6 configuration settings for the chassis.
   e. Click **Manage**.
   f. Enter the new user account credentials for the CMM; then, click **OK**.

      After the chassis-management operation is complete, management node access to the CMM is restored.

Common Agent problems

Use this information to solve performance problems related to common agent services (CAS) in the IBM Flex System Manager management software.

Table 6. Common Agent problems and corrective actions

Problem description	Corrective action

You experience either of the following problems:
• VIOS performance is sluggish after it is started.
• The following error is displayed after Common Agent (or CAS) is restarted:
`SEVERE: ALR0412E: The authorization property com.ibm.lwi.localhost was not found in /var/opt/tivoli/ep/conf/admin/adminAuth.properties`
	The reason for the problem might be that the Domain Name Server (DNS) that is configured to provide hostname resolution to VIOS is offline. The name resolution order in VIOS is set to bind the hosts by default, which causes CAS to timeout when trying to resolve the hostname from DNS before it gets the hostname from the local hosts file.
	
	To change the DNS hostname resolution and fix the problem, complete the following steps on the managed endpoint that has the error or poor performance:
	1. If CAS is running, stop CAS.
	2. Add the local host to the `\etc\hosts` directory on the managed compute node.
	a. Open the local hosts file on the compute node operating system.
	b. Add an entry in the hosts file for the local hostname and IP address. The entry might be similar to the following:
	`172.16.254.1  localhost`
	
	where `172.16.254.1` and `localhost` are the IP address and hostname of the local host.
	c. Save and close the hosts file.
	3. Change the host order in the `/etc/netsvc.conf` configuration file to `local,bind`:
	a. Open the `/etc/netsvc.conf` file on the compute node operating system.
	b. Add the following entry:
	`hosts=local,bind`
	c. Save and close the configuration file.
	4. Start CAS.

Discovery problems

Use this information to solve problems with resource discovery in the IBM Flex System Manager management software web interface. During initial setup, the management software automatically discovers chassis on the management network. You can manage the chassis after it is discovered.

Troubleshooting discovery problems with the management software user interface

Table 7. Discovery problems and corrective actions

Problem description	Corrective action
You selected a chassis and clicked **Manage** on the FSM Management Domain page, and the status type `Discovery Pending` is displayed for more than a few minutes.	• Check the Resource Explorer page for the resource. After a few minutes, the resource might be visible in Resource Explorer. Open the FSM Management Domain page again and click **Manage**. **Note:** The Resource Explorer link is in the navigation area, which is hidden by default in the management software web interface. To open the navigation area, click the arrow icon on the left side of the screen. • Discover the resource manually. Click **Inventory** > **System discovery**; then, enter the IP address for the resource.
You selected a resource and clicked **Manage** on the FSM Management Domain page, and the status type `Unlock Pending` is displayed for more than a few minutes.	• Try to request access to the resource from the Navigate Resources page. **Note:** The Navigate Resources link is in the navigation area, which is hidden by default in the management software web interface. To open the navigation area, click the arrow icon on the left side of the screen. • From the Resource Explorer page, delete the resource. Go back to the FSM Management Domain page, select the resource again, and click **Manage** again.
You deleted a resource from the Resource Explorer page, and the status type `Delete Pending` is displayed for more than a few minutes on the FSM Management Domain page.	The resource deletion process might take 15 minutes or more.
You attempted to lock access to a resource and the status type `Lock Pending` is displayed for more than a few minutes on the FSM Management Domain page.	From the Resource Explorer page, attempt to revoke access by selecting the resource and using the **Actions** menu.
You attempted to discover a Flex System CN4093 10Gb Converged Scalable Switch with its IPv6 address through either the web interface or with the **`mkdatasource`** command, but the management software cannot connect to the switch.	Use the IPv4 address for the switch to discover it.

Troubleshooting with discovery and resource-management CLI commands

The CLI commands in the following table might assist you in troubleshooting resource-discovery problems. See *IBM Flex System Manager Command Reference Guide* document for more information about using CLI commands.

Table 8. Discovery-related CLI commands

Command	Function
smcli lsChassis	Shows a list of all managed and unmanaged chassis
smcli lsFSM	Shows a list of all management nodes on the management network
smcli lssystem	Shows information about a specific chassis or compute node
smcli manageChassis	Manage a chassis
smcli unmanageChassis	Unmanage a chassis
smcli eventListener	Watch events that are generated during manage or unmanage command operations
smcli lsAutomanage	Check if auto-manage option is enabled **Note:** If enabled, the management software attempts to manage all chassis that it finds on the management network
smcli dmStatus	Check if the proper data management plug-in is started
smcli printDMData	Provides additional debug information
smcli collectsptfile	Collects support files from a specified system and copies them to the management node. See "collectsptfile" in the *IBM Flex System Manager Service and Support Manager* document for more information. **Note:** You can also collect support files through the Service and Support Manager web interface. See "Manually collect support files" in the *IBM Flex System Manager Service and Support Manager* document for more information.
smcli submitsptfile	Sends support files on the management node to the service provider. See "submitsptfile" in the *IBM Flex System Manager Service and Support Manager* document for more information.

Features on Demand problems

Use this information to solve problems with activating Features on Demand keys on Flex System Manager Types 7955, 8731, and 8734 management nodes and X-Architecture compute nodes in the IBM Flex System Manager management software web interface.

Table 9. Features on Demand problems and corrective actions

Problem description	Corrective action
You activated a Features on Demand key for the management node, but you can't access the feature associated with that key.	• Most Features on Demand keys require you to restart the management node after the key is installed. After you restart the management node, the feature should be available. • The key might have been installed on the Integrated management module II (IMM2) of the management node. From a CLI prompt, run the command **smcli registerAllFeatureKeys**; then, restart the management node. **Note:** Additionally, the command **smcli lsFeatureKey** shows which keys are installed on the management node. See the *IBM Flex System Manager Command Reference Guide* document for more information about CLI commands.
You are not able to activate Features on Demand keys on X-Architecture compute nodes through the Features on Demand page in the management software web interface.	You can only enable Features on Demand keys on compute nodes through the management software if the compute node is configured to boot a UEFI-compatible operating system. If the compute node was configured in the Setup Utility to boot in legacy mode, you cannot activate Features on Demand keys.

Handling Request Access failures

The management software uses an *agent manager* to communicate with Common Agent after it is installed on a managed system. The agent manager provides authentication and authorization services for installed common agents and the management software. It also maintains a registry of configuration information about Common Agent-managed systems. There are several actions you can take to investigate and resolve Request Access failures for a system that is managed by IBM Flex System Manager and has Common Agent installed.

Make sure that the system is not being managed by more than one agent manager

An IBM Flex System Manager managed resource can be managed by only one agent manager at a time. If the managed resource is an operating system and IBM Flex System Manager stops managing it, its agent is not unregistered from the agent manager. To manage the agent with IBM Flex System Manager, unregister the agent manually:

1. Optional: On the operating system endpoint, query the usma service detail information to determine the current agent manager. Issue the following command that is applicable for the managed compute node operating system.

   Note: To run the following command on a system with VIOS, you must first exit the restricted shell. To get out of the restricted shell, run the command **oem_setup_env** before you attempt to query the usma service detail information.

   AIX or Windows

   ```
   slp_query --type=* --address=<system_IP_address>
   ```

```
Linux

/opt/ibm/icc/bin/slptool -u 127.0.0.1 findattrs service:management-software.IBM:usma
```

2. On the operating system endpoint, issue the following command that is applicable for the managed compute node operating system:

```
AIX or Linux

/opt/ibm/director/agent/runtime/agent/toolkit/bin/configure.sh -unmanaged -force
Windows

<install_root>\agent\runtime\agent\toolkit\bin\configure.bat -unmanaged -force
```

3. Remove the operating system endpoint from the IBM Flex System Manager by using the IBM Flex System Manager management software.
4. Rediscover the operating system endpoint. For instructions see, Performing a system discovery.
5. Request access again.

Ensure you are using the correct userid or password

- When requesting access to a secured system from the IBM Flex System Manager Request Access page, you cannot enter a password longer than 45 characters. The Request Access task has a password length limit of 45 characters. Additional characters will be ignored. You cannot gain access to a Common Agent-managed system using a user credential that has a password greater than 45 characters in length. To correct this problem, shorten the password on the managed system to gain access.
- Check by manually logging into the managed system via ssh, telnet (tn) or mstsc.exe to confirm that the password is correct.

  Note: The default management software security policy (Secure) does not allow unencrypted communication protocols such as telnet.
- Many browsers will pre-fill the password field. Empty it and make sure it is the right password.

Check the firewall

Request Access requires a reliable connection between the IBM Flex System Manager and Common Agent. You will need a connection in both directions: agent to server and server to agent. Make sure you can ssh, telnet (tn) or mstsc.exe from either direction.

Note: The default management software security policy (Secure) does not allow unencrypted communication protocols such as telnet.

Example checks are below:

```
Agent side

  telnet AM_IP 9513, make sure the connection works

  AIX or Linux

    /opt/ibm/director/agent/runtime/agent/toolkit/bin/checkconn.sh -host AM_IP -password AM_password

  Windows

    <install_root>\agent\runtime\agent\toolkit\bin\checkconn.bat -host AM_IP -password AM_password

  For example, the checkconn command might display the following information:
    BTC8614I The connection to the agent manager has been established successfully.

Server side

  telnet Agent_IP 9510, make sure the connection works
```

Note: AM_IP is the IP address of the agent manager. AM_password is the register password for the agent manager.

Check the time difference

As a general rule, the time difference between Common Agent and IBM Flex System Manager - adjusted for time zone - should not be more than 1 hour. Please ensure that the system clocks on the systems that contain IBM Flex System Manager and Common Agent remain synchronized.

Check to see if the IBM Flex System Manager IP address has changed

If there is an IBM Flex System Manager IP address change, please restart the server before issuing a Request Access. A correct server IP address is a prerequisite for Request Access.

You can run the following commands to check the IP address.

Note: AM_IP is the IP address of the agent manager. AM_password is the register password for the agent manager.

```
wget -O AgentMgr.Info http://AM_IP:9513/AgentMgr/Info

AIX or Linux

  /opt/ibm/director/lwi/runtime/agentmanager/toolkit/bin/HealthCheck.sh -toolkitPassword AM_password

Windows

  <install_root>\lwi\runtime\agentmanager\toolkit\bin\HealthCheck.bat -toolkitPassword AM_password

For example, the HealthCheck command might display the following information:
  CTGEM2470I It is the agent manager instance ID: 375ec6e115283ddaab37ec3b80771062

  AGENT_CONFIG_SERVICE                    = https://127.0.0.1:9512/AgentMgr/AgentConfiguration
  CRL_REQUEST                             = http://127.0.0.1:9513/AgentMgr/CRLRequest
  MULTI_SCHEDULER_SYNCHRO_SERVICE         = https://127.0.0.1:9512/AgentMgr/MultiScheduleSynchronizer
  FILE_DOWNLOAD_SERVICE                   = http://127.0.0.1:9513/AgentMgr/Patches
  UPGRADE_SERVICE                         = https://127.0.0.1:9512/AgentMgr/UpgradeService
  REGISTRATION_SERVICE                    = https://127.0.0.1:9511/AgentMgr/Registration
  SERVICE_CATALOGUE_REQUEST               = http://127.0.0.1:9513/AgentMgr/ServiceCatalogueRequest
  AGENT_MANAGER_QUERY                     = http://127.0.0.1:9513/AgentMgr/AgentManagerQuery
  AGENT_QUERY                             = https://127.0.0.1:9512/AgentMgr/AgentQuery
  MIGRATION_SERVICE                       = https://127.0.0.1:9512/AgentMgr/MigrationService
  MANAGER_CREDENTIALS_SERVICE             = https://127.0.0.1:9512/AgentMgr/AuthAdmin
  TRUSTSTORE_REQUEST                      = http://127.0.0.1:9513/AgentMgr/TrustedCertificateQuery
  PATCH_SERVICE                           = https://127.0.0.1:9512/AgentMgr/PatchService
  COMMON_AGENT_QUERY                      = https://127.0.0.1:9512/AgentMgr/CommonAgentQuery
  CERT_REVOCATION_SERVICE                 = https://127.0.0.1:9512/AgentMgr/CertificateRevocation
  SCHEDULER_ADMIN_SERVICE                 = https://127.0.0.1:9512/AgentMgr/ScheduleManager
  DELETE_AGENTS_SERVICE                   = https://127.0.0.1:9512/AgentMgr/DeleteAgents
  SCHEDULER_SYNCHRO_SERVICE               = https://127.0.0.1:9512/AgentMgr/ScheduleSynchronizer
  VERSION_SERVICE                         = http://127.0.0.1:9513/AgentMgr/Version
  DEREGISTER_SERVICE                      = https://127.0.0.1:9512/AgentMgr/DeregistrationService
  CONFIG_UPDATE_SERVICE                   = https://127.0.0.1:9512/AgentMgr/ConfigurationUpdate
  CERT_RENEWAL_SERVICE                    = https://127.0.0.1:9512/AgentMgr/CertificateRenewal
  FILE_ADMIN_SERVICE                      = https://127.0.0.1:9512/AgentMgr/PatchAdmin
  INFO_PAGE                               = http://127.0.0.1:9513/AgentMgr/Info
  IPADDRESS_SERVICE                       = http://127.0.0.1:9513/AgentMgr/IPAddress
  JOB_MANAGER_SERVICE                     = https://127.0.0.1:9512/AgentMgr/JobManager

  CTGEM2450I The Health Check tool passed.
```

Note: AM_IP is the IP address of the agent manager. AM_password is the register password for the agent manager.

Check the Common Agent status

Request Access requires that the Common Agent is in good status. You can run the following queries to check agent status:

```
AIX or Linux

  /opt/ibm/director/agent/runtime/agent/bin/endpoint.sh status
  Running.
  /opt/ibm/director/agent/runtime/agent/bin/agentcli.sh connector alive
  BTC7101I The connector is active.

Windows
```

```
<install_root>\agent\runtime\agent\bin\endpoint.bat status
Running.
<install_root>\agent\runtime\agent\bin\agentcli.bat connector alive
BTC7101I The connector is active.
```

If the Common Agent status is not active, complete the following steps:

1. Issue the following command to check to make sure that the SLP is in an operational state:

   ```
   rcc-pok-idg-1992:~ # ps -ef|grep slp
   root     15198 15059  0 03:18 pts/0    00:00:00 grep slp
   daemon   21276     1  0 Apr23 ?        00:01:13 /opt/ibm/icc/bin/slpd
   root     23450     1  0 Apr23 ?        00:00:00 /opt/ibm/platform/bin/tier1slp
   ```

2. Make sure that the DNS is set correctly on the agent system. If no DNS is configured, check the host files in the following directories on the agent system:

   For Linux or AIX®: `/etc/hosts`
   For Windows: `C:\Windows\System32\drivers\etc\hosts`

   The following entry is available:

   ```
   - 127.0.0.1 localhost
   - ::1 localhost
   ```

   Note: `- ::1 localhost` only applies if there are IPv6 addresses.
   Every global IP address should be mapped to the hostname of the endpoint.

Check common agent services (CAS) status

Request Access requires that the CAS client is in good status.

Note: You must be logged in with the system admin user ID (USERID) and password to run the smcli commands in the following example.

Below is an example query for checking CAS status:

```
USERID@myfsm1:~> smcli getAgentManagers

****************************************
Agent manager id/name : 45C7862A505D34FC9F8D8C8D6D3850E5
Agent manager versoin : 1.4
Agent manager ip      : 10.10.6.60
Is this default?      : true
Agent Manager userid   : root
Agent Manager port     : 9511
Agent Manager ipaddress list: 10.10.6.60, fd55:faaf:e1ab:1b09:214:5eff:fe5a:3035, fe80:0:0:0:214:5eff:fe5a:3035,
Is this Embedded: true
****************************************

USERID@myfsm1:~> smcli queryAgents
Agent
--------------- AGENT [0dac826ed7d73d2883034c99a2286f72] ---------------
Agent directory = file:///opt/ibm/director/agent/runtime/agent;
...
Agent registration time: Wed Mar 14 03:33:54 EDT 2012
AgentOperationalStatus[0]:
AgentContactInfo[0]:
```

Configure the Common Agent for managed mode

Use the following command to configure the Common Agent for managed mode without Request Access. You can then run discovery, which will automatically unlock the operating system or IBM Flex System Manager resources.

AIX and Linux

```
/opt/ibm/director/agent/runtime/agent/toolkit/bin/configure.sh
-amhost active_agent_manager_IP_address -passwd active_agent_registration_password -force
```

Windows

```
install_root\agent\runtime\agent\toolkit\bin\configure.bat
-amhost active_agent_manager_IP_address -passwd active_agent_registration_password -force
```

Note: *active_agent_manager_IP_address* is the IP address of the agent manager. *active_agent_registration_password* is the register password for the agent manager.

Make sure the CA certificate of the CMM that is managing the endpoint is imported

Make sure that the CA certificate for the Chassis Management Module (CMM) that is managing the endpoint has been imported to the management software certificate trust store. To view the certificate trust store, click the arrow icon on the left side of the screen to open the navigation area (which is hidden by default); then, click **Security** > **Certificate Trust Store**.

If the Request Access action fails and the displayed state is Not Trusted, then the certificate that was presented by the endpoint is not trusted. To download the CA certificate and import it, complete the following steps:

1. From the CMM web interface, click **Mgt Module Management** > **Security** > **Certificate Authority** > **Download Certificate**.

   Note: You can also use the CMM CLI command **sslcfg** to download the certificate.
2. From the IBM Flex System Manager web interface, click the arrow icon on the left side of the screen to open the navigation area (which is hidden by default).
3. Click **Security** > **Certificate Trust Store**.
4. Click **Import...** and complete the fields to import the certificate.
5. Try the Request Access action again for the managed endpoint.

IBM Flex System Manager for mobile devices application problems

Use this information to identify the cause of an access state that is problematic (any access state other than *OK*), and configure access for the managed resource to correct the access state.

Connectivity problems

If your IBM Flex System Manager for mobile devices application cannot connect to the management node, see the following problem scenarios.

Table 10. IBM Flex System Manager for mobile devices connectivity problems – possible causes and corrective actions

Possible cause of connectivity problem	Corrective action
Airplane mode is enabled on the mobile device.	Disable Airplane mode.
The management node is configured to use a Virtual Private Network (VPN), and cannot be accessed from the IBM Flex System Manager for mobile devices application.	Make sure that you log on to the VPN before you use the IBM Flex System Manager for mobile devices application.
The management node is behind a firewall.	Use your mobile browser to authenticate to the firewall.

Table 10. IBM Flex System Manager for mobile devices connectivity problems – possible causes and corrective actions (continued)

Possible cause of connectivity problem	Corrective action
The management node can be reached on 443, the default port for HTTPS, but the data port that was configured for the management node is 8422.	Talk to your IT administrator about enabling port 8422 on the firewall.
The management node Secure Sockets Layer (SSL) certificate is not trusted by your mobile device.	Make sure that the management node and mobile device are configured to establish a trusted connection with SSL certificates. For more information, see the *IBM Flex System Manager Systems Management Guide* document.

Security problems

If you are unable to authenticate with the management node, the IBM Flex System Manager for mobile devices application might have saved an incorrect management software password or IP address. To resolve this type of problem, update the password or IP in the Connections settings for the management node in the Settings menu.

If you use the application to change the password to an existing management node connection, and the application cannot connect, or the application can still connect when it should not, you might have to clear the session information.

The application uses cookies to cache connection information for a management node after connecting to it. In order to clear the session information for the application, close the application and restart it. The new connection information will then be used.

Other problems

Table 11. Other IBM Flex System Manager for mobile devices problems and corrective actions

Problem description	Corrective action
The IBM Flex System Manager for mobile devices application generates the message *No object store found*.	The application might be corrupt. Delete the application from your mobile device and reinstall it.
The application is connected to a management node and some chassis information is displayed, but other application screens remain blank or the loading icon spins indefinitely.	Make sure that you have not lost your network connection. See the preceding "Connectivity Issues" section for more information.
The screen orientation of the IBM Flex System Manager for mobile devices application is horizontal, instead of vertical, on a BlackBerry Bold or Curve device that has BlackBerry OS version 7.0.	The application does not support BlackBerry OS version 7.0 or earlier. Update the device to BlackBerry OS version 7.1. See the BlackBerry Support Community at http://supportforums.blackberry.com for more information about how to update your BlackBerry operating system.

Image repository problems

Use this information if an image repository for AIX, IBM i, or Linux on IBM Flex System Power Systems™ was previously configured, but no longer appears on the IBM Flex System Manager.

Image repository problems and corrective actions

An image repository that was created previously does not appear on the IBM Flex System Manager.

To recover the image repository, collect inventory in the IBM Flex System Manager management software web interface for the following managed endpoints in the following order.

1. Storage array (for example, the Flex System V7000) managed endpoint
2. Storage Area Network (SAN) switch managed endpoint
3. Storage farm managed endpoint
4. Every compute node managed endpoint that hosts a VIOS logical partition (LPAR)
5. Every virtual server managed endpoint that represents a VIOS LPAR
6. Every operating system managed endpoint that represents a VIOS installation

If the image repository does not appear on the IBM Flex System Manager after you collect inventory for the preceding managed endpoints, you can use the **smcli dumpstcfg -v** command to investigate the problem.

To run the **smcli dumpstcfg** command, complete the following steps:

1. Open the management software command-line interface.
2. Log in with the `USERID` account credentials.
3. Enter command **smcli dumpstcfg -v**

Information about the SAN configuration is displayed.

After you restored an management software image and collected inventory on the storage farm managed endpoint without errors, you experience storage fabric errors and the management software incorrectly displays multiple endpoints for image repositories and virtual appliances.

To solve the problems, complete the following steps:

1. From the management software web interface, click the Chassis Manager tab and make sure that the chassis status is `Managed`.
2. Click **General Actions** > **Resource Explorer**; then, after the Resource Explorer page opens, click **All Systems**. Make sure that all of the discovered endpoints are displayed with an Access status of `OK` (and not the status `Not Trusted`).
3. Verify your network configuration from the SMIA Configuration Tool:
   a. From the Home page, click the **Applications** tab; then, make sure that the SMIA Configuration Tool is running.

      Note: If you have external versions of the SMIA Configuration Tool, make sure that those are also running and can be pinged from the management node.
   b. From the Applications tab, click **Launch administration console** and log in to the SMIA Configuration Tool.
   c. In the SMIA Configuration Tool, click the **CIMOM** tab and make sure that the CIMOM settings are correct.

d. Click the **Home** tab; then, click the **Fabric Discovery** link. Make sure that all of the required network switches are discovered, with a green check mark that indicates proper SNMP trap communication.

4. Use the management software command-line interface (CLI) to check data sources, remove an Fabric Data Source object, rediscover the object, and ping the operating system endpoints that host image repositories:
   a. From the management software CLI, use the **lsdatasource** command to verify that all of the expected data sources are present, and an OID is listed for each network device.
   b. Use the **rmdatasource** to remove the Fabric Data Source object, as shown in the following example:

      ```
      smcli rmdatasource -c fabric -i <IPv6>
      ```

      where the *IPv6* is the address for Fabric Data Source 3.
   c. Use the **mkdatasource** to rediscover the Fabric Data Source object, as shown in the following example:

      ```
      smcli mkdatasource -c fabric -t https <IPv6> -p 25989 -u USERID -w Passw0rd -n /interop
      ```

      where the *IPv6* is the address for Fabric Data Source 3, and `USERID` and `Passw0rd` are the management software administrator user name and password.
   d. Use the **pingsys** command to ping the each of the operating system endpoints that host image repositories.
5. Use the management software web interface to view operating-system endpoint access states and collect inventory:
   a. Open the Resource Explorer page.
   b. Click **All Systems**; then, make sure that all of the operating system endpoints that host image repositories are displayed with an Access status of `OK`.
   c. Select the operating system and farm endpoints from the Resource Explorer table; then, click **Actions** > **Inventory** > **Collect Inventory**.
6. After inventory has been collected, check the image repositories and virtual appliances in VMControl:
   a. From the VMControl summary page, click the **Virtual Appliances** tab.
   b. Under `Where to deploy:`, click the **<*number*> Image repositories** link, where <*number*> is the number of image repositories in your environment. The Image Repositories page opens.
   c. Select each image repository; then, click **Actions** > **Related Resources** > **Server**. Make sure that the server endpoint that hosts each image repository is displayed with an Access status of `OK`.
   d. With each image repository still selected, click **Actions** > **Related Resources** > **Server**. Make sure that the server endpoint that hosts each image repository is displayed with an Access status of `OK`.

      If you find that the server access for an image repository is OK, but the image container is missing, then an image repository endpoint remains, even though it was deleted after the management software backup was created. The errant image repository endpoint must be deleted manually.

Attention: Make sure that you do not remove the image repository that still has one or more virtual appliances.

e. Make sure that each virtual appliance is associated with its captured disk in the storage device.

   Note: You can verify the Captured SCS Virtual Appliances for the storage device from the management software web interface. For example, if your storage device is an IBM Flex System V7000 Storage Node, click **Launch IBM Flex System V7000**, log in to the V7000 Storage Node management GUI, and click **Volumes**. For other storage devices, go to the Plug-ins tab and click **Systems and Volumes** under Storage Management.

f. From the Virtual Appliances tab, under `What to deploy:`, click the **<*number*> Virtual appliances** link, where <*number*> is the number of virtual appliances in your environment. The Virtual Appliances page opens.

g. Select each virtual appliance; then, click **Actions** > **Related Resources** > **Software Image**.

h. Compare the virtual appliance software images with the volumes listed for the storage device. Any virtual appliance that does not have an associated software image must be removed manually; the virtual appliance might have been deleted after the management software backup was created, but still exists in the management software database. After you remove the errant virtual appliance endpoint, the management software reflects the current state of your environment.

Inventory problems with the Flex System PCIe Expansion Node

If a PCIe expansion node is connected to an X-Architecture compute node that is managed by the management software, but you cannot view the PCIe expansion node details on the Inventory page of the management software, make sure that the compute node operating system is supported.

To view the PCIe expansion node details in the management software web interface, you must use the management software to discover and collect inventory for the attached compute node before you discover the compute node operating system.

If the connected X-Architecture compute node is running a Linux, Windows, or VMware ESXi operating system, you can view information about the PCIe expansion node on the Inventory page for the connected compute node after the compute node is discovered and inventory is collected.

However, if the compute node has an unsupported operating system installed, you cannot view the PCIe expansion node.

For more information about the PCIe expansion node, see https://www-01.ibm.com/common/ssi/rep_ca/9/897/ENUS112-139/ENUS112-139.PDF.

Inventory problems with the Flex System Storage Expansion Node

If a Storage expansion node is connected to an X-Architecture compute node that is managed by the management software, but you cannot view the Storage expansion node details on the Inventory page of the management software, make sure that the compute node operating system is supported.

To view the Storage expansion node details in the management software web interface, you must use the management software to discover and collect inventory for the attached compute node before you discover the compute node operating system.

If the connected X-Architecture compute node is running a Linux, Windows, or VMware ESXi operating system, you can view information about the Storage expansion node on the Inventory page for the connected compute node after the compute node is discovered and inventory is collected.

However, if the compute node has an unsupported operating system installed, you cannot view the Storage expansion node.

For more information about the Storage expansion node and supported operating systems, see the *Flex System Storage Expansion Node Installation and Service Guide*.

Login problems

Use this information to solve problems related to logging in to the IBM Flex System Manager management software web interface.

Login problems

When you attempt to log into the management software using the IBM Flex System Manager management software web interface, the following error message is displayed:

```
Login failed. Check the user ID and password and try again.
```

This problem can occur when logging into the management server either locally or remotely.

Investigation

Before resolving this problem, review the following considerations:

- Make sure that the password is correct and that the Caps Lock and Number Lock keys are not on.

  From the management software command-line interface (CLI), you can use the following command to reset a user's password:

  ```
  smcli resetuserpwd -u <user_name> -p <temporary_password>
  ```

  The user must change the password at the next login attempt; see "Logging in with a temporary password after a password reset" on page 83.
- If you created the password in the CLI and the password contains special characters, you might have to reset the password.

  Important: If you use any of the following characters in a password that you create in the command-line interface, you must add \ (backslash) in front of each special character: `@`, `$`, `#`, `!`, `&`, `(`, `)`, `|`, `<`, `>`, `"`, `'`. If you do not use the backslash

with each of these characters, an error occurs or an unexpected password value is stored in the management software. The following characters can cause conflicts with other components in the system and should not be used: ", |, <, >, and any whitespace character such as *space* or *tab*.

- Make sure the password does not require updating, and has not expired in the user registry.

  From the management software CLI, you can use the following command to determine if the user's password is expired:

  ```
  smcli pwdexpired -u <user_name>
  ```

- Make sure the user is not locked or disabled in the user registry.

  Note: If a user fails to log in 20 or more times, the user is locked out.

  From the management software CLI, you can use the following command to determine if the user's account is locked:

  ```
  smcli userlocked -u <user_name>
  ```

- A reset password must be changed, either through the web interface or a CLI command, the first time the user attempts to login.

Resolution

If you failed to log in 20 or more times, open a management software command-line interface prompt and type the following command to unlock your user name:

```
smcli unlockuser -u <user_name>
```

where *user_name* is the locked user name.

Note:

1. You must have a user account with SMAdministrator or SMManager permissions to use this command.
2. You can use the *pe* user account to unlock user accounts. When you completed the Management Server Setup wizard, the password for the pe account was automatically set to be the same as the password for the system-level user account (the default system-level user account is USERID).

Note: If the password for the USERID account is expired, the pe account does not have the authority to reset the USERID password. If this occurs, contact IBM support to obtain a temporary password that will allow you to use **su** to temporarily become the root user, which will allow you to reset this password.

Logging in with a temporary password after a password reset

Use this information to log in with a temporary password in the IBM Flex System Manager management software web interface or command-line interface (CLI).

When an administrator resets a user password in the management software web interface or CLI, the user is assigned a temporary password by the administrator.

The following procedures describe the procedure that the user must follow to log in with the temporary password and enter a new password.

Logging into the web interface after a password reset

After the administrator who reset your password provides you with your temporary password, complete the following steps:

1. Log in to the web interface with your user ID and temporary password. The Log in page refreshes.
2. In the **Old Password** field, type the temporary password.
3. In the **New Password** field, enter a new password.
4. In the **Confirm New Password** field, enter the new password again.
5. Click **Log in**.

   The Log in page refreshes, and you can log in with your user ID and new password.

Logging into the CLI after a password reset

After the administrator who reset your password provides you with your temporary password, complete the following steps:

1. Log in to the CLI with your user ID and temporary password.
2. When you are prompted, `You are required to change your LDAP password immediately. Enter login(LDAP) password:`, enter the temporary password.

   Note: If you do not enter the temporary password immediately, your account is locked out of the management software.
3. When you are prompted, `Enter login(LDAP) password:`, enter the temporary password again.
4. When you are prompted, `New LDAP password:`, enter a new password.
5. When you are prompted, `Retype new LDAP password:`, enter the new password again.

   The following message is displayed:

   `LDAP password information changed for` *`user_ID`*

   where *user_ID* is your user name.

Remote Control problems

IBM Flex System Manager management software Remote Control problems and troubleshooting information are described in the Remote Control documentation.

See the *IBM Flex System Manager Systems Management Guide* for Remote Control troubleshooting information.

Security policy problems

Use this information to solve security policy problems with IBM Flex System Manager management software. The management software security policy defines security-related constraints that apply to IBM Flex System hardware. The default security policy level that is enforced by the management software is *Secure*.

Determining the security policy level that is being used by the management software

To determine the active security policy level, complete the following steps:

1. From the Home page in the management software web interface, click the **Administration** tab.
2. Under Security tasks, click **Configure Security Policy**. The Configure Security Policy page opens, and the current security policy level is displayed.

For more information about security policies, see the *IBM Flex System Manager Systems Management Guide* for more information about security policies.

Setup Wizard problems

Use this information to solve IBM Flex System Manager management software problems that you encounter in the Setup Wizard and the network validation that occurs after the Setup Wizard is complete.

Troubleshooting problems with the Setup Wizard

Table 12. Management software Setup Wizard problems and corrective actions

Problem description	Corrective action
The web browser that you used to start the Setup Wizard was closed accidentally before you completed the Setup Wizard.	Re-open the browser and go to this address: `https://<IP or Hostname>:8722/SWPortlet /SWPortlet/portletwindow` where *<IP or Hostname>* is the IP address or hostname of the management node.
You completed the Setup Wizard, but the web browser was closed accidentally while the Server status page (which allows you to monitor the server status) was displayed.	Re-open the browser and go to one of the following: • The hostname that you defined in the Setup Wizard • The IP address of the management node. • The address `https://<IP or Hostname>:8422/ibm/console`, where *<IP or Hostname>* is the IP address or hostname of the management node.
The Setup Wizard does not finish successfully.	Run the **`smcli collectsptfile`** command (and use the command options to specify the target system) to gather support files and copy them to the management node. Then, run the **`smcli submitsptfile`** command to send support files to IBM Support. See "collectsptfile" and "submitsptfile" in the *IBM Flex System Manager Service and Support Manager* document for more information.

Troubleshooting failed network validation after the Setup Wizard is complete

If you check the **Perform network validation and recovery when the setup wizard is complete** box on the LAN Adapters page of the Setup Wizard, and the configuration settings you entered in the Setup Wizard generates errors, the management node is reset and the Setup Wizard restarts.

Table 13. Network validation problems in the Setup Wizard and corrective actions

Problem description	Corrective action
Network validation fails and you are redirected to the first page of the Setup Wizard.	Complete the following steps: 1. Click **Next** until you reach the LAN Adapters page. An error message is displayed that shows the invalid settings. **Note:** If you believe the settings are correct, clear the **Perform network validation and recovery when the setup wizard is complete** box, and complete the Setup Wizard. If the box is cleared, the Setup Wizard ignores network validation errors. 2. Change the values for the invalid settings and complete the Setup Wizard.

Update problems

Use this information to solve problems with updating the management node or managed resources through the IBM Flex System Manager management software.

Troubleshooting managed resource updates

Table 14. Updating managed resources

Problem	Action
You cannot update firmware on an X-Architecture compute node.	The LAN over USB interface might be disabled on the compute node. To check if the interface is enabled, and to enable the LAN over USB interface if necessary, complete the following steps: 1. Log in to the Chassis Management Module (CMM) web interface (see Starting the web interface for more information). 2. From the CMM web interface home page, click **Chassis Management** > **Compute Nodes**. 3. Click the compute node name. 4. Click the **General** tab. 5. Select **Enable Ethernet Over USB** to enable the LAN over USB interface. 6. Try to update the compute node firmware again. **Note:** After you update the firmware, you can disable the LAN over USB interface again.

Table 14. Updating managed resources (continued)

Problem	Action
You cannot update IBM Power Systems compute node device drivers in the operating system that is running on the compute node.	DNS server configuration is required on the data network (Eth1) to update the device drivers in the operating systems that are running on IBM Power Systems compute nodes. To configure a DNS server for the management software, complete the following steps: 1. From the Home page, click the **Administration** tab. 2. Under Configuration tasks, click **Configure Network**. 3. From the LAN adapter page, select the data network (Eth1) and click **Next**. 4. Select the settings for your management node on the Host and Gateway and Advanced Routing pages, and click **Next**. 5. On the DNS page, select the DNS server settings and click **Finish**.

Troubleshooting IBM Flex System Manager management software updates

Table 15. Updating the management software to version 1.2.0

Problem	Action
You are not able to update the IBM Flex System Manager management software to version 1.2.0 with Update Manager.	If Update Manager fails to acquire the version 1.2.0 updates, run the following CLI command before you import the updates with the management software CLI: `smcli cleanupd -mva` **Note:** 1. After you run the preceding command, compliance policies indicate that all systems are in compliance because there are no longer any updates in the library. After you upgrade the management software to version 1.2.0, you must acquire updates for your compliance policies before the management software will show needed updates. 2. See cleanupd command for more information about the command.

User registry problems

Use this information to solve user registry problems in IBM Flex System Manager management software.

Determining the type of user registry that is being used by the management software

The most common user registry problems are related to one of the following categories:

- Logging in to the management software
- Accessing the management software or managed resources
- Managing user accounts, user groups, or roles

To determine the type of user registry that is being used by the management software, complete the following steps:

1. From the Home page in the management software web interface, click the **Plug-ins** tab.
2. Click **IBM Flex System Manager**. The management software summary page opens.
3. Click **IBM Flex System Manager Status**; then, check the user registry that is displayed to determine whether the correct registry is in use. If the registry location shows the IP address of the management node, the IBM Flex System Manager user registry is in use. Otherwise, an external user registry is in use.

Troubleshooting the IBM Flex System Manager user registry

Complete the following steps:

1. Verify that the management node is active.
2. The watchdog process restarts OpenLDAP if the process ends.
3. Log in and verify that the expected permissions are available.

Troubleshooting an external user registry

To investigate the problem with your external user registry, you might take the following actions:

- Verify that the external user registry server is active and accessible.
- Check for possible network problems.
- Check for possible security problems (for example, firewalls, certificates, and registry access).
- Contact IBM Support.

If you cannot log in to the management software because your external user registry is not available, you can log in with the default administrator account and use the management software web interface to change the user registry setting to the local IBM Flex System Manager user registry.

Management software recovery and reinstallation

If a hard drive fails, or if the management software is configured incorrectly or becomes corrupted, you might need to reinstall all or part of the management software on the management node.

The IBM Flex System Manager management node comes with three drives: one hard disk drive and two solid state drives. Each of the management node drives comes pre-configured with components of the IBM Flex System Manager management software. The hard disk drive contains the following:

- The recovery partition, which is used to install the management software
- The spare virtual disk images, which are used to perform upgrades
- Storage space for backup images

The solid state drives are mirrored (RAID 1), and contain the following:

- The management software virtual machine
- The host operating system

A fully functional management node requires that all three hard drives, and the software components on each one, be operational. If the hard disk drive fails, or if both solid state drives fail, you must reconfigure the RAID boot settings through the LSI Corp Configuration Utility before you can reinstall the management software.

If a hard drive fails, or if the management software is configured incorrectly or becomes corrupted, you might need to reinstall all or part of the management software on the management node. The type of reinstallation that is required depends on the type of management node or management software problem.

Before you reinstall all or part of the management software, determine whether the hard drives and other management node hardware components are functional. Then, determine which of the following procedures is necessary for your management node. For more information about troubleshooting hard drives, see the Flex System Manager Types 7955, 8731, and 8734 Installation and Service Guide at http://publib.boulder.ibm.com/infocenter/flexsys/information/topic/com.ibm.acc.8731.doc/printable_doc.html.

Reinstalling the management software from the recovery partition

Use this recovery method if the management software is inoperable because of misconfiguration or corruption, but the management node hardware is operational and the hard drives have not failed.

About this task

This procedure returns the management node and management software to factory defaults, and destroys data on the system (but not backups stored on the hard disk drive). After the recovery process is complete, you must configure the system with the Management Server Setup wizard or restore the system from a backup image.

Procedure

1. Restart the management node.
2. When the firmware splash screen is displayed, press F12. The setup menu is displayed. The screen displays confirmation that F12 has been pressed.
3. Select **Recovery partition**.
4. When the boot options screen is displayed, select **Full system recovery**. After approximately 30 to 45 minutes, the recovery process ends and the Management Server Setup wizard opens.

   Note: The system displays Loading Bootloader, but no additional messages are displayed during the recovery process. If the screen saver is activated and the screen goes blank during this stage, press the Shift key to deactivate the screen saver.

5. Either complete the Management Server Setup wizard or restore a previous configuration from a backup.

What to do next

Important: If your recovery partition is an earlier version of the management software than the version before the recovery procedure, update the management software to the same version as before the recovery operation after you complete the Management Server Setup wizard. If you do not update the management software in this situation, the management software is older than other components in your environment, which might cause compatibility problems.

For more information about setting up the management node with the wizard, see the configuration section in the *IBM Flex System Manager Systems Management Guide*.

For more information about restoring a backup image, see the backup and restore section in the *IBM Flex System Manager Systems Management Guide*.

Reinstalling management software components from optical media after replacing the hard disk drive

If the management node fails and only the hard disk drive has been replaced (and not a solid state drive), use the following information to recover the IBM Flex System Manager management software image.

About this task

Note: If a management node solid state drive has also failed and been replaced, use the procedure that is described in "Reinstalling the management software from optical media after replacing an SSD" on page 92.

If the Flex System Manager Types 7955, 8731, and 8734 hardware fails, a solid state drive, the hard disk drive, or both might have to be replaced, and the management software might have to be recovered from the IBM Flex System Manager management software Recovery DVDs.

If the hard disk drive has failed but the solid state drives have not, the management software image might still be operational. The recovery process boots the management node from the Recovery DVDs.

To complete the management software recovery process, you need the following items:

- Flex System Manager Types 7955, 8731, and 8734 console breakout cable
- External DVD-ROM drive with a USB connection and an external power adapter

  Note: Some DVD-ROM drives (and most USB-powered DVD-ROM drives) might not be compatible.
- USB cable
- IBM Flex System Manager management software Recovery DVDs (from IBM Support)

  Note: Before you request the Recovery DVDs from IBM Support, see "Obtaining the IBM Flex System Manager Recovery DVDs" on page 94 to determine the FRU part number for your version of the management software.

For more information about removing and replacing hard disk drives, see the relevant topics in the *Flex System Manager Types 7955, 8731, and 8734 Installation and Service Guide* document.

Important: The RAID reconfiguration that is described in step 1 is necessary only if you have replaced a failed hard disk drive or both of the SSDs. If only one SSD has failed and been replaced, the RAID is restored automatically.

Procedure

1. During the restart of the management node (after the splash screen), start the LSI Corp Configuration Utility and reconfigure the RAID settings:
   a. When the following message is displayed on your screen, press Ctrl+C.

      ```
      Please wait, initializing legacy usb devices...Done

      LSI Corporation MPT SAS2 BIOS
      MPT2BIOS-7.19.00.00 (2011.05.16)
      Copyright 2000-2011 LSI Corporation.

      Press Ctrl-C to start LSI Corp Configuration Utility...
      ```

   b. Select the adapter and press Enter.
   c. Select **SAS Topology** and press Enter.
   d. Expand **Direct Attach Devices** so that the hard disk is displayed.
   e. Make sure that the hard disk is set as the alternate boot device, or `Alt`, and that the RAID is set to `Boot`. If `Alt` and `Boot` are not displayed, use the following key combinations to modify the configuration:
      - **Alt+B**: Select or deselect a device as the preferred boot device.
      - **Alt+A**: Select or deselect a device as the alternate boot device.

   f. Press Escape; then, select **Save changes then exit this menu** and press Enter.
   g. Press Escape; then, select **Exit the Configuration Utility and Reboot** and press Enter. The management node restarts.
2. Use the Recovery DVDs to reinstall the management software partitions:
   a. Install the console breakout cable in the front of the management node.
   b. Connect the external optical media drive to the console breakout cable.
   c. Insert the Recovery DVD 1 in the external optical drive.
   d. Power® on the management node.
   e. From the splash screen, press F12 to select the Recovery DVD for the next node boot. After the management node boots, the Recovery menu is displayed.
3. Use the Recovery menu to destroy the corrupted partitions and reinstall the management software image:
   a. After the management node boots, select **Recover the management node**; then, press Y.
   b. From the menu, select the third option in the list: **Recover HDD (use if the HDD failed, but neither SSD failed)** for management software version 1.2.1 or later,or **Reinstall HDD image only** for versions 1.2.0 and earlier. After you make the selection, press Y. The node begins copying data from the Recovery DVD 1.
   c. When you are prompted, remove the Recovery DVD 1 and insert the Recovery DVD 2 in the external optical drive.

Note: After you insert Recovery DVD 2, wait approximately one minute before you press Enter. If you press Enter and the DVD is ejected, reinsert the DVD and wait two minutes before you press Enter again.

Depending on the version of IBM Flex System Manager management software you are recovering, you might have more than 2 DVDs to insert. If so, continue with this step for each of the DVDs.

d. To complete the process of recovering the IBM Flex System Manager management software, you must import the ISO files again. For more information about importing ISO files, see Importing operating system images.

4. After the recovery process is complete, disconnect the external optical drive and restart the management node.

   Note: After all of the DVDs have been copied, you might receive an "unknown error." If that occurs, press **Enter**. Then, select **Exit** and allow the system to restart.

Reinstalling the management software from optical media after replacing an SSD

Use this recovery method if your management node experienced hardware failures that required you to replace a solid state drive (SSD) or an SSD and the hard disk drive.

Before you begin

Before you perform the following management software reinstallation procedure, make sure that you have replaced the failed SSD (and hard disk drive, if applicable) and returned the management node to its default configuration.

For more information about removing and replacing solid state drives and hard disk drives, see the relevant topics in the *Flex System Manager Types 7955, 8731, and 8734 Installation and Service Guide* document.

To complete the management software recovery process, you need the following items:

- Flex System Manager Types 7955, 8731, and 8734 console breakout cable
- External DVD-ROM drive with a USB connection and an external power adapter

  Note: Some DVD-ROM drives (and most USB-powered DVD-ROM drives) might not be compatible.
- USB cable
- IBM Flex System Manager management software Recovery DVDs (from IBM Support)

  Note: Before you request the Recovery DVDs from IBM Support, see “Obtaining the IBM Flex System Manager Recovery DVDs” on page 94 to determine the FRU part number for your version of the management software.

About this task

This procedure returns the management node and management software to factory defaults, and destroys all of your data on the management node. Therefore, you must complete the initial setup again after the recovery is complete.

Note: If the hot-swap SAS drive has failed, but the solid state drives have not, the IBM Flex System Manager management software image might still be operational.

Important: The RAID reconfiguration that is described in step 1 is necessary only if you have replaced a failed hard disk drive or both of the SSDs. If only one SSD has failed and been replaced, the RAID is restored automatically.

Procedure

1. If you replaced only one SSD, skip to step 2. If you replaced both SSDs, a hard disk drive, or all three, you must reconfigure the RAID. During the restart of the management node (after the splash screen), start the LSI Corp Configuration Utility and reconfigure the RAID settings:
   a. When the following message is displayed on your screen, press Ctrl+C.

      ```
      Please wait, initializing legacy usb devices...Done

      LSI Corporation MPT SAS2 BIOS
      MPT2BIOS-7.19.00.00 (2011.05.16)
      Copyright 2000-2011 LSI Corporation.

      Press Ctrl-C to start LSI Corp Configuration Utility...
      ```

   b. Select the adapter and press Enter.
   c. Select **SAS Topology** and press Enter.
   d. Expand **Direct Attach Devices** so that the hard disk is displayed.
   e. Make sure that the hard disk is set as the alternate boot device, or `Alt`, and that the RAID is set to `Boot`. If `Alt` and `Boot` are not displayed, use the following key combinations to modify the configuration:
      - **Alt+B**: Select or deselect a device as the preferred boot device.
      - **Alt+A**: Select or deselect a device as the alternate boot device.

   f. Press Escape; then, select **Save changes then exit this menu** and press Enter.
   g. Press Escape; then, select **Exit the Configuration Utility and Reboot** and press Enter. The management node restarts.
2. Install the console breakout cable in the front of the management node.
3. Connect the external optical media drive to the console breakout cable.
4. Insert Recovery DVD 1 in the external DVD drive; then, start the management node.
5. After the management node boots, select **Recover the management node**; then, press Y.
6. From the menu, select the second option in the list: **Recover complete system (use if both SSDs failed, or to update a down-level recovery partition)** for management software version 1.2.1 or later,or **Destroy and remake all partitions** for versions 1.2.0 and earlier. After you make the selection, press Y.
7. When you are prompted, select **Yes** to confirm that you want to reinstall the management software.

   Attention: After you confirm that you want to proceed with the reinstallation, all of your data on the management node will be destroyed.
8. When you are prompted, remove the Recovery DVD 1 and insert the Recovery DVD 2 in the external optical drive.

   Note: After you insert Recovery DVD 2, wait approximately one minute before you press Enter. If you press Enter and the DVD is ejected, reinsert the DVD and wait two minutes before you press Enter again.

Depending on the version of IBM Flex System Manager management software you are recovering, you might have more than 2 DVDs to insert. If so, continue with this step for each of the DVDs.

9. When you are prompted, disconnect the external DVD drive.

   Note: After all of the DVDs have been copied, you might receive an "unknown error." If that occurs, press **Enter**. Then, select **Exit** and allow the system to restart.

10. The management node reboots. When the firmware splash screen is displayed, press F12. The setup menu is displayed. The screen displays confirmation that F12 has been pressed.
11. Select **Full system recovery**. After approximately 30 to 45 minutes, the recovery process ends and the Management Server Setup wizard opens.

    Note: The system displays Loading Bootloader, but no additional messages are displayed during the recovery process. If the screen saver is activated and the screen goes blank during this stage, press the Shift key to deactivate the screen saver.

12. Either complete the Management Server Setup wizard or restore a previous configuration from a backup.

    Note: To restore from backup, you must have previously saved the backup on either a USB drive or secure FTP server.

What to do next

For more information about setting up the management node with the wizard, see the configuration section in the *IBM Flex System Manager Systems Management Guide*.

For more information about restoring a backup image, see the backup and restore section in the *IBM Flex System Manager Systems Management Guide*.

Obtaining the IBM Flex System Manager Recovery DVDs

Before you contact IBM Support, use this information to determine the part number of the IBM Flex System Manager Recovery DVD package for your management software version.

About this task

The following table shows the Recovery DVD package part number for each IBM Flex System Manager management software version.

To order the Recovery DVDs, provide the applicable part number for your management software version to IBM Support. You can also contact IBM Support for information on where and how to obtain the Recovery DVD image by download.

Note: For more information about determining the installed version number, see “Determining the installed IBM Flex System Manager version” in the *IBM Flex System Manager Systems Management Guide* (PDF).

Table 16. IBM Flex System Manager Recovery DVDs

FSM version number	Recovery DVD package part number
1.3.4	01CV500
1.3.3	00WA653
1.3.2	00FH545
1.3.1	00FH622
1.3.0	No longer available
1.2.1	No longer available
1.2.0	No longer available
1.1.1	No longer available
1.1.0	No longer available

Appendix. Getting help and technical assistance

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

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

Before you call

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

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

- Check for updated 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.

  You can obtain the latest downloads for your IBM product from http://www.ibm.com/support/fixcentral/systemx/groupView?query.productGroup=ibm%2FBladeCenter .
- 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.
- Use the troubleshooting information in your system documentation, and use the diagnostic tools that come with your IBM product. Information about diagnostic tools is in the *Problem Determination and Service Guide* on the IBM *Documentation* CD that comes with your 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 service. This data will help IBM service 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 (or BIOS) and firmware levels
  - Other pertinent information such as error messages and logs
- Go to http://www.ibm.com/support/electronic/portal/ 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 service quickly and efficiently. IBM service technicians can start working on your solution as soon as you have completed and submitted an Electronic Service Request.

Using the documentation

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

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

You can find the most up-to-date information for BladeCenter products at http://publib.boulder.ibm.com/infocenter/bladectr/documentation/index.jsp .

Getting help and information from the World Wide Web

Put your short description here; used for first paragraph and abstract.

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

You can find the most up-to-date product information for BladeCenter products at http://publib.boulder.ibm.com/infocenter/bladectr/documentation/index.jsp .

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://publib.boulder.ibm.com/infocenter/bladectr/documentation/index.jsp .

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

Hardware service and support

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

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

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

IBM Taiwan product service

Use this information to contact IBM Taiwan product service.

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

IBM Taiwan product service contact information:

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

Notices

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

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

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

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

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

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

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

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

Trademarks

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

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

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

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

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

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

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

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

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

Important notes

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

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

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

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

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

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

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

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

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

Particulate contamination

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

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

Table 17. 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 52.21. • 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 71.04-19853 • Silver: Corrosion rate of less than 300 Å in 30 days
1 ASHRAE 52.2-2008 - Method of Testing General Ventilation Air-Cleaning Devices for Removal Efficiency by Particle Size. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc. 2 The deliquescent relative humidity of particulate contamination is the relative humidity at which the dust absorbs enough water to become wet and promote ionic conduction. 3 ANSI/ISA-71.04-1985. Environmental conditions for process measurement and control systems: Airborne contaminants. Instrument Society of America, Research Triangle Park, North Carolina, U.S.A.	

Documentation format

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

Information Development
IBM Corporation

205/A015
3039 E. Cornwallis Road
P.O. Box 12195
Research Triangle Park, North Carolina 27709-2195
U.S.A.

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

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

Telecommunication regulatory statement

This product is not intended to be connected directly or indirectly by any means whatsoever to interfaces of public telecommunications networks, nor is it intended to be used in a public services network.

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 Technical Regulations, Department M456
IBM-Allee 1, 71137 Ehningen, Germany
Telephone: +49 7032 15-2937
Email: tjahn@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
Technical Regulations, Department M456
IBM-Allee 1, 71137 Ehningen, Germany
Telephone: +49 7032 15-2937
Email: tjahn@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

이 기기는 업무용(A급)으로 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.

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

Part Number: 00FH233

Printed in USA

(1P) P/N: 00FH233