IBM System Storage™

Data Center Fabric Manager v10.4.2 Release Notes

CONTENTS

Overview

IBM Data Center Fabric Manager (DCFM) v10.4 is a feature release, which focuses on three areas: 1) support for new hardware, 2) feature enhancements across multiple platforms and 3) integrated SMI and partner integration. DCFM 10.4 includes support for the new FC8-64 High Density Blade, which will enable server and fabric consolidation. DCFM 10.4 simplifies management of this higher density of ports and management of key data center solutions including security, virtualization, and converged IP/SAN networks. DCFM v10.4 includes integration with IBM and other products, providing end users with seamless, standards-based storage management solutions. Below is a summary of the main feature enhancements of the DCFM v10.4 release:

New Hardware Platforms

- FC8-64 High Density Blade
- Brocade Mezzanine HBA 804 and CNA 1007

New Software Features

- Management Plug-In for VMware vCenter 4.0
  - Plug-in is invoked from vSphere client on selection of a tab, displaying the following information from DCFM:
    - VM Connectivity Information
    - Statistics Information
    - Event Information
  - Integrated SMI Agent
    a. Provides the ability to manage both Fabric Operating System (FOS) and M-EOS hardware
    b. Integrated into DCFM; includes SMI-only installation option
  - Partner Integration
    - IBM Systems Director
    - EMC Ionix SRM7
  - FCoE
    - Support for SAN06B-R in Access Gateway mode

Enhancements to existing features

- **Fibre Channel over IP enhancements (FCIP)**
  - Support for IPSec for the IBM Converged Switch B32 and the FX8-24 extension blade
  - Support for IPv6 on 1G and 10G ports
  - VEX support on 1G and 10G ports
  - Support for VLAN tagging from Fabric Operation System (FOS) v6.3.1
  - Additional Enhancements
    - Disable Min/Max bandwidth text fields for unsupported platforms
    - Suggest button display appropriate message when selected for unsupported platforms
    - Refresh the information in DCFM immediately upon successful FCIP configuration
- **FCoE and CEE Management**
  - Support for Startup, Running configurations
    - Save configuration to repository saves both running and startup configurations
    - Copy running to startup configuration within the switch
    - Restore to startup configuration (and reboot option)
    - Replicate to startup configuration
- **Virtualization**
  - Support for vSphere 4.0 (ESX 4.0 hypervisors) for monitoring
  - Virtual Machine (VM) icon change in the device tree and topology

- Port icon & Host enclosure used for source/destination columns in the End-to-End monitor and Top Talkers dialog
- VM Path discovery for File System of type VMFS (Virtual Machine File System)

- **Encryption Enhancements**
  - Support for disk-based device decommissioning for RKM and LKM key vault
  - Support for hosting disk & tape containers on same encryption engine
  - Support for EMC Symmetrix Remote Data Facility (SRDF)
  - Support for Access Gateway mode on Brocade Encryption Switch for Cisco Interoperability
  - Usability enhancements
    - Disk LUN View
    - Edit Smart Card dialog
    - Blade Processor Link Configuration
    - Display Blade Processor Link Status
    - Dynamic view update on Encryption Center and LUN Dialog
    - Provide commit state on target container
    - Show all rekey sessions for LUN on view
    - Export Certificate support
    - NCKA Key Vault renamed to TEMS
- **HBA / CNA Management**
  - Addition of 13 measures of performance statistics have been added for CNA (JSON), such as Rx % utilization, Received Paused Frames, Received Alignment Error Frames, etc.
  - Updates to Property Sheets, including Remote Port (e.g. Speed, Bind Type, Target ID, Vendor, etc.), add NWWN property in HBA port properties.

Additional Enhancements

- "Accept changes" summary dialog
- Event policies dialog is enhanced to pass event parameters to script in Launch script action
- Call Home changes
  - Removed EMC Email and HP Modem call home centers
  - HP LAN port number is customizable
  - SMTP over SSL is introduced for Email based call home centers
  - Support added for IBM and Brocade International call home centers to configure Time out and retry values
- Export option in the port mapping dialogs
- Overall security enhancements to application
- Support for authenticated SMTP over SSL
- Display of SNMP/ Syslog/ Internal FTP port status display
- Ability to export the topology as an image
- Incremental support for Traffic Isolation Zoning
- Limited support for Admin Domains
  - Physical Fabric (AD 255 context) Discovery
  - Asset & Fabric (Nameserver, Topology) information collected in Physical Fabric context
  - Defined and Active Zone configuration is collected in AD 0 context
  - Switch Configuration, Firmware Management, Performance Monitoring, Basic Switch Configuration operations (switch enable/disable, port enable/disable)
- Implemented main end user Requests For Enhancements (RFEs)
  - Switch SS folder name change as <Switch name>-<Switch IP>-<Switch WWN>
  - Copying switch/host support saves to another ftp server through view repository dialog
  - Port group reordering
  - Server/client memory restriction in options dialog
  - ASM bit changes for PDCM
  - List zone member's enhancement
  - Offline zone db activations
  - Filter ICL ports in zoning dialog
  - Zone member rendering in zoning dialog

- Delete button in VF dialog
- Inheriting the fabric properties
- Port unbind
- Unassigned port address
- Addressing mode changes in VF dialog

- Support for new FOS features
  - Enhanced TI zones support
  - Exchange based routing for lossless DLS
  - FX8-24 Extension Blade support in VF dialog

Operating Systems Supported

DCFM 10.3.3 is supported on the following operating systems.

Table 1 Server / Client Operating System Support

Operating System	Versions
Windows	Windows Server 2003 Std SP2 (x86 32-bit) Windows 2008 Std (x86 32-bit) Windows XP Pro SP3 (x86 32-bit) Windows Vista Business Edition SP1 (x86 32-bit) Windows 7 Professional Edition
Linux	RedHat AS 4.0 (x86 32-bit) RedHat Enterprise Linux 5 Adv (x86 32-bit) SUSE Linux Enterprise Server 10 SP1 (x86 32-bit)
VMWare	VMWare ESX 3.5 with Guest VMs of: Windows Server 2003 Std SP2 (x86 32-bit) RedHat Enterprise Linux 5 Adv (x86 32-bit) SUSE Linux Enterprise Server 10 SP1 (x86 32-bit) Windows XP Pro SP3 (x86 32-bit) Windows Vista Business Edition SP1(x86 32-bit) Windows 2008 Std (x86 32-bit) RedHat AS 4.0 (x86 32-bit) VMware ESX 4.0 with Guest VMs of: Windows Server 2003 Std SP2 (x86 32-bit) Red Hat Enterprise Linux 5 Adv (x86 32-bit) SUSE Linux Enterprise Server 10 SP1 (x86 32-bit) Windows XP Pro SP3 (x86 32-bit) Windows Vista Business Edition SP1(x86 32-bit) Windows 2008 Std (x86 32-bit) Windows 7 Professional edition RedHat AS 4.0 (x86 32-bit)

Switch Platform and Firmware Requirements

The following table lists the versions of Brocade software supported in this release. IBM and Brocade recommend using the latest software versions to get the greatest benefit from the SAN. IBM and equivalent Brocade hardware products are listed.

Operating System	IBM Switch/Director	Brocade Switch/Director
Switch (b-type and B-Model) Firmware Versions		
FOS 5.0.x, 5.1.x, 5.2.x, 5.3.x, 6.0.x, 6.1.x, 6.2.x, 6.3.x, and 6.4.x	SAN Switch F32 (2109-F32)	Brocade 3900
	SAN Switch H08 (2005-H08)	Brocade 3250
	SAN Switch H16 (2005-H16)	Brocade 3850
	SAN32B-2 (2005-B32, -32B)	Brocade 4100
	SAN04B-R (2005-R04)[1]	Brocade 7500E[1]
	SAN18B-R (2005-R18)[1]	Brocade 7500[1]
	SAN16B-2 (2005-B16, -16B)	Brocade 200E
	SAN64B-2 (2005-B64)[2]	Brocade 4900[2]
	SAN32B-3 (2005-B5K, -5KB)[3]	Brocade 5000[3]
	SAN24B-4 Express (2498-B24, -24E)[5]	Brocade 300[5]
	SAN40B-4 (2498-B40, -40E)[5]	Brocade 5100[5]
	SAN80B-4 (2498-B80)[5]	Brocade 5300[5]
	IBM Converged Switch B32 (3758-B32)[10]	Brocade 7800[10]
	SAN06B-R (2498-R06)[9]	Brocade 8000[9]
	VA-40FC[11]	VA-40FC[11]
	SAN Switch M12 (2109-M12)	Brocade 12000
	SAN Switch M14 (2109-M14)	Brocade 24000
	SAN256B (2109-M48) with FC4-16, FC4-32 and FC4-48 blades[2]	Brocade 4800 with FC4-16, FC4-32 and FC4-48 blades[2]
	SAN256B (2109-M48) with FR4-18i blades[1]	Brocade 4800 with FR4-18i blades[1]
	SAN256B (2109-M48) with FC4-16IP blades[2]	Brocade 4800 with FC4-16IP blades[2]
	SAN256B (2109-M48) with FC10-6 blade[4]	Brocade 4800 with FC10-6 blades[4]
	SAN768B (2499-384) with FC8-16, FC8-32, and FC8-48 blades[6]	Brocade DCX with FC8-16, FC8-32, and FC8-48 blades[6]
	SAN768B (2499-384) with FC8-64 blades[11]	Brocade DCX with FC8-64 blades[11]
	SAN768B (2499-384) with FR4-18i blades[6]	Brocade DCX with FR4-18i blades[6]
	SAN768B (2499-384) with FC10-6 blades[6]	Brocade DCX with FC10-6 blades[6]
	SAN768B (2499-384) with FX8-24 blades[10]	Brocade DCX with FX8-24 blades[10]
	SAN768B (2499-384) with FCoE10-24 blades[10]	Brocade DCX with FCoE10-24 blades[10]
	SAN384B (2499-192) with FC8-16, FC8-32, and FC8-48 blades[8]	Brocade DCX-4S with FC8-16, FC8-32, and FC8-48 blades[8]
	SAN384B (2499-192) with FC8-64 blades[11]	Brocade DCX-4S with FC8-64 blades[11]
	SAN384B (2499-192) with FR4-18i blades[8]	Brocade DCX-4S with FR4-18i blades[8]
	SAN384B (2499-192) with FC10-6 blades[8]	Brocade DCX-4S with FC10-6 blades[8]
	SAN384B (2499-192) with FX8-24 blades[10]	Brocade DCX-4S with FX8-24 blades[10]
	SAN384B (2499-192) with FCoE10-24 blades[10]	Brocade DCX-4S with FCoE10-24 blades[10]

[1] Requires FOS v5.1.0 or higher
[2] Requires FOS v5.2.0 or higher
[3] Requires FOS v5.2.1 or higher
[4] Requires FOS v5.3.0 or higher
[5] Requires FOS v6.1.0 or higher
[6] Requires FOS v6.0.0 or higher
[7] Requires FOS v6.1.1_enc or higher
[8] Requires FOS v6.2.0 or higher
[9] Requires FOS v6.1.2_CEE or 6.3
[10] Requires FOS v6.3.0 or higher
[11] Requires FOS 6.4.0 or higher

Operating System	IBM Switch/Director	Brocade Switch/Director
Switch (m-type, M-Model) Firmware Versions		
M-EOSc 9.6.x, 9.7.x, 9.8.x, and 9.9.x	SAN12M-1 (2026-E12, -12E) SAN16M-2 (2026-416, -16E) SAN24M-1 (2026-224) SAN32M-1 (2027-232) SAN32M-2 (2027-432, -32E) SAN140M (2027-140)	Spheron 4300 Spheron 4400 Brocade M4500 Spheron 3232 Brocade M4700 Brocade M6140
M-EOSn 9.6.x, 9.7.x, 9.8.x, and 9.9.x	SAN256M (2027-256)	Brocade Mi10K

Installing DCFM

Refer to the *IBM System Storage Data Center Fabric Manager Installation Guide* for complete installation instructions. The installation instructions below provide a brief overview for the following operating systems:

- Microsoft Windows
- Solaris
- Linux

The DCFM Server runs as multiple services on Windows and multiple processes on Solaris and Linux; and they start automatically after installation.

Migrating From a Previous Version

DCFM 10.4 supports a seamless upgrade path from previous versions of DCFM (10.1.x and 10.3.x). EFCM 9.6.x/9.7.x and FM 5.4 / 5.5 users must upgrade to DCFM Enterprise v10.1.1 or higher before upgrading to DCFM Enterprise v10.4.

To install DCFM Enterprise on Windows (Server)

1. Download and extract the zip archive
2. Navigate to the **Windows** folder
3. Execute *install.exe*
4. Follow the instructions to complete the installation.

To install DCFM Enterprise on Linux (Server)

1. Download and extract the tar.gz archive
2. Navigate to the **Linux** folder.
3. Execute *Install.bin* from the File Manager window.
4. Follow the instructions to complete the installation.

To install DCFM Enterprise on Solaris (Server)

1. Download and extract the tar.gz archive
2. Navigate to the **Solaris** folder.
3. Execute *Install.bin*.

4. Follow the instructions to complete the installation.

To launch the DCFM Client

- DCFM Professional Client
  - Launch DCFM as follows:
    Windows & Linux: Double-click on the DCFM Client shortcut on the desktop
    Solaris: Open a command prompt and launch the *dcfm* shell script; i.e.: */opt/DCFM_Pro_10_4_2/bin/dcfm*
- DCFM Enterprise Client
  - To launch the DCFM Enterprise Client on the same local machine as the DCFM Server, launch the client as follows:
    Windows: Select **Start > Programs > DCFM 10.4.2 > DCFM 10.4.2**
    Linux & Solaris: Follow the below steps on launching the client from a web browser.
  - To launch the DCFM Enterprise Client from a remote host, launch the client as follows:
    Open a browser window and type the DCFM server hostname or IP address in the **Address** field; for example:
    http://DCFMserverhost1.companyname.com/
    http://192.x.y.z/
  - If when the DCFM server was installed, a DCFM web server port number was specified (instead of the default 80), you must specify the port number after the hostname or IP address. In the following examples, 8080 is the web server port number:
    http://DCFMserverhost1.companyname.com:8080/
    http://192.x.y.z:8080/

Installation Notes

- If you are upgrading from the professional or enterprise trial versions of DCFM, refer to the *DCFM Migration Guide* for step-by-step procedures.
- Ensure the network environment does not have any firewall installations between the client and the server and the switches. If one exists, ensure that proper rules are set up to allow access. See the *DCFM Administrator's Guide* for additional information.
- You must choose the SAN size during the installation of DCFM v10.4.1. See the *DCFM Administrator's Guide* for additional information.
- If you install DCFM Server on a Windows host that has anti-virus software, you must disable the anti-virus software during the installation**.**
- Install DCFM Server on a dedicated machine that is not running any other server applications, such as another database server.
- DCFM is supported under Windows, RedHat Linux, and SUSE Server guest operating systems that run under VMware ESX 3.5 and 4.0. Refer to the *Operating Systems Supported* table. Other virtualization software is not supported.
- Modem-based Call Home is not supported under Windows guest operating system that runs under VMware ESX 3.5.
- DCFM v10.4.2 is tested under English, Japanese, German, and is supported under other non-English Windows operating systems. Most of the displayed text is in English, even though message strings and dates may display in the local language
- DCFM 10.4.2 cannot run on the same host as EFCM, FM or older versions of DCFM, when actively monitoring fabrics.

Management application server running in Windows 2008:

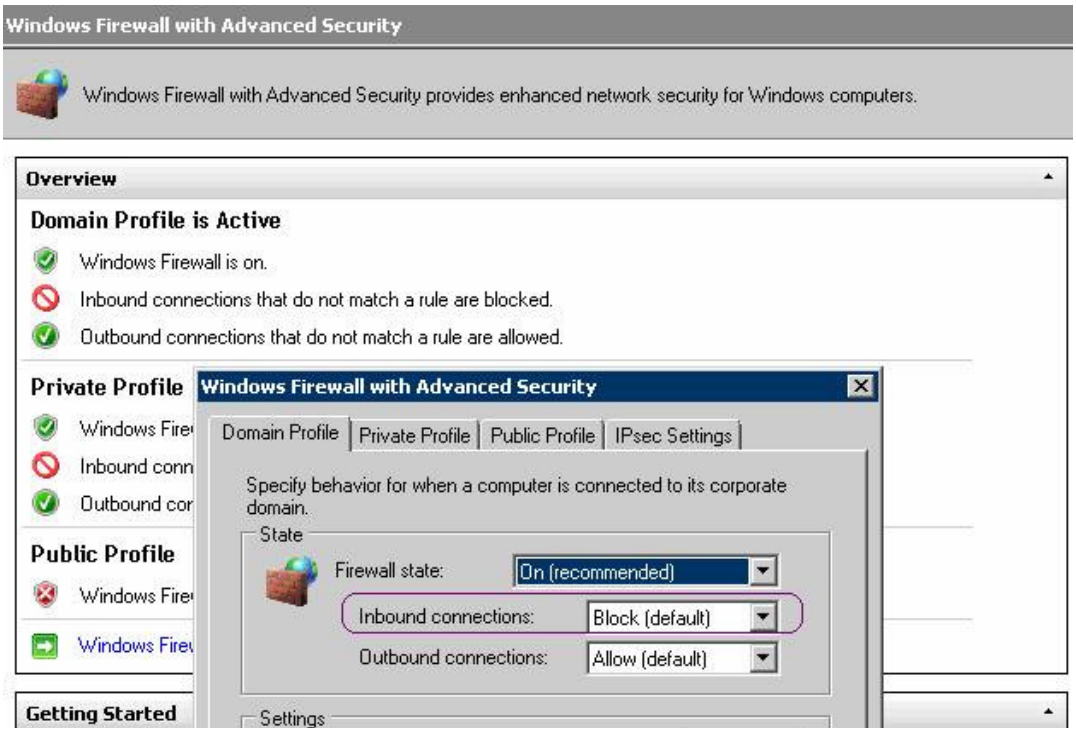
By default, when the Firewall is in "On" state in Windows 2008, it blocks all inbound connections to the host. You must select **Allow** in the **inbound connections** drop down list to allow clients from other hosts to access the Management application server.

To change this setting, complete the following steps.

1. Select **Start > Administrative Tools > Server Manager**.
2. Click **Continue** in the **User Account Control** dialog box.
3. Under **Security Summary**, click **Go to Windows Firewall**.
4. Click **Windows Firewall Properties**. The **Windows Firewall with Advanced Security** dialog box displays.
5. In the **Windows Firewall with Advanced Security** dialog box, based on the Active Profile[1], select **Allow** from the **Inbound Connections** list.

   [1]**Note:** Windows Firewall with Advanced Security supports separate profiles (sets of firewall and connection security rules) for when computers are members of a domain, or connected to a private or public network.
6. Click **OK** to save the changes.

Once the "Allow" option is selected in the **Inbound Connections** drop down list, the user can launch the client to the server running in 2008 host. In the screen capture below, the Domain profile is Active.



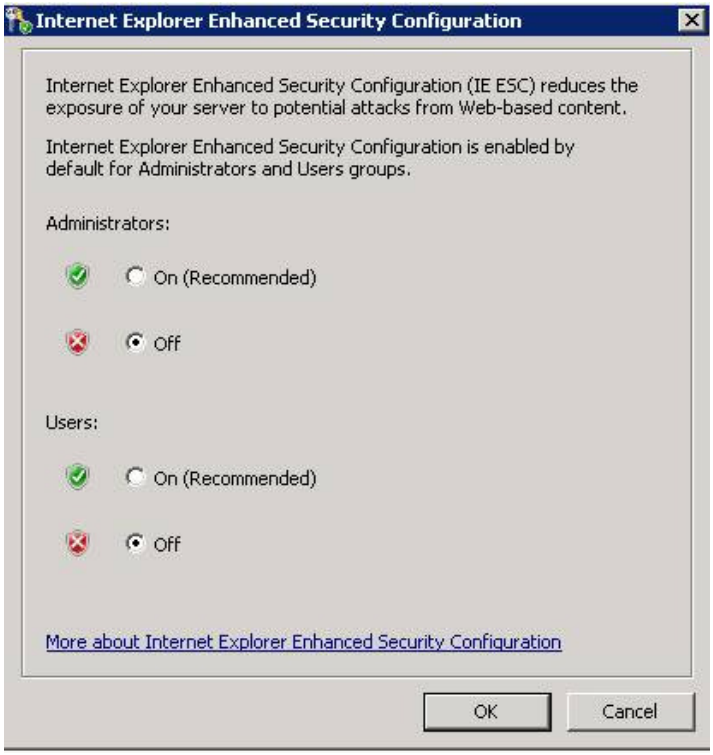
For more information on Windows Firewall with Advanced Security, refer to http://technet.microsoft.com/en-us/library/cc748991(WS.10).aspx

To launch client from Windows 2008 host to Management application server:

By default, Internet Explorer Enhanced Security Configuration (IE ESC) is enabled in Windows 2008. When you try to launch the client from the 2008 host to another host in which the Management application server is running, the following warning message displays. Click **Add** to add the site (Server IP) on which the Management application server is running, to download the client.

If you do not want to see the warning message again, disable the IE ESE by completing the following steps.

1. Close all instances of Internet Explorer.
2. Select **Start > Administrative Tools > Server Manager**.
3. Click **Continue** in the **User Account Control** dialog box.
4. Under **Security Summary**, click **Configure IE ESC**.
5. Under **Administrators**, select the **Off** option.
6. Under **Users**, select the **Off** option.
7. Click **OK**.


Internet Explorer Enhanced Security Configuration
Internet Explorer Enhanced Security Configuration (IE ESC) reduces the exposure of your server to potential attacks from Web-based content.
Internet Explorer Enhanced Security Configuration is enabled by default for Administrators and Users groups.
Administrators:
On (Recommended)
Off
Users:
On (Recommended)
Off
More about Internet Explorer Enhanced Security Configuration
OK
Cancel

Important Notes

This section lists information that you should consider before you use DCFM v10.4.2. See the *DCFM User Manual* for full details on the following notes. See the *DCFM Installation Guide* for installation procedures. See the *DCFM Migration Guide* for migration procedures.

M-EOSc switches with SNMPv3 enabled cannot be managed through DCFM. SNMPv3 needs to be disabled.

If SNMPv3 is enabled on M-EOSc switches, SNMPv1 is automatically disabled. SNMPv3 and SNMPv1 cannot be enabled simultaneously. Since DCFM 10.4.x uses only SNMPv1 to manage the M-EOSc switches, the manageability link will not be established if SNMPv3 is enabled. It is recommended to disable SNMPv3 using the CLI.

Upgrade switches running FOS v5.2.1_NI to v6.0.0 or higher

To completely manage a fabric in DCFM, where the seed switch is running FOS v52.1_NI, it is recommended to upgrade the switch to FOS v6.0.0 or higher. Failure to do so will limit the ability to manage fabric services such as Zoning. However, monitoring features such as Status, Events, and Performance Monitoring should not be affected.

Creating tape pool in a mixed FOS version environment

If FOS versions 6.2.0 and 6.1.1_enc_X (where X is any released version) are deployed in an environment the user should not configure any Tape Pool information. If Tape Pool information is configured and a failover occurs where the 6.1.1_enc_X node becomes the group leader, the user will not be able to remove the created tape pool.

Event priority mismatch

Error-level policies can sometimes be triggered by warning-level events.

Config Download fails when all parameters are selected

When Configdownload is attempted from one virtual switch to another virtual switch and when all parameters are selected where the Fabric IDs are not identical, download will fail.

Switch name update delay

When changing the name of a switch from outside of DCFM the new name for the switch will not be reflected within DCFM for up to 15 minutes, depending on SAN Size selection.

Event-based file actions fail

DCFM event-actions will fail to run scripts on remote-mounted file systems under Windows.

EX-Port disabled when configuring Routing Domain IDs

In the Routing Domain IDs dialog, if a user adds the appropriate Domain IDs to the front and xlate domains, clicking **OK** will disable the Ex_ports with the message “EX_PORT ISOLATE”.

Removing switches

If you plan to segment and remove multiple switches (more than 2) from a fabric and you have historical performance collection enabled, it is recommended that you ‘accept changes’ after each switch segmentation from the client rather than performing it at one time.

DCFM Clients

As a best practice it is recommended that the clients that are not being used actively should be shut down. This will free up the server resources. In some scenarios, if **duplicate** entries are seen in the 'Product List', restart the client.

Secure FOS fabrics cannot be discovered from DCFM

DCFM doesn't support Secure FOS (SFOS). If user tries to discover the fabric, DCFM will show an error message that "Discovery Failed". The user will need to remove the secure FOS settings and then change it back to normal fabric before discovering it from DCFM.

Encryption config has limited support and slow to register change for LUN provisioning

The current commit limitation of 25 is for the total transactions which includes add, update, and remove LUNs. To work around this, commit the transaction first, before making further changes.

IFL connection shown in topology after deleting all the VE-VEX tunnels present between the SAN06B-R switches

After deleting all the VE-VEX tunnels present between the SAN06B-R switches, sometimes the IFL connection is still shown in topology. It is recommended to select **Unmonitor** and then select **Monitor** the switch again. Defect: 259685

F ports connected to Access Gateway are not shown as attached ports under the switch

If Access Gateway is connected to a switch, F_ports connected to access gateway are not shown as attached virtual ports under the switch. It is recommended to launch a new client. Defect: 253462

Connection between AG and switch are not shown when F_port trunking is enabled on the AG

If switch is configured with F_port trunking and the AG is connected to the switch, the F_port trunk group icon is not shown in the product tree and the connection between the switch and AG is also not shown in the topology. It is recommended to disable F_port trunking on the switch. Defect: 253201

DCFM Users who use SysLog Host Configuration for events

HCM Agent needs to be restarted if firewall settings on port # 514 changed in VMware. VMware (Esx 3.5 & 4) blocks the Syslog outgoing port 514 by default. You need to configure the firewall to allow outgoing port 514 for Syslog if you plan to use Syslog Host configuration or use HCM as part of DCFM. Use the command '*esxcfg-firewall -o 514, udp, out, syslog'* to open the port 514 and use the command '*esxcfg-firewall -c 514, udp, out, syslog'* to block outgoing traffic thru port 514. Defect# 259950

Display of Logical switches

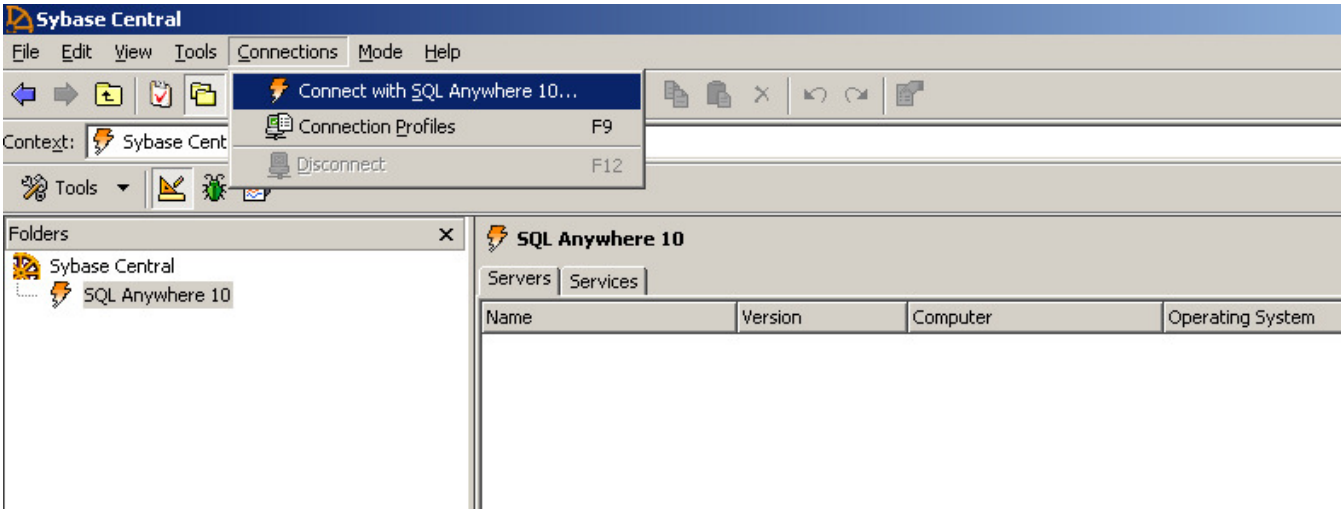
If Logical switches are created through the **Logical Switch** dialog, they will be displayed under **Undiscovered Logical Switch** in the existing **Logical Switches** panel. To display properly, discover the new logical Fabric.

Device Port update in topology View

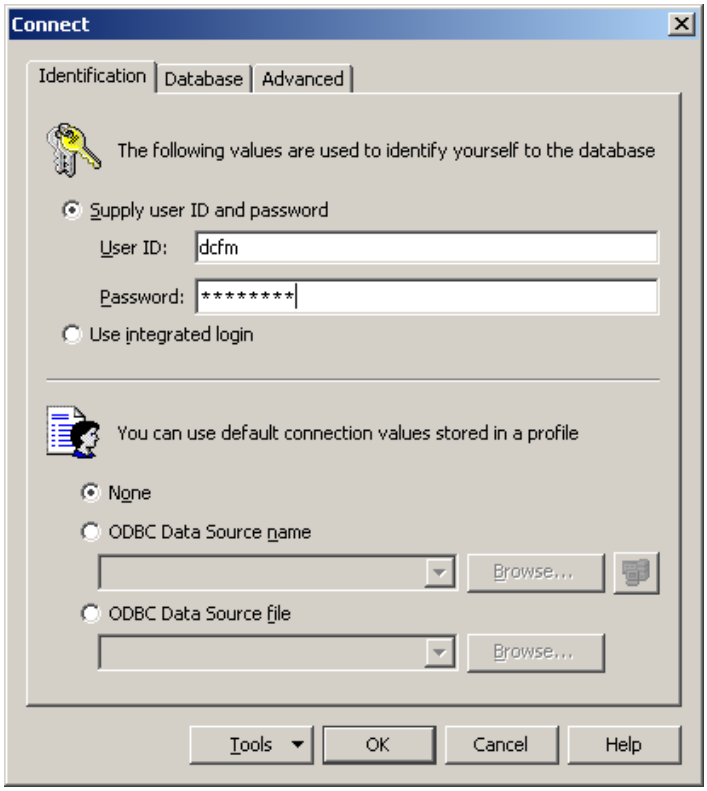
In the case of a non-VF environment, when the switches are discovered using SNMP V3, and if SSN (Soft Serial Number) is configured and if the EXT MIB is enabled, the device ports' status update can take between 2 to 30 minutes (based on SAN size) to get updated in the GUI. In order to get updates within 1 to 3 minutes (based on SAN size) in these scenarios, disable EXT MIB.

Procedure to update the FTP SERVER table with the new IP Address

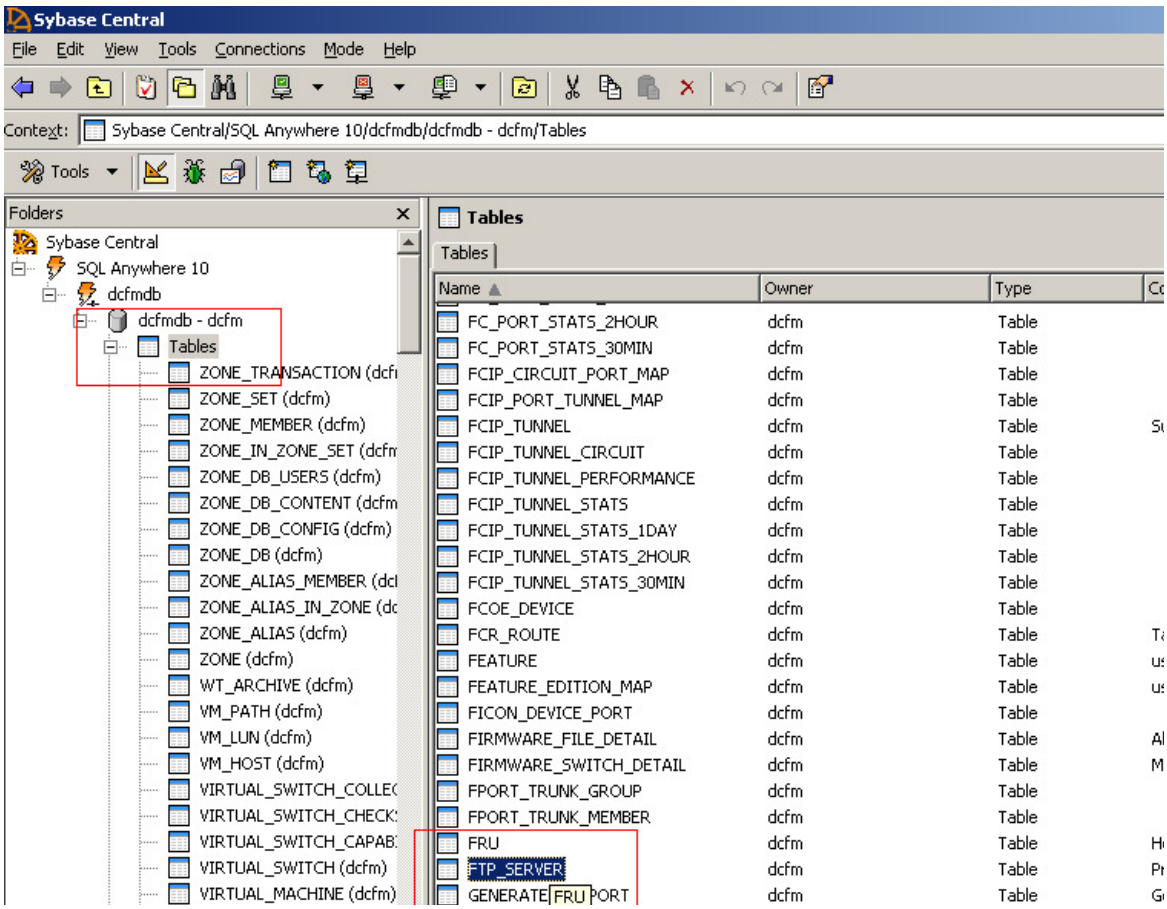
1. Go to <DCFM Home location>\db\Sybase Central 5.0.0\win32



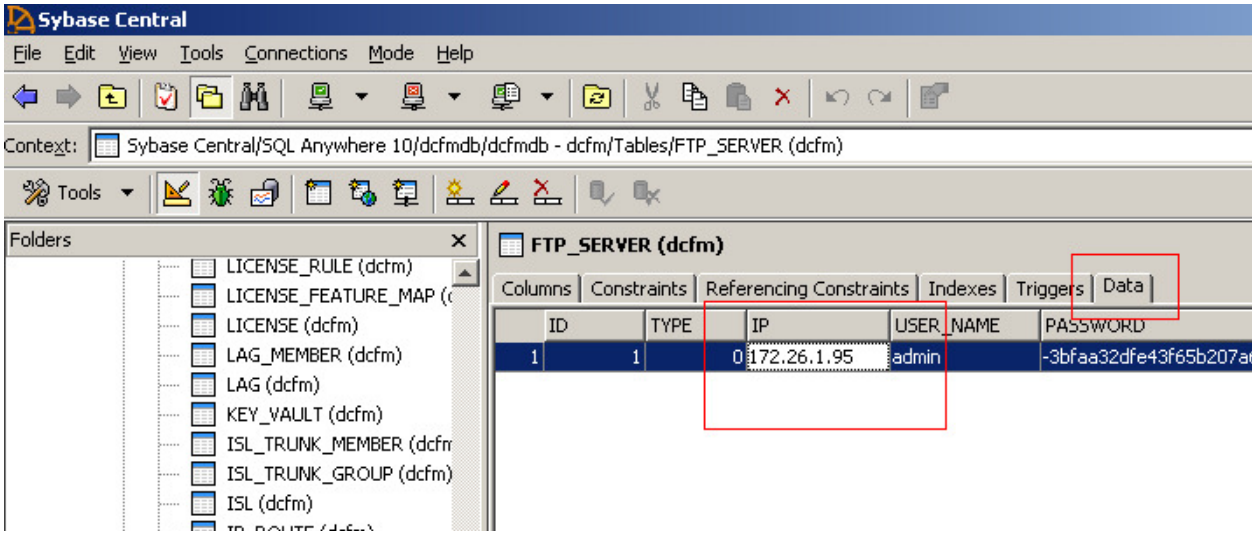
2. Launch the DB Application by clicking **scjview.exe**. Click on **Connections Menu > Connect with SQL Anywhere 10…**
3. Enter the username (“dcfm”) and password (“passw0rd”).



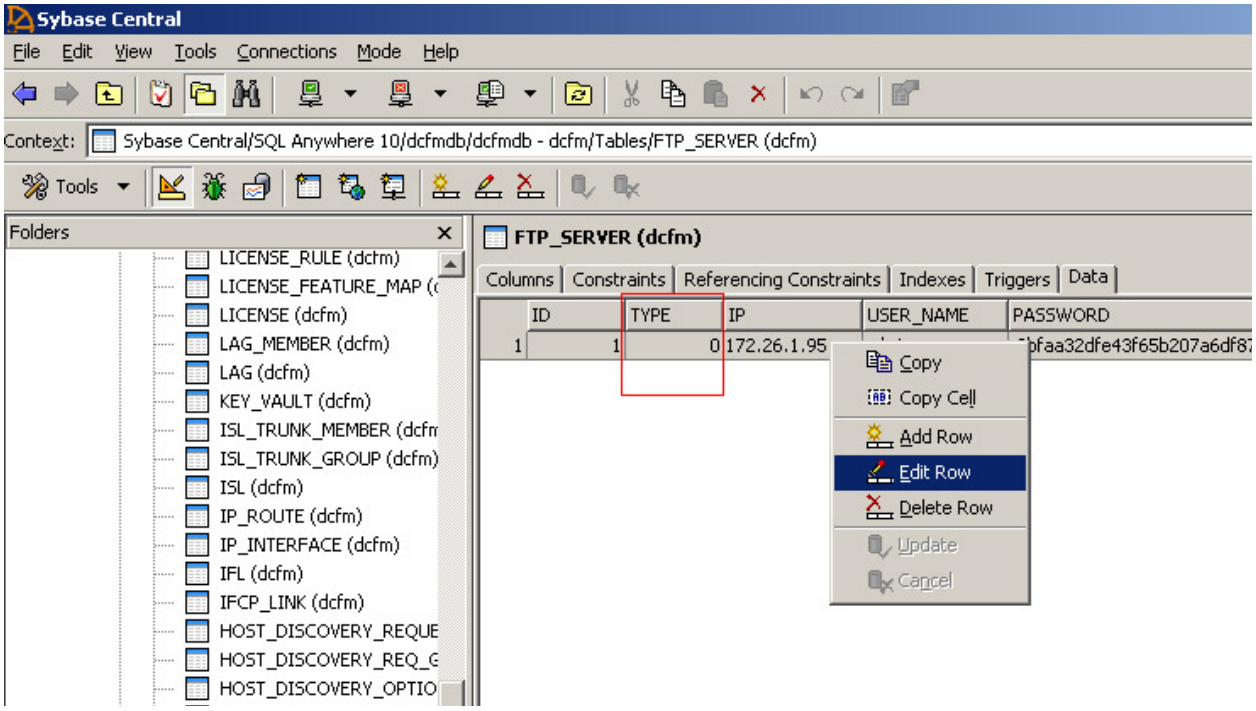
4. Click **Tables,** and then in the right pane, find and double click **FTP_SERVER**.



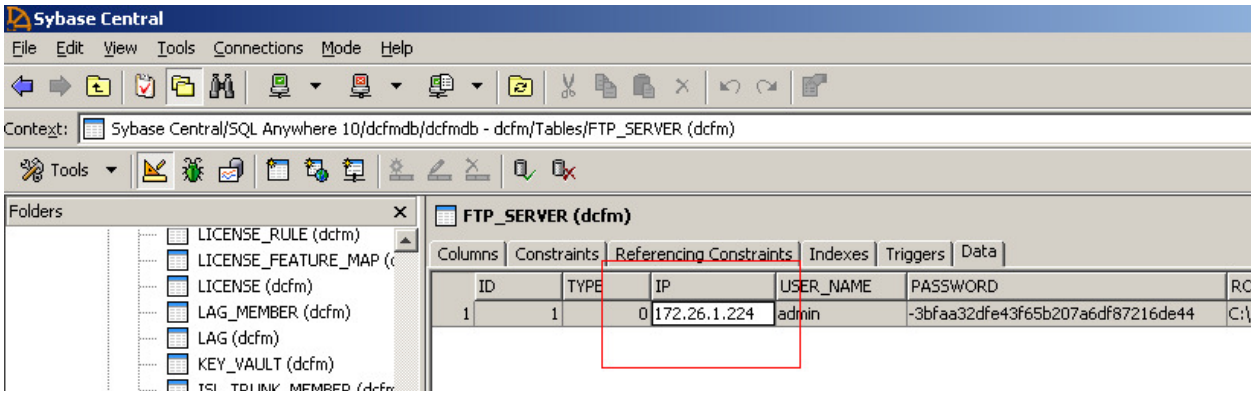
5. Click the **Data** tab.



6. Right click on the record with Type=0 (i.e. Internal) and select **Edit Row**.



7. Enter the new IP and click **Enter**. DO NOT modify any other column



8. Close the DB Connection and close the application

Changing the password to the Database

You are advised to change the default password to the database to prevent unauthorized access to the database. To change the database password, go to the *Install_Home/bin* directory and 1) open a command window and 2) type **dbpassword User_Name Password New_Password Confirm_Password** and click **Enter**. Further details are provided in the *DCFM User Manual*, Chapter 1, "*Getting Started*," in the "Changing the database user password" section.

Access Control List display

Access Control Lists are not displayed in the **ACL** tab of the **Edit** switch dialog for a CEE switch with FOS versions 6.3.1 and below.

SMI Enumeration issue

Enumeration instance fails for the following classes:

Brocade_EthernetPortLANEndPOint, Brocade_EthernetAdminDomainHostedLanEndPoint, Brocade_EndpointOfNetworkPipe, Brocade_EthernetSwitchHostedLANEndPoint, Brocade_InEthernetLogicalNetwork, Brocade_LANEndpoint, Brocade_PlatformHostedLANEndPoint

When DCFM discovers an IBM Converged Switch B32 connected to another IBM Converged Switch B32 running in AG mode and running FOS 6.3.x or lower, connected to FDMI enabled CAN.

Indications

The time to deliver the indication will vary based on DCFM SAN size selected during installation. If large SAN size is selected, indication delivery time will be longer.

SNMP Registration

Provider classes may take more time to update the fabric changes if the switches managed in DCFM are not SNMP registered. As this would cause a delay in indication delivery, all the switches managed in DCFM should be SNMP registered

Logging for CIMOM

The default logging level is "INFO" in integrated Agent. To change the logging level to DEBUG, update the "com.brocade" category value in cimom-log4j.xml file present in <Installation Dir>\conf folder.

The log file size and number of log files also can be changed by modifying the file rolling appender parameters in this cimom-log4j.xml file.

Logging level, file size, and number of log files can be changed by modifying the following fields: **Log Level**, **File Size**, and **Number of Files** from the configuration tool in the **CIMOM** tab

Accept Changes doesn't remove the plus or minus sign in Topology/Device Tree

The plus/minus sign will not be removed in the **Topology/Device Tree** when Accept Changes is performed after segmenting/Merging the switch/End Device. It is recommended to relaunch the client will remove the plus/minus sign. TR285364

Brocade Encryption SAN Switch is not identified as Router though FCR and IR license enabled

The Brocade Encryption SAN switch has FCR enabled and integrated routing license applied. But the router configuration dialog does not list it as a router in the router configuration dialog. Hence, the user cannot configure EX-ports for the Brocade Encryption Switch using DCFM. TR288917

Error message will not be shown for FC Ports when seclevel is set in the switch

Once the switches are discovered and seclevel is set in the switch on launching Realtime Graph dialog, no error message will be shown to the user. TR287843

DCFM is not processing the SNMPV3 traps for AG switches

If the AG switches are registered for SNMPV3 traps and acting as logical AGs, then if there are any changes made from the CLI, DCFM will update on lazy polling cycle. TR296597

DCFM is taking more time (2 mins for small SAN, 15 mins for medium SAN and 30 mins for large SAN) to update the CNA which is connected to IBM Converged Switch B32 in AG mode.

If the AG switches are registered for SNMPV3 traps and acting as Logical AGs, and if the user makes the CNA online from the CLI then DCFM will update on lazy polling cycle. TR282704

Syslog troubleshooting:

If the default syslog port number is already in use, you will not receive any syslog messages from the device. Use one of the following procedures (depending on your operation system), to determine which process is running on the Syslog port and to stop the process.

Windows Operating Systems

Finding the process

1. Open a command window.
2. Type *netstat –anb* | *find /i "514"* and press **Enter**.

   The process running on port 514 displays.

   For example, *UDP 127:0:0:1:514 *:* 3328.*

   Stopping the process

   Type **taskkill /F /PID "<PID>"** and press **Enter**.

   For example, **kill -9 "<3328>".**

OR

1. Select **CTRL + SHIFT + ESC** to open Windows Task Manager.
2. Click the **Processes** tab.
3. Click the **PID** column header to sort the process by PID.
4. Select the process you want to stop and click **End Process**.

Linux Operating Systems:

Finding the process

1. Open a command window.
2. Type *netstat –nap* | *grep 514* and press **Enter**.

   The process running on port 514 displays.

   For example, *UDP 0 0 ::ffff:127:0:0:1:514 :::* 27397*.

   Stopping the process

   Type **kill -9 "<PID>"** and press **Enter**.

   For example, **kill -9 "<27397>".**

Solaris Operating Systems:

Finding the process

1. Open a command window.
2. Type **ps –ef | grep syslog** and press **Enter**.

   The process running on port 514 displays.

   For example, *root 27154 1 0 13:49:14 ?.*

   Stopping the process

   Type **kill -9 "<PID>"** and press **Enter**.

   For example, kill -9 "<27154>".

Uninstalling ODBC DCFM install location

When ODBC installed in the <DCFM install> location, uninstalling ODBC will not remove the "odbc" folder from DCFM location and the ODBC driver shortcut menu item will not be removed. It is recommended to remove it manually.

Configuring OBDC connection manually

When the configuration page is skipped during ODBC installation, later user can create DSN by accessing <Install Home>\odbc\createdsn.bat

Performance Data Aging tab has been removed from Server Management Console (SMC)

User cannot configure the Performance Data Aging setting in DCFM 10.4.2, the tab has been removed from Server Management Console. The following are the default configuration settings:

- 288 samples for 5 minute period
- 144 samples for 30 minute period
- 84 samples for 2 hour period
- 90 samples of 1 day period
- Total number of samples –606

During migration from earlier releases all the historical data will be truncated with respect to the default samples and the aging configuration will not be migrated to 10.4.2.

Failover restriction in Mixed Fabric

In the case of Mixed Fabrics, only a FOS switch can be the seed Switch. Also, it is not possible to change the seed switch to EOS manually. In order to manage the fabric with EOS as seed switch, do the following:

1. Disconnect the ISL between the FOS and EOS switches
2. Unmonitor/Delete the FOS fabric
3. Discover the Pure EOS Fabric by providing EOS seed switch's IP Address"

Failover (i.e when seed switch is not reachable falling back to other switch as seed switch) can happen in all the cases mentioned below:

- FOS to FOS switches
- EOS to EOS switches
- EOS to FOS switches
- FOS to EOS switches

FICON Emulation restrictions in FCIP Tunnel configuration

The FICON Emulation tab in FCIP Advanced Settings dialog allows (requires) configuration of FICON Debug Flags setting to configure any FICON settings. The recommended value for FICON Debug flag should be set to 0x90010 (Even though the dialog indicates the supported range of 0x00000000 to 0xFFFFFFFF). Configuring this setting with any other value will interfere with the FICON Tape Write pipelining settings. This is applicable to 10.4.0/10.4.1/10.4.2

Documentation Updates

This section provides information on last-minute additions and corrections to the documentation. The most recent DCFM 10.4.x documentation manuals are available are available on the IBM SAN Support site: http://www.ibm.com/systems/support/storage/san

DCFM Installation Guide

On page 12, in the Client and server system requirements section, edit the supported clients as follows:

DCFM has the following client and server system requirements:

• Enterprise Trial — A single server supports a maximum of 8 clients (local or remote).

• Enterprise Edition — A single server supports a maximum of 8 clients (local or remote).

DCFM Migration Guide

On page 11, in the Client and server system requirements section, edit the supported clients as detailed above for the Installation Guide.

DCFM User Manual

On page 46, in the **Configuring virtual machine credentials** section, edit the instructions as follows:

Configuring virtual machine credentials

To configure credentials for a virtual machine, complete the following steps.

1. Select **Discover > Setup**.
   The **Discover Setup** dialog box displays.
2. Click **Add Host**.
   The **Add Host Discovery** dialog box displays.
3. Specify the hosts for discovery.
   To discover a host, refer to **Discovering Hosts by IP address or hostname** on page 42, **Importing Hosts from a CSV file** on page 43, or **Importing Hosts from a Fabric** on page 44.
4. Click the **Host Credentials** tab.
5. Select the **Discover Brocade HBAs in the hosts** check box.
6. Enter the HCM Agent port number in the **Brocade HBAs - Port** field, if necessary.
7. Enter your username and password in the appropriate fields.
8. Select the **Discover Virtual Machine information in the hosts** check box.
9. Enter the virtual machine port number in the **Virtual Machines - Port** field, if necessary.
10. Enter your username and password in the appropriate fields.
11. Click **OK** on the **Add Host Discovery** dialog box.
    If an error occurs, a message displays. Click **OK** to close the error message and fix the problem.
    A Host Group displays in **Discovered Addresses** table with pending status. To update the status from pending you must close and reopen the **Discover Setup** dialog box.
12. Click **Close** on the **Discover Setup** dialog box.

Starting on page 175, in the **SMI Agent configuration** section, change the Service Location Protocol (SLP) support information as follows:

Change the subsection title "***SLP support includes the following components:"*** to:

Management application SMI Agent SLP support includes the following components:

Replace the information on pages 177 and 178 with the following information:

SLP on UNIX systems

This section describes how to verify the SLP daemon on UNIX systems.

SLP file locations on UNIX systems

- SLP log—*Management_Application/cimom /cfg/slp.log*
- SLP daemon—*Management_Application*/cimom */cfg/slp.conf*
  You can reconfigure the SLP daemon by modifying this file.
- SLP register—*Management_Application/cimom /cfg/slp.reg*
  You can statically register an application that does not dynamically register with SLP using SLPAPIs by modifying this file. For more information about these files, read the comments contained in them, or refer to *www.openslp.org/doc/html/UsersGuide/index.html*

Verifying SLP service installation and operation on UNIX systems

1. Open a command window.
2. Type % su root and press **Enter** to become the root user.
3. Type # *Management_Application*/*cimom/bin/slptool findsrvs service:service-agent* and then press **Enter** to verify the SLP service is running as a Service Agent (SA).
4. Type # < *Management_Application >/cimom/bin/slptool findsrvs service:wbem* and then press **Enter** to verify the SLP service is advertising its WBEM services.
5. Choose one of the following options to verify the SLP service is advertising the WBEM SLP template over its configured client protocol adapters.
   - Type # *Management_Application/cimom /bin/slptool findattrs service:wbem:http://IP_Address:Port* and press **Enter.**
   - Type # *Management_Application/cimom /bin/slptool findattrs service:wbem:https://IP_Address:Port* and press **Enter.**

Note: Where *IP_Address:Port* is the IP address and port number that display when you use the **slptool findsrvs service:wbem** command.

SLP on Windows systems

This section describes how to verify the SLP daemon on Windows systems.

SLP file locations

- SLP log—*Management_Application\cimom \cfg\slp.log*
- SLP daemon—*Management_Application\cimom\cfg\slp.conf*
  You can reconfigure the SLP daemon by modifying this file.
- SLP register—*Management_Application\cimom\cfg\slp.reg*
  You can statically register an application that does not dynamically register with SLP using SLPAPIs by modifying this file. For more information about these files, read the comments contained in them, or refer to *www.openslp.org/doc/html/UsersGuide/index.html*

Verifying SLP service installation and operation on Windows systems

1. Launch the **Server Management Console** from the **Start** menu.
2. Click **Start** to start the SLP service.
3. Open a command window.
4. Type *cd c:\Management_Application\cimom \bin* and press **Enter** to change to the directory where *slpd.bat* is located.
5. Type > *slptool findsrvs service:service-agent* and press **Enter** to verify the SLP service is running as a Service Agent.
6. Type > *slptool findsrvs service:wbem* and press **Enter** to verify the SLP service is advertising its WBEM services.
7. Choose one of the following options to verify the SLP service is advertising the WBEM SLP template over its configured client protocol adapters.
   - Type > *slptool findattrs service:wbem:http:///IP_Address:Port* and press **Enter.**
   - Type > *slptool findattrs service:wbem:https:///IP_Address:Port* and press **Enter.**

Note: Where *IP_Address:Port* is the IP address and port number that display when you use the *slptool findsrvs service:wbem command*.

On page 146, in the **Single sign on support** section, change the procedure as follows:

To configure the Management application to support SSO, complete the following steps.

1. Create the trust store on the IBM product.

   The trust store is used to establish SSL communication between the Management application and the IBM product for authentication. For instructions, refer to the IBM Systems Director or TPC documentation about configuring users.

2. Configure the Management application by completing the following steps.

3. Copy the trust store to the tpc directory.
   The tpc directory is located in *Install_Home**bin**tpc* (Windows systems) or *Install_Home/bin/tpc* (UNIX systems).
   The trust store is located where you specified in step 1.

   a. Open a Command window.

   b. Type **cd** *Install_Home*\bin\tpc (Windows systems) or **cd** *Install_Home*/bin/tpc (UNIX systems) and press **Enter** to go to the tpc directory.

   c. Type **tpcssosetup.bat** (Windows systems) or **sh tpcssosetup** (UNIX systems) with the following parameters.

      IP address of the TPC or IBM Systems Director server as the 1st parameter,
      the port number of the TPC (default is 16311) or IBM Systems Director (default is 8422) server as the 2nd parameter,
      the trust store name (in current directory) as the 3rd parameter,
      password for the trust store as the 4th parameter,
      basic authentication user name as the 5th parameter, and
      basic authentication user's password the 6th parameter

      Example (Windows systems)

      tpcssosetup 10.32.1.1 16311 ibm_higgins_sso_10.32.1.1.jks password tipadmin super123

      Example (UNIX systems)

      sh tpcssosetup 10.32.1.1 16311 ibm_higgins_sso_10.32.1.1.jks password tipadmin super123

   d. Press **Enter** to configure single sign on for the Management application.

4. Create a new user account in the Management application, including user name, password, and resource group..
   This account must match the IBM Systems Director or TPC user account. To create a user account, refer to the **Adding a user account**.section
5. Make sure any switches you need to manage are discovered by the Management application.

   To discover a switch or fabric, refer to ***Discovery*** chapter in the *DCFM User Manual*
6. Restart the Management application.

Defects Closed with Code Change in DCFM 10.4.2

This section lists the defects with High and Medium Technical Severity closed with a code change in DCFM 10.4.2.

Defect ID: DEFECT000298392	**Technical Severity**: High
Summary: CIMOM: Indication subscription is failing when cimclient uses pegasus libraries.	
Symptom: User will not be able to use the indication feature when the OEM application / CIM client uses pegasus library.	
Feature: SMI Agent	**Function**: CIMOM
Probability: High	
Found in Release: DCFM10.4.0	**Service Request ID:**

Defect ID: DEFECT000300988	**Technical Severity**: Medium
Summary: The connectivity view of vCenter does not update in a timely manner.	
Symptom: The user will not be able to view the configured LUNs in the connectivity view within a minute.	
Feature: VM Plugin	**Function**: CONFIGURATION
Probability: High	
Found in Release: DCFM10.4.0	**Service Request ID:**

Defect ID: DEFECT000300724	**Technical Severity**: Medium
Summary: Issues renaming the changed name in the "Name" column to the original name.	
Symptom: User will not be able to change the name when the same fabric is unmonitored.	
Feature: Name Changes	**Function**: USABILITY
Probability: High	
Found in Release: DCFM10.4.0	**Service Request ID:**

Defect ID: DEFECT000299526	**Technical Severity**: Medium
Summary: In tape encryption if the media changer is added as "tape LUN" in a CTC, the status is reported incorrectly.	
Symptom: :Incorrect status is shown for media changer device in Tape LUN CTC.	
Feature: Encryption	**Function**: CONFIGURATION
Probability: Medium	
Found in Release: DCFM10.4.0	**Service Request ID:**

Defect ID: DEFECT000300991	**Technical Severity**: Medium
Summary: SMI ONLINE DB to be hidden in DCFM.	
Symptom: SMI_ONLINE_DB is not specific to DCFM but it is always being displayed in the DCFM zoning dialog.	
Feature: ZONING	**Function**: Zoning Dialog
Probability: Medium	
Found in Release: DCFM10.4.0	**Service Request ID:**

Defect ID: DEFECT000300522	**Technical Severity**: Medium
Summary: When configuring multiple LUN settings changing from plain to encrypted, not all LUNs can undergo FTE.	
Symptom: Not able to modify encryption mode and enable encrypt existing data when FTE inprogress for the LUNs.	
Feature: Encryption	**Function**: CONFIGURATION
Probability: High	
Found in Release: DCFM10.4.0	**Service Request ID:**

Defect ID: DEFECT000300536	**Technical Severity**: Medium
Summary: FCIP – Verify IP Connectivity operation fails but circuit comes up when same parameter is configured through CLI.	
Symptom Tunnel creation fails with the reason as destination unreachable..	
Feature FCIP	**Function**: CONFIGURATION
Probability: Medium	
Found in Release: DCFM10.4.1	**Service Request ID:**

Defect ID: DEFECT000300990	**Technical Severity**: Medium
Summary: SMI_ONLINE_DB to be created only if SMI agent is enabled.	
Symptom: SMI_ONLINE_DB is created even when SMI agent is not enabled during Installation	
Feature: SMI Agent	**Function**: Zone Control SubProfile
Probability: Medium	
Found in Release: DCFM10.4.0	**Service Request ID:**

Defect ID: DEFECT000298459	**Technical Severity**: Medium
Summary: Encryption – No error message is displayed when importing large sized certificates fails in the switch.	
Symptom: When importing certificates that contain both the text and Base64 encoded portion of a certificate, then the import will fails in switch but reports a success in the application.	
Feature: Encryption	**Function**: CONFIGURATION
Probability: Low	
Found in Release: DCFM10.4.0	**Service Request ID:**

Defect ID: DEFECT000299641	**Technical Severity**: Medium
Summary: ISL link not showing in topology view.	
Symptom: User will be misleaded with incorrect updates in the Topology.	
Feature: DISCOVERY	**Function**: ISL Discovery
Probability: High	
Found in Release: DCFM10.4.0	**Service Request ID:**

Defect ID: DEFECT000301516	**Technical Severity**: Medium
Summary: Hex Display – Incorrect FC Address is displayed in the Logical Switches dialog.	
Symptom: Incorrect address is displayed for few ports.	
Feature: Client	**Function**: USABILITY
Probability: High	
Found in Release: DCFM10.4.1	**Service Request ID:**

Defect ID: DEFECT000301071	**Technical Severity**: Medium
Summary: Discovery – Discovery of Pure EOS fabric with Access Gateways failed with no reason given in the error message.	
Symptom: Fabric is not discovered and no details are given in the error message for the failure.	
Feature: DISCOVERY	**Function**: Switch Discovery
Probability: Medium	
Found in Release: DCFM10.3.3	**Service Request ID:**

Defects Closed with Code Change in DCFM 10.4.1

This section lists the defects with High and Medium Technical Severity closed with a code change in DCFM 10.4.1.

Defect ID: DEFECT000297330	**Technical Severity**: Medium
Summary: The user is not allowed to enable FMS mode when 256-area limit is disabled for logical switches.	
Symptom: For a logical switch with 256-area mode disabled, if the user tries to enable the FMS mode, a warning message is displayed and the user is prevented from performing the operation.	
Workaround: Use the cli to enable the FMS mode.	
Feature: FICON	**Function**: Cascaded FICON Configuration
Probability: Medium	
Found in Release: DCFM10.4.0	**Service Request ID:**

Defect ID: DEFECT000297921	**Technical Severity**: Medium
Summary: Properties with wrong values are returned when the switch with firmware version 6.1.x or less managed with invalid snmp credentials.	
Symptom: User may not able to retrieve the correct Fabric WWN, switch information like vendor, model and serial number and zoning operation cannot be performed for the switch running with firmware 6.1.x or less with invalid snmp credentials.	
Workaround: Discover the switch with snmp credentials	
Feature: DISCOVERY	**Function**: USABILITY
Probability: Medium	
Found in Release: DCFM10.4.0	**Service Request ID:**

Defect ID: DEFECT000297082	**Technical Severity**: Medium
Summary: LUNs are listed twice in the Encryption Disk LUN View dialog.	
Symptom: In an FCR environment, each container may display duplicate entries for each of the LUNs.	
Workaround:	
Feature: DISCOVERY	**Function**: CONFIGURATION
Probability: Low	
Found in Release: DCFM10.4.0	**Service Request ID:**

Defect ID: DEFECT000296701	**Technical Severity**: Medium
Summary: When more than a million events are received in a single day, the Event Purge mechanism fails.	
Symptom: When more than a million events are received within a single day, the event purge mechanism may fail and the the number of events in the database continues to grow. In this condition, if the user tries to launch the Audit Log dialog, due to a large number of events being retrieved, the server may restart due to an out of memory exception.	
Workaround:	
Feature: FAULT MANAGEMENT	**Function**: USABILITY
Probability: Medium	
Found in Release: DCFM10.4.0	**Service Request ID:**