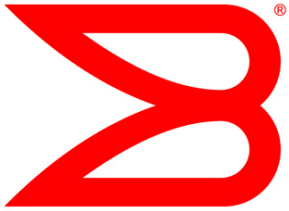


FROM THE SOLUTIONS CENTER

Solution Guide: Migrating from Brocade Enterprise Fabric Connectivity Manager to Brocade Data Center Fabric Manager

Brocade Data Center Fabric Manager (DCFM) simplifies infrastructure management with the performance and scalability required in the Brocade Data Center Fabric, which connects applications to infrastructure in the majority of the world's data centers.

BROCADE

CONTENTS

INTRODUCTION

Brocade® DCFM® is a management application that provides easy, centralized management of the Storage Area Network (SAN), as well as quick access to all product configuration applications. Using this application, you can configure, manage, and monitor your networks with ease. In order to introduce higher scalability and performance, Brocade DCFM was designed to perform discovery through a single Fabric OS® (FOS) director or switch, whereas Brocade Enterprise Fabric Connectivity Manager (EFCM) discovered all directors directly over an Ethernet connection. In an existing Storage Area Network (SAN) comprised of legacy McDATA directors, a Brocade discovery switch must be introduced prior to upgrading from EFCM to DCFM (see the "Planning" section).

In addition to reading this document, for further details about how to install, configure, and deploy Brocade DCFM, ensure that you have access to current product documentation:

- *Brocade Data Center Fabric Manager Enterprise User Manual*
- *Brocade Data Center Fabric Manager Migration and Transition Guide*: provides installation instructions, migration instructions from both Brocade EFCM and Brocade Fabric Manager, and information about the differences between EFCM and Fabric Manager interfaces and the Brocade DCFM interface.
- *Brocade Data Center Fabric Manager Enterprise Release Notes*

And other Brocade papers:

- *Brocade DCFM Features Brief*
- *Brocade DCFM Data Sheet*

NOTE: Although there are two editions of Brocade DCFM, unless otherwise noted, this document refers to Brocade DCFM Enterprise. Brocade DCFM Professional is another version of the application with a subset of capabilities.

This document is for Brocade customers who are currently using Brocade Enterprise Fabric Connectivity Manager (EFCM) and want to find out more about migrating to Brocade DCFM. It is not intended as a definitive technical reference on Brocade DCFM, but it provides guidelines for field engineers or IT personnel at customer sites.

Supported Firmware

FOS

- Version 5.0.0 or later for FOS only fabrics
- Version 6.0.0 for Native Interoperability (NI) fabrics

M-EOS

- Version M-EOSc 9.6.x or later
- Version M-EOSn 9.6.x or later

NOTE: Although you do not have to install or know the Java version used because it is bundled with both versions of Brocade DCFM, development was conducted using Java JDK 1.6.

Migration Facts

There is no charge for Brocade EFCM license conversion to Brocade DCFM Enterprise:

- EFCM customers with valid software licenses are entitled to upgrade to a DFCM Enterprise license at no additional charge.
- Customers upgrading to DCFM Enterprise are required to purchase a service agreement with a minimum one-year term.
- You can upgrade to Brocade DCFM if you currently have the EFCM Enterprise Base, EFCM Enterprise + Advanced Module, EFCM Standard 9.6 or 9.7 to DCFM Enterprise
- Data from your Brocade EFCM will be migrated to DCFM Enterprise. Brocade DCFM Enterprise supports a mixed M-EOS and FOS fabric. On pure M-EOS fabrics, consult your sales representative to help you decide the right solution for your environment.

Migration Overview

The migration is described in detail in the *Brocade DCFM Migration and Transition Guide*. For your convenience, this section lists high-level steps required for the migration in a Windows environment, including:

- Review the "pre-flight" checklist, making sure that:
  - You have the DCFM license key (on the *Key Certificate*) and serial number (from the DVD jewel case).
  - A version of EFCM is installed on your server that meets migration requirements.
  - The fabric is using the required version of M-EOS.
  - The EFCM data is fully backed up on your current management servers.

  NOTE: Ensure that all instances of the EFCM client are closed on the management server and on remote workstations.
- Insert the Brocade DCFM installation DVD into the drive on a Windows management server and follow onscreen directions.
- Migrate data from your Brocade EFCM application. This could take up to 30 minutes.
- Specify the following settings and apply them (could take up to 30 minutes):
  - Configure the IP server.
  - Configure server Syslog, Web server, SNMP, and starting ports.
  - Configure the fabric size (small, medium or large).
  - Select the FTP server.
- Start the DCFM server and client. Once all the DCFM services are started, you can log in. You can use your user ID and password from EFCM.

PLANNING

As with all technology upgrades in the data center, planning is a critical part of the process. When you are migrating from one software application to another, you need to find out as much as you can about the new application and how it differs from the application you are currently using, that is, Brocade EFCM. Then decide when is the right time to upgrade and start putting a task list, task owners, and a timeline in place.

Migration Considerations

There are several things to consider when you are making the decision to migrate to Brocade DCFM. Note the following:

- Export to database (MySQL and DB2) not supported: the EFCM flat-file structure is replaced by a Sybase database in DCFM.
- Third party integration API support: SMI-S is the third party integration management interface for DCFM.
- Event Management Rules: DCFM has different Event Management capabilities (see the product documentation for details).
- Manager of Managers (MoM): Master/subordinate instances are not supported.
- Group-by function in Views: All views are migrated, but any views customized by a "Group-by" revert to their default grouping.
- The Performance Data and Master log is not migrated from EFCM to DCFM.

The Discovery Switch

A switch, which is called a "discovery switch" when it is used in this context, must be a B-Series device running Fabric OS® (FOS). The discovery switch is a switch in the fabric that uses in-band communication to get fabric-wide information about the Name Server, Zoning, and fabric membership. *There must be at least one discovery switch configured in pure Fabric OS fabrics and present and configured in mixed fabrics.* The presence of a discovery switch provides significant help in improving the scalability of the application.

NOTE: In the Brocade DCFM interface, the discovery switch may be called the "seed switch."

The following devices can be configured as a discovery switch:

- For pure FOS fabrics: B-Series switch running FOS 5.0.x or later
- For mixed fabrics: B-Series switch running FOS 6.0.x or later in Native Interop mode

Note the following:

- DCFM expects the FOS discovery switch to be running the most recent level of firmware in the fabric.
- You cannot use a switch in Access Gateway mode or a switch connected to the fabric either via EX_Ports or VEX_Ports.
- DCFM end users need to have administrative privileges on the discovery switch (or equivalent access, such as root, factory, or admin).
- Eclipse (McDATA routers) discovery and configuration is not supported.
- Pure QLogic/Cisco fabrics are not discovered.
- Only basic information is displayed for non-Brocade devices.

Brocade DCFM allows you to bring down the current discovery switch for maintenance or replacement. For High Availability (HA) with one discovery switch, the recommendation is to configure Inter-Switch Links (ISLs) to more than one switch in the fabric to handle potential port failures. You could also support HA with two discovery switches, in which case the recommendation is to have at least two B-Series switches for failover (manual).

General recommendations for a discovery switch are:

- Small fabrics: Use an entry level switch, such as the Brocade 200E (in switch not Access Gateway mode) or the Brocade 300.
- Medium fabrics: You can use a Brocade 5000 Switch, but Brocade DCX Backbone or 48000 Director is recommended.
- Large fabrics: You can use a Brocade 5000 Switch, but Brocade DCX Backbone or 48000 Director is recommended.

Using FOS 6.2 or later, you can take advantage of the Virtual Fabrics feature in Fabric OS to partition a switch and use the resulting Logical Switches as discovery switches for multiple M-EOS fabrics. Doing so allows you to manage them using a single FOS discovery switch for all of them, something that was not available prior to version 6.2.

Deployment Best Practices for Public/Private Networks

They are many different ways that a DCFM server can be deployed. Some configurations are restrictive and provide greater levels of security. Other configurations are more flexible and may make it easier to deal with change. Planning the LAN connectivity for DCFM will help to ensure that your deployment matches the needs of your environment.

Open Management Network

For the purpose of this document an Open Management Network is one where the DCFM server is attached to the company intranet with a single Ethernet attachment, as shown in Figure 1. The devices to be managed by DCFM are also attached directly to the company intranet via Ethernet. Typically the server and the devices are in the same location and likely on the same subnet, but devices could be remote as well.

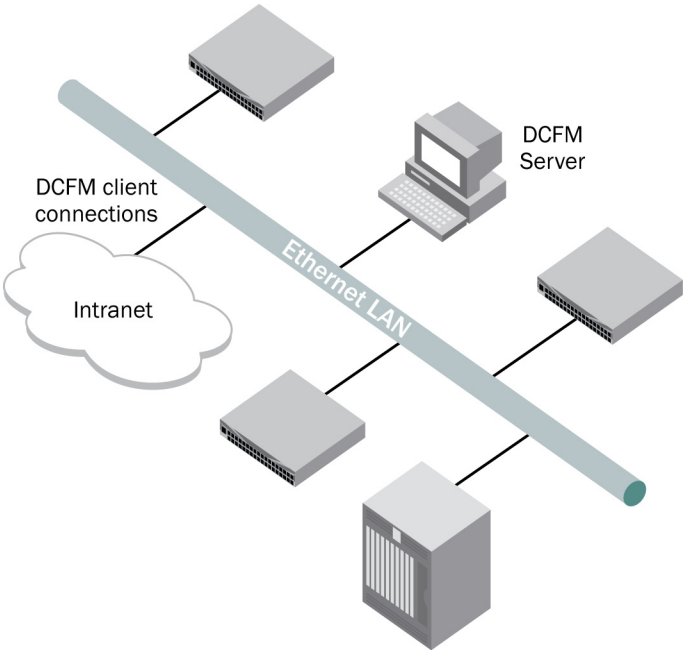


Figure 1. Open management network configuration

There are several advantages to an open management network:

- Configuring DCFM and the devices is straightforward as there is little concern for IP routes or the DCFM server having multiple Network Interface Cards (NICs). Furthermore, a SAN administrator who wishes to use Web Tools, Telnet, SSH, or other management protocols outside Brocade DCFM can easily do so from any client station with access to the intranet that the SAN devices are attached to.
- Another benefit of an open management network is that the devices can be configured to send asynchronous messages to a server other than the DCFM server. For example, SNMP or SYSLOG could be configured on each of the managed devices to send messages to a server (other than the DCFM server), which would receive and process those messages accordingly.
- One of the most important benefits of an open management network is the ability to have a server that runs scripts that utilize SSH, Perl, Expect, or other scripting protocols to communicate with and make changes on the Fibre Channel (FC) devices under management.

There are some caveats, however, to using an open management network:

- Probably the most critical is the other viewpoint of one of the strengths of this configuration, that is, that any device on the customer intranet can use any of the available protocols to access any backbone, director, or switch attached to the network.
- Protecting the FC devices with strong passwords is especially important in this configuration.
- In addition, access restrictions can be set at either the managed SAN device (backbone, director, switch) or in the managed Ethernet switch to which the SAN device's management port(s) are connected. Restrictions can be set by IP address, IP ports, or both. Doing so reduces the security concerns of running an open management network. Attaching SAN devices to a company intranet could expose them to other security threats, including attempts to gain access, denial of service attacks, and others. As previously explained, the risks of running in an open management network can be greatly reduced by creating access restrictions.

Private Management Network

In a private management network, Brocade DCFM is attached to both the company intranet with one Ethernet connection and a private network, to which managed devices are also be attached. DCFM client connections are accepted on the Ethernet connection attached to the company intranet, and all management traffic between DCFM and the devices are on the private network, as shown in Figure 2.

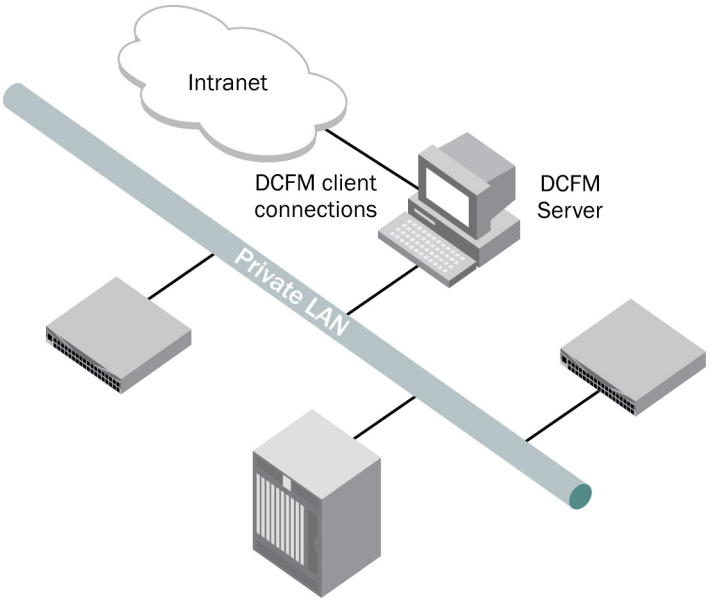


Figure 2. Private management network configuration

The private management network was a common configuration with Brocade EFCM in the past. Many customers used an Ethernet hub, which was included as part of a rack system into which the FC switches or directors were installed in. While it is still possible to run DCFM with a private management network on a hub, you can achieve better performance between the DCFM server and the managed devices using a minimum of one dedicated fast Ethernet switch (100 MB, full-duplex device). A private Virtual LAN (VLAN) on a larger network switch would provide the most robust solution.

A private management network provides the benefit of having the DCFM server act as a firewall between the company intranet and the managed FC switches. Denial of service attacks and attempts to log in could largely be performed only against the DCFM server itself and not against the managed devices. Access to the DCFM server should be protected in the same way that other critical servers in the data center are—to prevent unauthorized access.

While the private management network provides a configuration that can prevent access other than the DCFM server to managed devices, note that there are proxy agents on the DCFM server that will allow limited access to the managed devices through other protocols. A telnet and HTTP proxy both exist in the DCFM server.

- (M-EOS only) The telnet proxy requires that you log in to the proxy first with the login/password combination you would use to log in to the DCFM server, and then a client will be allowed to establish a telnet session through the DCFM server to a given managed FC device.
- The HTTP proxy provides a mechanism to use Brocade Web Tools from stations on the company intranet other than the DCFM server. No proxy agents exist on the DCFM server for SSH, SCP, SNMP, FTP, or Syslog.

While it may still be possible to use some level of scripts (Perl, Expect, and so on) to make changes on the managed devices, it can be much more complex in the private management network configuration mostly due to the inability to have clients outside the private network communicate directly with the managed devices. It is likely that the only way to do it securely would be to run the scripts on the DCFM server or add another connection to the private network from a server that runs the scripts to make changes on the managed devices.

Hybrid Management Network

In rare cases, hybrid management networks, that is, private management network topology and open network management topology are both implemented with the same server, as shown in Figure 3. In most cases these configurations started as private management networks and later managed devices not close enough to be included in the private management network were added and were therefore brought under management in an open management network configuration. Some data centers may decide to stay with a hybrid configuration for various reasons. There may be mission critical directors on the private network, while the devices on the company intranet may be much less critical. Note that a hybrid configuration is a valid configuration and that the benefits and drawbacks of the private and open management network types apply to their respective portions of the hybrid management network.

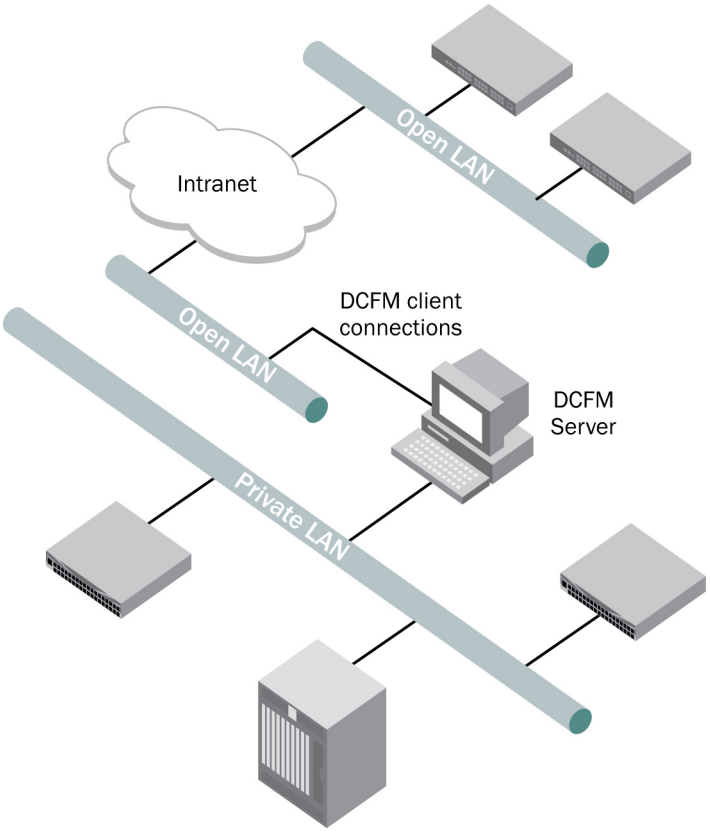


Figure 3. Hybrid management network configuration

Split Management Network

Split management networks are usually found when a Fibre Channel network spans more than one location or data center, as shown in Figure 4. In a split management network, some portion of the SAN is under management of a DCFM server in its location, while another portion of the SAN is under management of a different DCFM server at another location. The actual LAN topology for management is still likely to be either an open management network or a private network management network as described above.

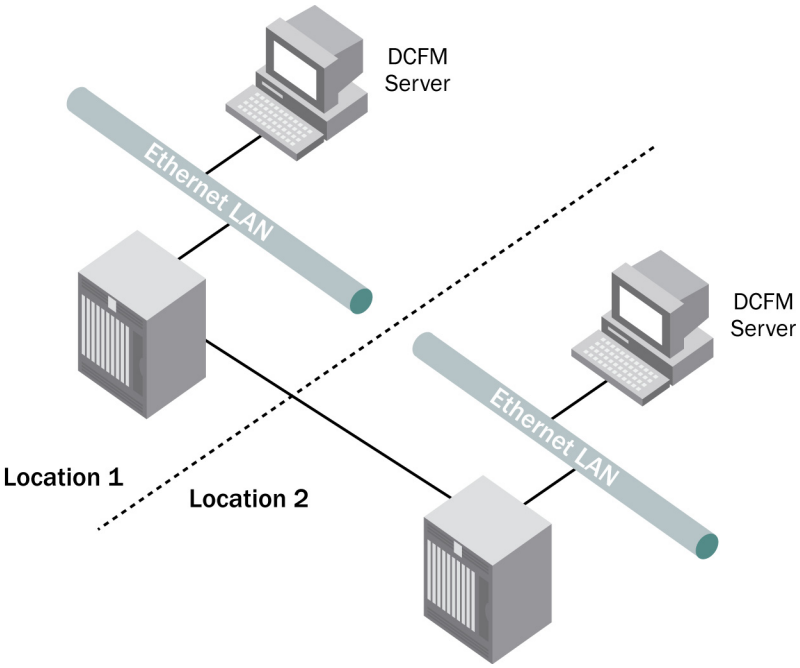


Figure 4. Split management network configuration

Zoning

Using Brocade EFCM, you can construct offline zone sets and save them into a global library or into individual per-fabric libraries in the EFCM database. The only time that an EFCM zone set is sent to the fabric is during a Zone Set Activation operation.

In Brocade DCFM, the Zone DB menu (shown in Figure 5) is equivalent to the Zone Library menu in EFCM and can display up to three items immediately following a migration:

- **Fabric Zone DB:** This function is implemented to access the defined and effective offline zone configurations stored in the fabric when a FOS switch is present.

  NOTE: Because switches in an M-EOS fabric cannot contain more than one zone configuration, EFCM has no equivalent capability. Legacy EFCM users can disregard the Fabric Zone DB data.

- **Zone Library:** This library reflects zoning information contained in the autonomous EFCM per-fabric zoning libraries. If you were not using per-fabric libraries prior to migration (that is, using the global library instead), then this selection will not contain any data.

- **Global Zone Library:** This library reflects zoning information contained in the common EFCM global zoning library. If you were not using the global zoning library prior to migration (that is, using per-fabric libraries instead), then this selection will not contain any data.

  DCFM Operational Difference: The DCFM Global Zone Library is NOT as common a library as it was in EFCM. During migration, the EFCM Global Zone Library is simply replicated into a per-fabric Zone Library for each fabric. Therefore, a DCFM Global Zone Library behaves like any autonomous per-fabric Zone Library.

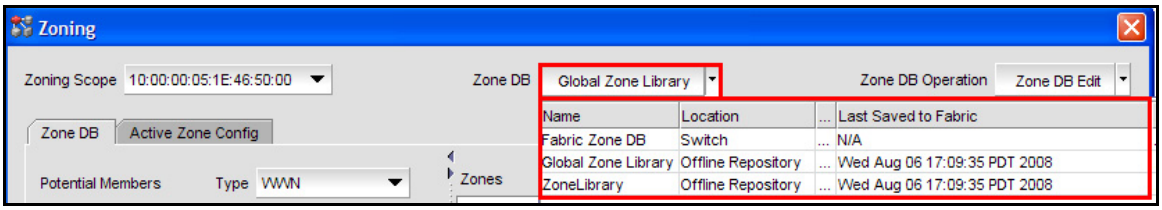


Figure 5. Zoning window showing the Zone database menu

Nicknames

Called "Nicknames" in Brocade EFCM, you can use Names in DCFM as a way of providing simple user-friendly names for products and ports. During migration, nicknames are converted to names and are exported to a CSV file. Once you have logged into DCFM, you can import this file. Note that the user-configurable setting for whether or not to use unique or non-unique names is also migrated.

NOTE: If you have nicknames that are greater than 128 characters in length, they are truncated at 128 characters during data migration. Although it is unlikely that truncating names will cause problems, if you know you have very long nicknames, you might want to make them 128 characters or less in EFCM before the migration.

Third-Party Management Products

Many customers use a combination of Brocade EFCM and third-party Storage Resource Management (SRM) products to manage their storage and fabric infrastructure. The most commonly used SRM products include:

- EMC ControlCenter (ECC)
- IBM TotalStorage Productivity Center (TPC)
- HP Storage Essentials (SE)
- Hitachi Storage Services Manager
- NetApp Onaro SANscreen
- Symantec CommandCentral Storage (CCS)

Customers leverage these SRM products primarily for LUN-level activities (for example, LUN provisioning, LUN masking/mapping, reporting, chargebacks, and performance characterization). They are also used in conjunction with EFCM to manage storage provisioning for applications via the connected network fabric (configuring the fabric ports for appropriate protocol/speed, zoning, configuring QoS parameters, collecting performance statistics, monitoring for error conditions, and so on).

EFCM is used to support both proprietary API interfaces (ECC API for EMC ECC, SWAPI for other SRM products) and standards-based SMI-S interfaces to enable these SRM products to discover and manage SAN elements. With DCFM, the proprietary APIs are not being carried forward, since they reached End of Life (EOL) a while ago in favor of the standards-based SMI-S approach. Therefore, customers migrating from EFCM to DCFM will have to ensure that they use SMI-S for any fabric and switch related activities that they

want managed through these SRM products. All of Brocade's key partners have already migrated their SRM products to SMI-S and therefore, this shouldn't pose any issues.

NOTE: For more details on best practices regarding deployment of SMI-S providers for various scenarios (public/private networks, FOS and M-EOS intermixed fabrics in IM2 and IM3 modes, and so on), refer to either the OEM best practices.

Table 1. Compatibility between SRM products and SMI-S for FOS and M-EOS

SRM Product	SRM Product Version	SMI for FOS Version	SMI for M-EOS Version
EMC ControlCenter (ECC)	6.1	120.7.2	2.5
IBM TotalStorage Productivity Center (TPC)	3.1 3.3.0 3.3.1 3.3.2	120.7.2	2.5
HP Storage Essentials (SE)	5.1 6.0	120.7.2	2.5
NetApp Onaro SANscreen	TO COME	TO COME	TO COME
Symantec Command Central Storage	5.0 5.1	120.7.2	2.2.2

IMPORTANT: Information provided in the table above is current as of the writing of this document

Integration APIs (SMI, SWAPI)

Storage Management Initiative (SMI) is a broad-based initiative sponsored by the Storage Networking Industry Association (SNIA) that is standardizing all aspects of storage management for multivendor storage networking products. SMI encompasses the storage aspects of the Common Information Model (CIM) from the Distributed Management Task Force (DMTF). "CIM provides a common definition of management information for systems, networks, applications and services, and allows for vendor extensions. CIM's common definitions enable vendors to exchange semantically rich management information between systems throughout the network."

The Brocade SMI Agent (SMI-A) is a "proxy" agent to multiple fabrics; it resides on a separate host. When it is deployed, the SMI-A does not require any modification or upgrade to deployed fabrics. All the support required in Brocade switches is already in place.

The Brocade SMI Agent supports the evolving SMI-S standard and the Brocade functionality not available through the standard.

The Brocade SMI Agent provides the following features:

- CIM agent compliant with SMI-S, with support for the following profiles:
- Server profile (supported by the SMI-A with CIMOM vendor-supplied providers)
- Fabric profile
- Switch profile
- Extender profile (discovery only)

- Fibre Channel (FC) Host Bus Adapter (HBA) profile
- Additional support for physical objects such as chassis, blades, fans, power supplies, temperature sensors, and transceivers

It supports the following:

- Connection and account management
- Port performance and error statistics
- HBA and device information via FDMI
- Configuration download to switches
- Firmware download to switches
- SLP (Service Location Protocol) to discover SMI-S profiles
- CIM agent management using CIM
- Indications: life-cycle indications for fabrics, SANs, nodes, switches, and switch ports; and alert indications for many fabric events.
- Basic support for non-Brocade switches (switches, ports, topology information, and so on)
- HTTP and HTTPS protocols
- HTTP and HTTPS port configuration
- Mutual authentication for clients and indications
- Security authorization using native OS access control mechanisms
- Provider logging of exceptions, operations, and performance metrics for diagnostic purposes
- Secure SAN fabrics
- Secure RPC communication
- CIM queries, using WBEM Query Language (WQL)

Northbound notification – SNMP, Syslog forwarding

- **SNMP Trap Forwarding:** You can configure the application to send SNMP traps to other computers. To correctly configure trap forwarding, you must configure the target computer's IP address and SNMP ports.
- **Syslog Forwarding:** Syslog messages are available only on B-Series platforms.

  Syslog forwarding is the process by which you can configure the management application to send Syslog messages to other computers. Switches send the Syslog information only through port 514; therefore, if port 514 is being used by another application, you must configure the management application to listen on a different port. Then you must configure another Syslog server to listen for Syslog messages and forward the messages to the management application Syslog listening port.

  Syslog messages are persisted in the database. You can view the Syslog messages from the management application. However, the management application does not convert the Syslog messages into event objects except for the audit Syslog messages.

Topology Maps

Client Interface

Users of EFCM will be very familiar and comfortable with the DCFM interface, as the two are almost identical. The key difference between the two interfaces is that the Event Management and Security tabs are in different places.

- You can access Event Policies available through **Monitor > Event Policies** .
- Security Center is available only through the M-Series Element Managers. One change on the toolbar is that the Export function is no longer available as that functionality has been moved to individual dialog boxes.

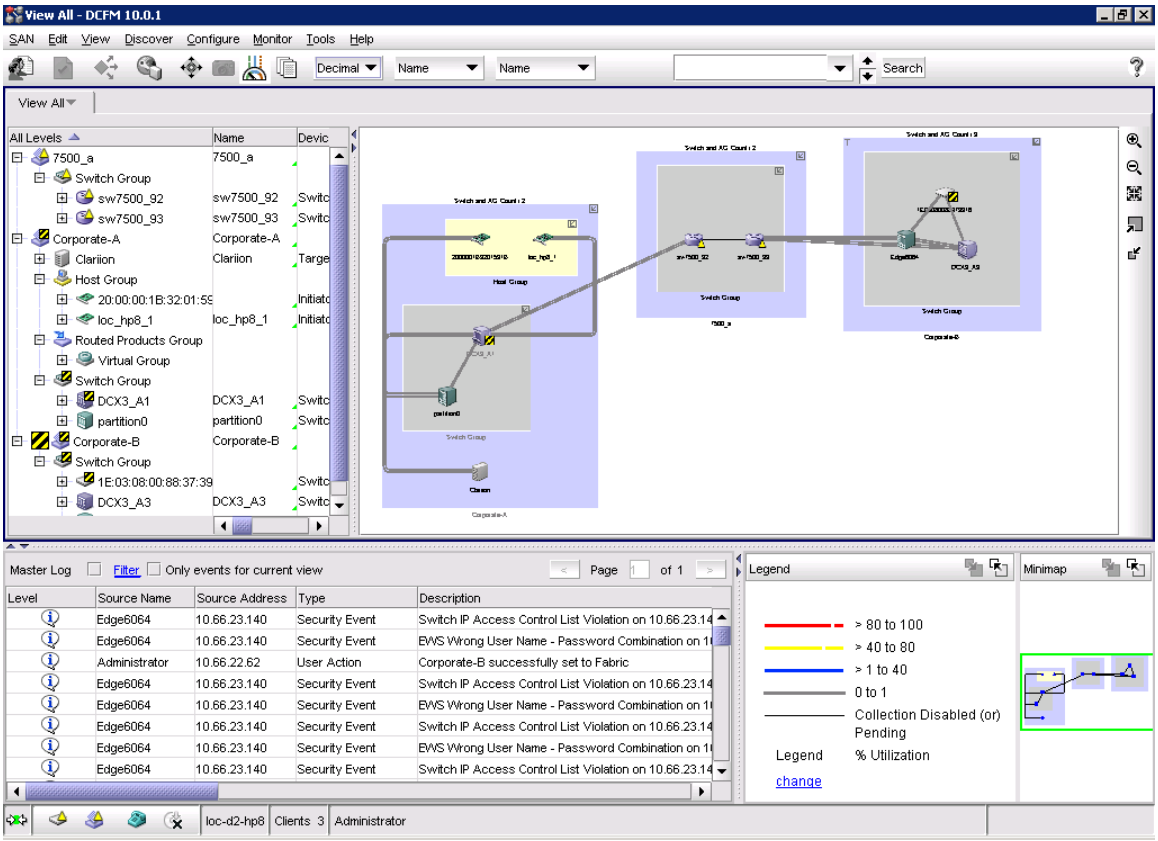


Figure 6. Example DCFM topology screen

Topology Layout

After upgrading to DCFM, the topology layout options may be set back to defaults. If that is the case, you will still be able to customize various parts of the topology, including the layout of devices and connections as well as group background colors, to easily and quickly view and monitor devices in your SAN. See the "Topology Layout" section in the *Brocade DCFM Enterprise User's Manual* for details on how to customize your topology map.

Views

All of the user-created views are migrated to DCFM during the upgrade process. However, there may be some views that do not display as expected. For example, views in EFCM can be grouped by many different fields (labels), such as location, enclosure, vendor, and so on. However in DCFM, views can be grouped only by fabric.

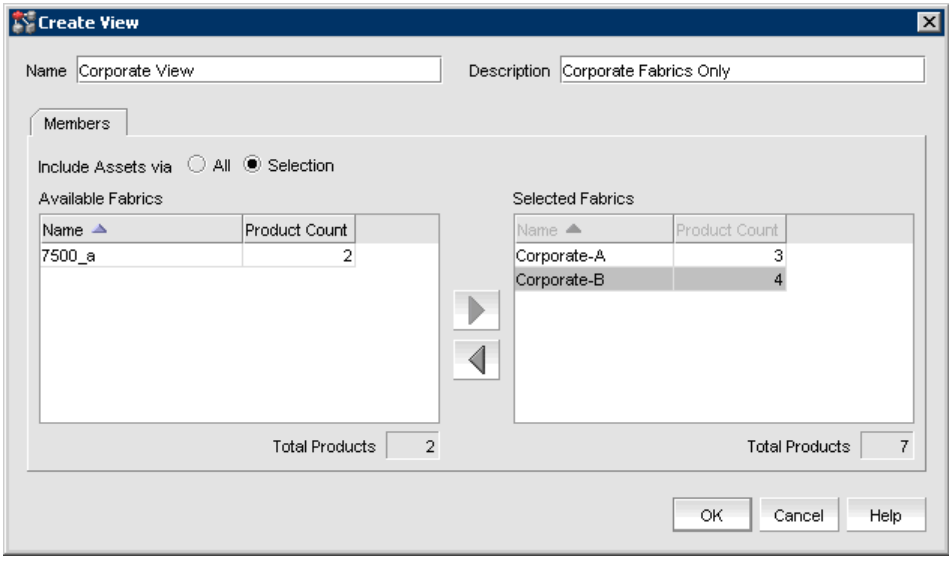


Figure 7. Create Views dialog box

Instructions to create customized views can be found in the "View Management" section of the *Brocade DCFM Enterprise User's Manual*.

One of the most common uses of views was to group all of the HBAs together for a single server. A better way to achieve this grouping is to use the Server Port Mapping feature, which performs the same function. Right-click an HBA to initiate the HBA Server Mapping dialog box, shown in Figure 8.

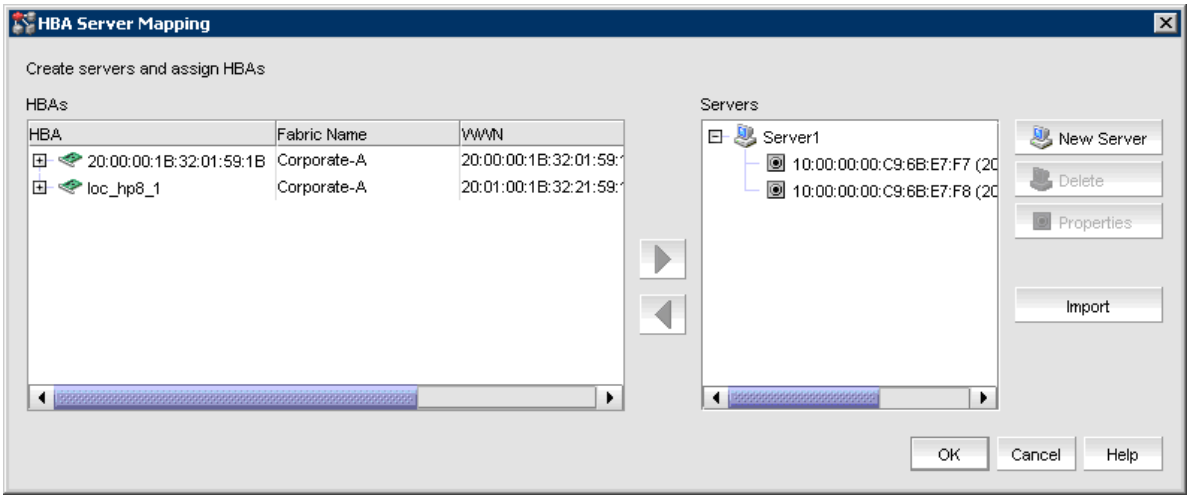


Figure 8. HBA Server Mapping dialog box

NOTE: In EFCM, ports from multiple fabrics could participate in a group, whereas in DCFM, only ports from a single fabric can participate in a group.

INSTALLATION AND DEPLOYMENT

Installing the Remote Client

With EFCM there were two methods to install the client application:

1) Install the client using the application CD.

2) Download and install the client from the EFCM server's Web site.

The DCFM client is now a Web start application launched from the DCFM server; type the IP address of the DCFM server in the browser window.

NOTE: If SSL was selected during the installation, you will need to use HTTPS:// to access the DCFM Web site, shown in Figure 9.

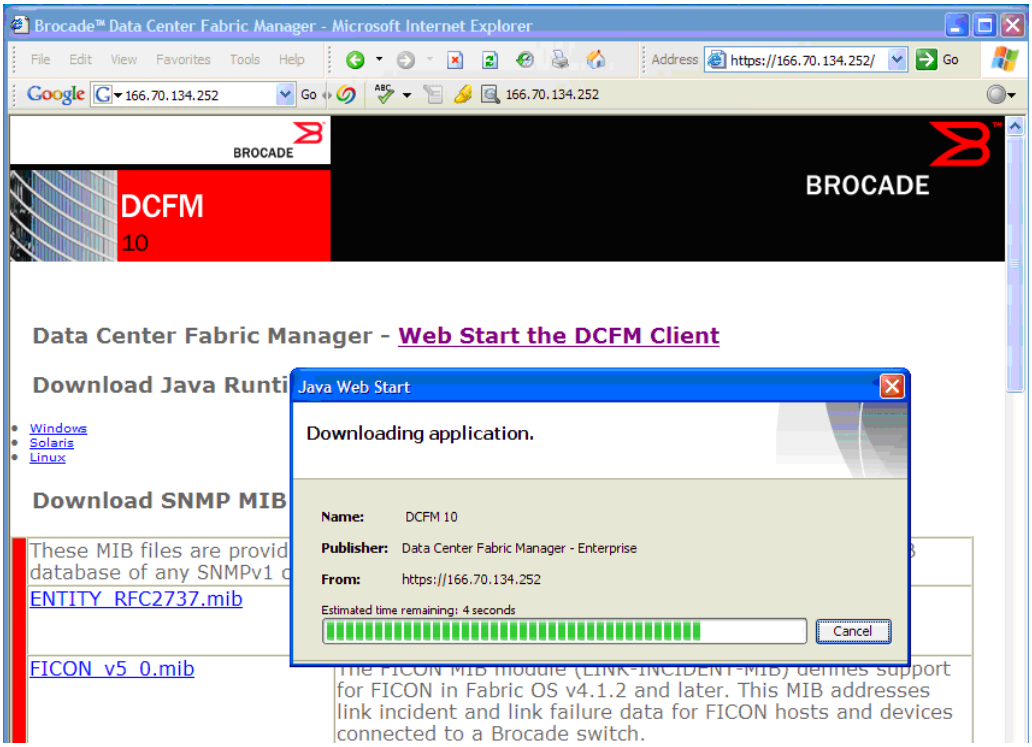


Figure 9. The DCFM Web site

You can change the SSL and port settings after the installation by going to **SAN > Options > Server Port**, as shown in Figure 10. (In EFCM, these settings were under Server Connections.)

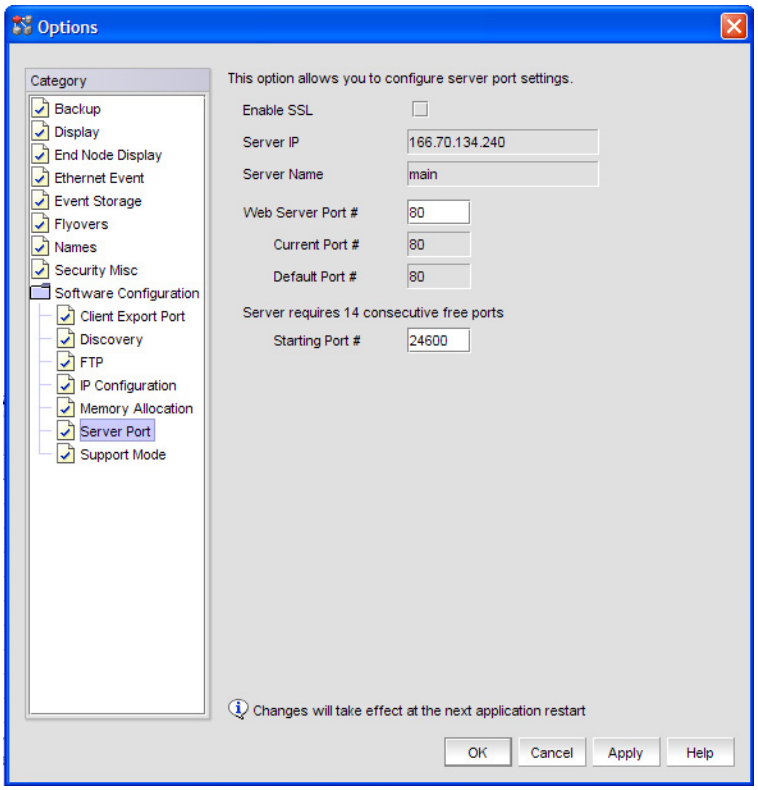
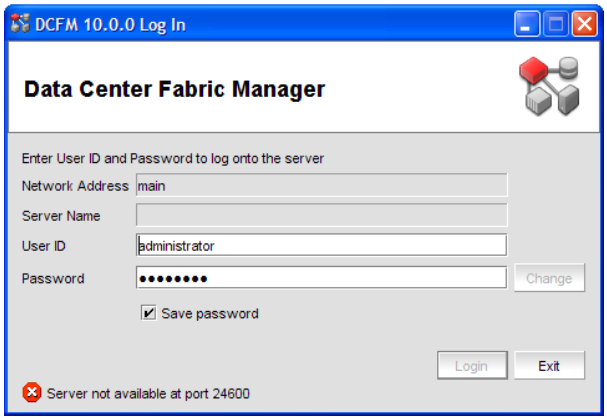


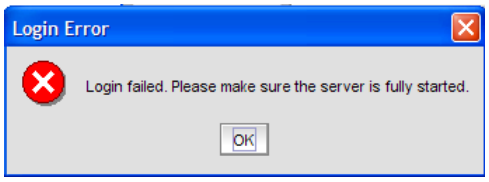
Figure 10. SAN Options dialog box

- If SSL is changed after the Web Start client has been installed, the DCFM client link that is created in the Start Menu, will no longer function. This is because the network address is embedded in the link with HTTP or HTTPS. That also means if the network address changes the link will fail.
- If you go from no SSL to enabling SSL, a "Server not available" message is displayed when you launch DCFM from the Start Menu:



To correct this you need to reinitiate the "Web Start the DCFM Client" from the DFCM Web page, which reinstalls the client and fixes the link.

- If SSL was enabled and you disable SSL, a “Login Error” message is displayed when you launch DCFM from the Start Menu:



  To correct this you need to delete the link, clear out the Java cache and reinitiate the “Web Start the DCFM Client” from the DFCM Web page. This will reinstall the client and add the correct link.

If you encounter these errors, you can always reach the client via the Web Start until you can fix the problem.

Running the Client

Launch the DCFM client by either using the Start Menu link or using “Web Start the DCFM Client” from the DCFM Web page. This displays the login screen, which is very similar to the EFCM client login screen. The two differences are the Network Address is now hard coded in and the setup button is missing. The options that were under the setup button can be changed from inside DFCM which is a more logical place to make the changes.

The default user name and password have also remained the same, Administrator and password. User names are no longer case sensitive but passwords continue to be case sensitive.

In some cases, a network may use virtual private network (VPN) or firewall technology, which can prohibit communication between servers and clients. In other words, a client can find a server, appear to log in, but is immediately logged out because the server cannot reach the client. To resolve this issue, the ports in the table below need to be opened up in the firewall.

The DCFM remote client application will run on Microsoft Windows 2000 or on Microsoft Windows 2003 or on Microsoft Windows XP Professional Service Pack 2 or later. If the patches have been applied, click the following button to begin the installation process. You will receive a Java Security warning requesting permission to download and start the installer program, and to read and write files on your system. You must grant these permissions to allow installation of the DCFM client application.

Importing Names

To import names (previously nicknames in EFCM), choose **Configure > Names** to display the Configure Names dialog box, shown in Figure 11. Click **Import** to display the Import Files dialog box, browse to the location of the CSV file, and follow onscreen instructions.

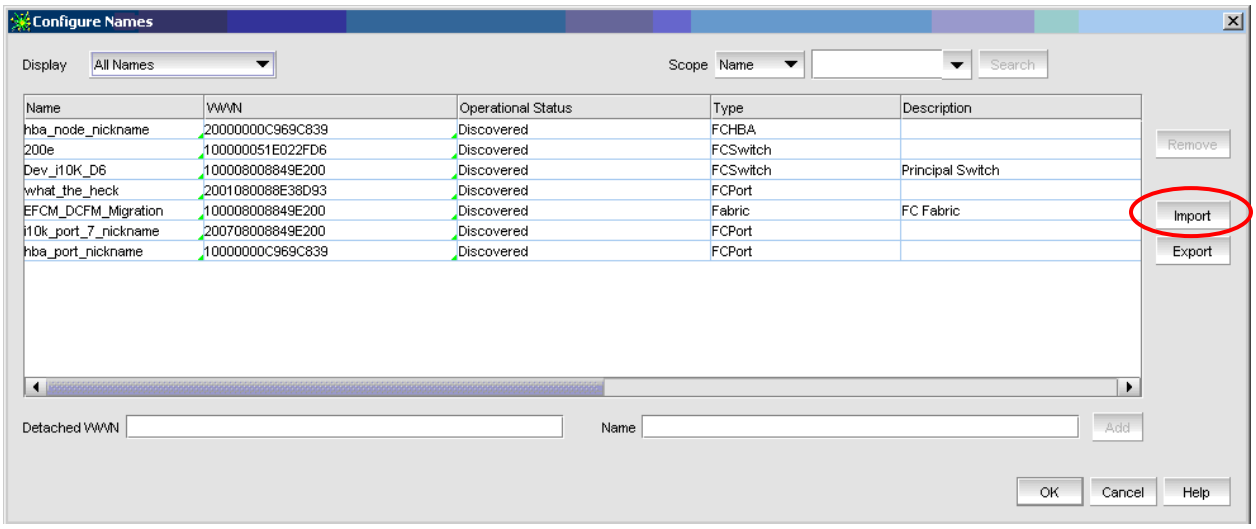


Figure 11. Configure Names dialog box

NOTE: If you have nicknames that are greater than 128 characters in length, they are truncated at 128 characters during data migration.

POST-DEPLOYMENT CONFIGURATION

Discovery of Environment

First display the Discovery dialog box by choosing **Discovery > Setup**. You can also use the Setup icon on the main toolbar. The RBAC Discovery permission controls access to displaying this dialog box and all its functions.

If you want to know if a switch has been discovered or not, use the switch's Properties dialog box.

Missing Switches

If a fabric has been discovered and some of its switches segment out into single or multiple new fabrics, you can now easily rediscover those new fabrics in the Discover Setup window without entering their credentials.

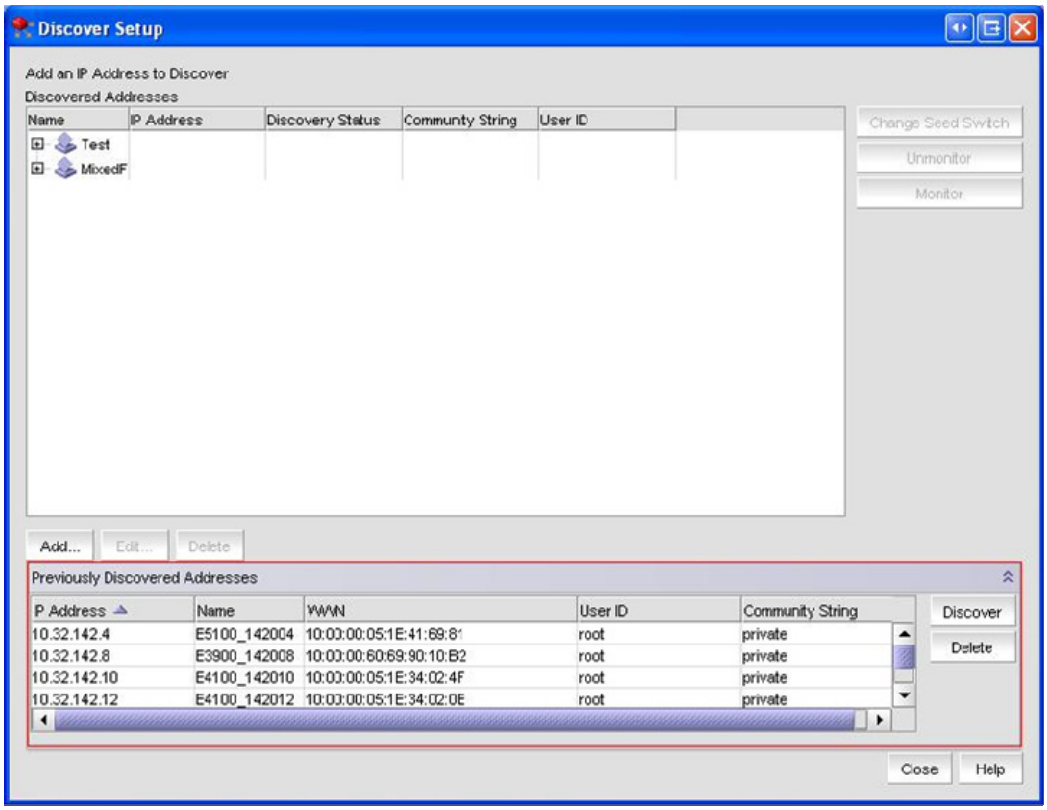


Figure 12. Discover Setup window

Validation Testing

The main way to ensure that data has been migrated from Brocade EFCM to DCFM correctly is to look at the data in DCFM. For example, check the following types of data:

- Zones
- Topology displays that you've customized (see also "Topology Maps" section earlier in this document)
- Role-Based Access Control (RBAC) data
- User list
- Names (see also "Names" section earlier in this document)
- ROV/TOV setting

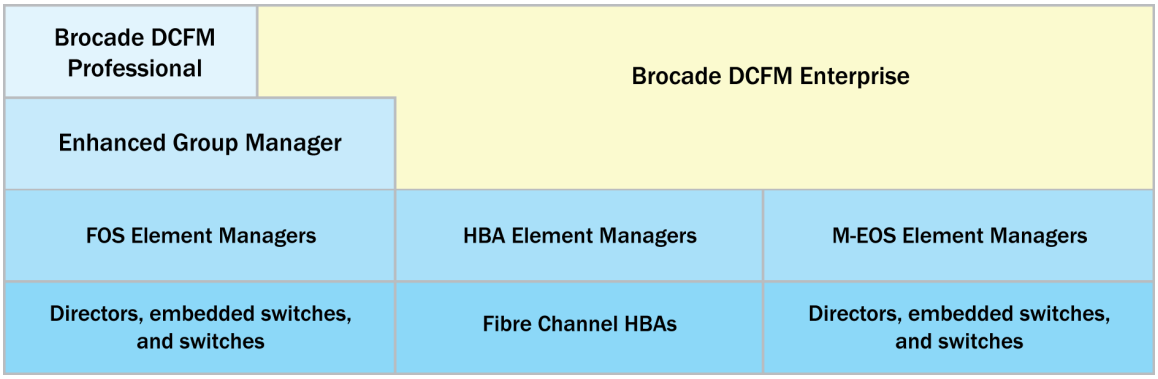
TROUBLESHOOTING

1) Click the Technical Support Information tab.
2) In the text field, specify the path to save the DCFM server technical support information to.
3) Click **Capture** to gather all the information, and then click **Close**.

APPENDIX A: BROCADE FABRIC MANAGEMENT PRODUCT FAMILY

(This information is available in several other documents, but as a convenience, it is added here too.)

Brocade DCFM manages both FOS fabrics and mixed FOS/M-EOS fabrics with product-specific element managers and enhanced group management functions. The DCFM architecture integrates the best management features of EFCM and Fabric Manager; it is based on the EFCM Graphical User Interface (GUI) and Fabric Manager messaging and data management design for improved performance and scalability.



Brocade DCFM is available as two different products—DCFM Professional and DCFM Enterprise.

Brocade DCFM Professional is targeted at customers seeking a less extensive management solution for smaller SANs. This software is included with Brocade switches and allows management of a single FOS fabric (up to a 1,000 switch ports) at a time. It performs group switch management beyond the scope of Brocade Web Tools

DCFM Professional is available with the purchase of any Brocade switch and is also available for download via the Brocade corporate Web. A seamless migration path is available from DCFM Professional to DCFM Enterprise.

Brocade DCFM Enterprise is an enterprise-class product targeted at customers that demand a management software solution with comprehensive support for:

- Brocade DCX Backbone-based Data Center Fabric (DCF)
- Fabric-based encryption support for data-at-rest solutions
- Unified manageability of the data center fabric from HBA ports through switch ports to storage ports

DCFM Enterprise provides a holistic view of up to 24 fabrics and the connected devices, whether local to the data center or geographically dispersed. Policy-based management enables IT organizations to meet their Service Level Agreements (SLAs). It provides unparalleled scalability and performance over existing Brocade management products. DCFM Enterprise provides multi-protocol networking support for:

- Fibre Channel
- Fiber Connectivity (FICON)
- Fibre Channel over IP (FCIP)
- Fibre Channel Routing (FCR)
- Internet SCSI (iSCSI)
- (Future) Fibre Channel over Ethernet (FCoE) and Converged Enhanced Ethernet (CEE)

APPENDIX B: INTEGRATION WITH PARTNER MANAGEMENT FRAMEWORKS

(This information is available in several other documents, but as a convenience, it is added here too.) Brocade DCFM is designed with open standards interfaces to simplify integration with management frameworks supplied by server, storage, and infrastructure management partners. The DCFM open standards architecture has the following characteristics:

- Simplifies partner integration using open standard interfaces (SNMP, SMI-S)
- Improves customer management of virtualized resources (server, fabric, storage)
- Reduces management complexity of virtualized data centers
- Improves administrator productivity, so that human resources scale efficiently with the growth of storage and virtual server workloads

DCFM provides integrated data path management for server networks, multi-protocol data center fabrics, and heterogeneous storage environments. Its open interfaces simplify partner management integration, anticipating the evolution of infrastructure management from physical switch management to policy-based service management, essential for cost-effective, scalable management of virtual data centers. To ensure that all of this works together seamlessly, we have architected the appropriate integration hooks into the code right from the beginning.