NETWORK MANAGEMENT

Migrating from Brocade Data Center Fabric Manager to Brocade Network Advisor

Brocade Network Advisor continues Brocade leadership in network management with a unified SAN/IP network management software platform. It integrates the SAN management capabilities of Brocade Data Center Fabric Manager (DCFM) and the IP network management capabilities of Brocade IronView Network Manager (INM).

BROCADE

CONTENTS

INTRODUCTION

Brocade® Network Advisor 11.0 is a new software management platform that unifies network management for SAN, IP, and converged networks. It provides users with a consistent user interface across Fibre Channel (FC), IP, and Fibre Channel over Ethernet (FCoE) / Data Center Bridging (DCB) along with custom views and controls based on users' areas of specialization. Network Advisor provides users with the utmost flexibility in deployment and operational models, including traditional SAN deployments (FC, iSCSI, and NAS), traditional Ethernet deployments (Access/Aggregation/Core) and end-to-end convergence (FCoE, iSCSI, and NAS over DCB).

Network Advisor's comprehensive data center SAN fabric management features include configuring, monitoring, and managing the Brocade DCX® Backbone and Brocade directors, routers, switches, Host Bus Adapters (HBAs), and Converged Network Adapters (CNAs). Network Advisor also helps organizations discover, monitor, and manage converged FCoE network environments. In addition, Network Advisor provides comprehensive Layer 2 configuration, with easy-to-use Data Center Bridging (DCB) interface administration, FCoE port and trunk configurations, and Quality of Service (QoS).

Audience

This document provides Brocade customers who are currently using Brocade Data Center Fabric Manager (DCFM®) with information about migrating to Brocade Network Advisor. It is not intended as a definitive technical reference, but it provides guidelines for installing or upgrading to Network Advisor for field engineers or IT personnel.

Documentation

For details about how to install, configure, and deploy Network Advisor, ensure that you have access to the product documentation, which can be downloaded from MyBrocade.

NOTE: Brocade Network Advisor manuals describe features for all versions, Professional, Professional Plus, and Enterprise. Features not supported in a particular version are noted in the document.

- *Brocade Network Advisor SAN User Manual.* Describes only the SAN part of Network Advisor for customers who want to use Network Advisor to manage their SAN only
- *Brocade Network Advisor IP User Manual.* Describes only the IP part of Network Advisor for customers who want to use Network Advisor to manage their IP network only
- *Brocade Network Advisor SAN + IP User Manual.* For customers who want to use Network Advisor to manage both their SAN and IP networks
- *Brocade Network Advisor Installation Guide.* Describes how to install Network Advisor (SAN, IP, and SAN + IP versions) and SMI Agent (SAN and SAN + IP versions only)
- *Brocade Network Advisor Migration Guide.* Describes how Network Advisor is different from Brocade INM for customers who are migrating from Brocade INM; note that there is no comparable Migration Guide for customers who are migrating from Brocade DCFM simply because the interface is very similar and if you are familiar with DCFM you will find it an easy transition to Network Advisor
- *Brocade Network Advisor Release Notes.* Of course, you should always read the Release Notes for this and all subsequent versions of Network Advisor!

And other Brocade papers:

- *Brocade Network Advisor Features Brief for Data Center Networks*
- *Brocade Network Advisor Features Brief for IP Networks*
- *Brocade Network Advisor Data Sheet*

Migration Overview

Supported Firmware

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

NOTE: Although you do not have to install or know the Java version used because it is bundled with Brocade Network Advisor, development was conducted using Java JRE 1.6.0_21.

Upgrade Paths

Brocade Network Advisor provides a non-disruptive path and functional continuity for organizations upgrading from Brocade DCFM without losing data and configuration settings. It might be helpful for you to know that Brocade Network Advisor 11.0 is based on the functionality and user interface from Brocade DCFM 10.4. So if you've been using DCFM 10.4, you won't experience a steep learning curve when you migrate to Brocade Network Advisor 11.0.

The following table details the supported upgrade paths.

Current Version	**Network Advisor for SAN Professional**	**Network Advisor Trial Version**		**Network Advisor Production License Version**	
		SAN Professional Plus	**SAN Enterprise**	**SAN Professional Plus**	**SAN Enterprise**
DCFM 10.3.x/10.4.x Professional	Yes	Yes	Yes	Yes	Yes
DCFM 10.3.x/10.4.x Professional Plus Trial version	No	Yes	Yes	Yes	Yes
DCFM 10.3.x/10.4.x Professional Plus	No	No	No	Yes	Yes
DCFM 10.3.x/10.4.x Enterprise Trial version	No	No	Yes	No	Yes
DCFM 10.3.x/10.4.x Enterprise	No	No	No	No	Yes
Network Advisor 11.0.x Professional	Yes	Yes	Yes	Yes	Yes
Network Advisor 11.0.x Professional Plus Trial version	No	Yes	Yes	Yes	Yes
Network Advisor 11.0.x Professional Plus	No	No	No	Yes	Yes
Network Advisor 11.0.x Enterprise Trail version	No	No	Yes	No	Yes
Network Advisor 11.0.x Enterprise	No	No	No	No	Yes

NOTE: If you want to migrate from Brocade EFCM, Fabric Manager (FM), or DCFM 10.0.x/10.1.x to Network Advisor 11.0.0, you first have to migrate from EFCM/FM/DCFM 10.0.x to DCFM 10.3.x and DCFM 10.1.x to 10.4.x—and then migrate to Network Advisor 11.0.0.

The quickest and simplest method of moving from one edition to another is to enter the new license information in the Network Advisor License dialog box.

Migration Procedure

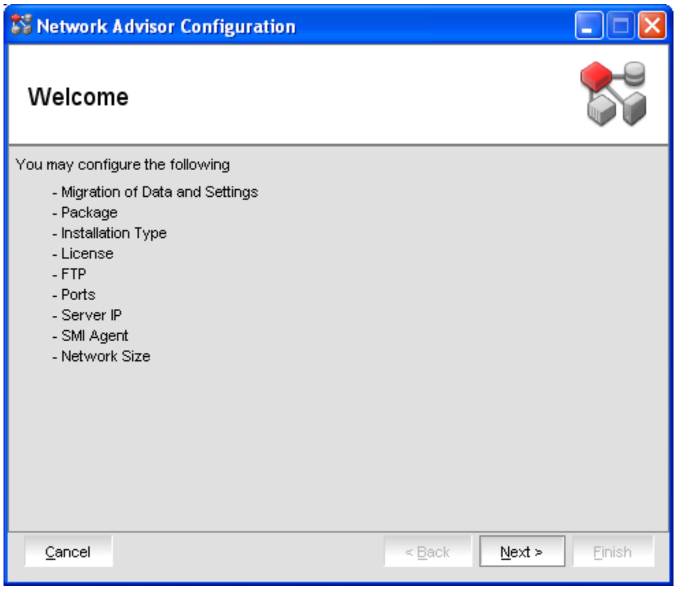
The migration is described in detail in the *Brocade Network Advisor Migration Guide*. For your convenience, this section lists high-level steps required for the migration in a Windows environment, including:

- Review the pre-migration requirements for your platform, making sure that:
    - A version of Brocade DCFM that meets migration requirements is installed on your server.
    - The fabric has FOS 5.0.x or EOS 9.6 or later running on all switches in the fabric.
    - You install Network Advisor on the same system as your current management application.

  NOTE: Ensure that all instances of the DCFM client are closed on the management server and on remote workstations.

- Insert the Network Advisor installation DVD into the DVD-ROM drive on a Windows or UNIX server and follow onscreen directions.

- Install Network Advisor and use the wizard to migrate data and settings (could take several minutes) and to perform other configuration tasks listed on the Welcome screen.



Network Advisor Configuration

Welcome

You may configure the following

- Migration of Data and Settings
- Package
- Installation Type
- License
- FTP
- Ports
- Server IP
- SMI Agent
- Network Size

- Start the Network Advisor server and client. Once all the Network Advisor services are started, you can log in. *You can use your Admin User ID and password from DCFM.*

DCFM 10.x license keys are forward compatible in Network Advisor 11.0. This means that DCFM 10.x license keys are migrated and considered as SAN-only license keys. Existing DCFM customers can upgrade to SAN + IP using a valid license key during migration or they can upgrade to SAN + IP at a later date by installing a new license key.

Below is a summary of the supported DCFM -> Network Advisor license migrations:

- DCFM Enterprise 10.3.x and 10.4.x licenses are migrated to Network Advisor for SAN Enterprise licenses.

- DCFM Professional Plus 10.3.x and 10.4.x licenses are migrated to Network Advisor for SAN Professional Plus or Enterprise licenses.

- DCFM Professional 10.3.x and 10.4.x licenses are migrated to Network Advisor for SAN Professional.

Migration Facts

- All DCFM data, including discovered fabrics, performance monitoring data, events, firmware images, etc. are migrated from DCFM to Network Advisor, except for the following:
  - Client login information (saved username and password and save password selection)
  - Client font size
  - Tools menu customizations
  - Client/Server communication ports

  When migrating from DCFM Professional or Professional Plus, these additional items will not be migrated to Network Advisor:
  - Polling interval and memory size customizations
  - SAN size setting
- Brocade Network Advisor for SAN Enterprise supports a combination of pure FOS, pure M-EOS, mixed FOS/M-EOS fabrics, and host/HBA management.
- Some differences from Brocade DCFM (discussed in more detail later) are:
  - Packaging of PostgreSQL database (in place of Sybase and Derby)
  - Role-Based Access Control (RBAC) enhancements
  - Authorization, Authentication, and Accounting (AAA) enhancements
  - Fault management enhancements
  - Customers upgrading to Brocade Network Advisor Enterprise are required to purchase a service agreement with a minimum one-year term.

Remote Client Launch

This section describes the shortcut menu upgrade from DCFM 10.3.x/10.4.x to Network Advisor 11.0.0 during remote client launch. Following are the steps to perform while doing the upgrade from DCFM 10.3.x/10.4.x to Network Advisor 11.0.0:

1) With DCFM 10.3.x/10.4.x installed on machine A, launch remote client from machine B. The shortcut menu is created with name DCFM 10.3.x/10.4.x.

2) Upgrade the server to Network Advisor 11.0.0 on machine A.

3) From machine B, launch the remote client in a browser window, NOT by clicking the DCFM 10.3.x/10.4.x shortcut menu icon. Another shortcut menu is created with the name Network Advisor 11.0.0.

4) If you want to remove the DCFM 10.3.x/10.4.x shortcut menu, right-click on the menu item and select Delete.

For details about migrating to DCFM 10.4, see the *Brocade DCFM Installation and Migration* Guide for version 10.4.x.

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 DCFM. Then decide 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 Network Advisor:

- Back up the Brocade DCFM server before starting the migration. To do this, open the Options dialog box from the DCFM client: 1) select **Server > Options** from the client menu bar, 2) select the **Server Backup** category on the left side of the Options dialog box, 3) enter a value in the **Output Directory** field (if needed) and click **Backup Now.**
- It is recommended that you capture Technical Support information for the switches in your fabrics. See "Technical Support Information" later in this document.
- The supported database in Network Advisor is PostgreSQL. See the "Databases" section later in this document for details.

Roles and Privileges

In both Network Advisor 11.0 and in DCFM, privileges are assigned to role and are not directly assigned to a user. However, in DCFM, users are assigned a single role, and in Network Advisor, users may be assigned multiple roles. Each role in turn can contain read-write privileges and read-only privileges. Default roles, their associated privileges, and consolidated privileges for Network Advisor are outlined in the product documentation.

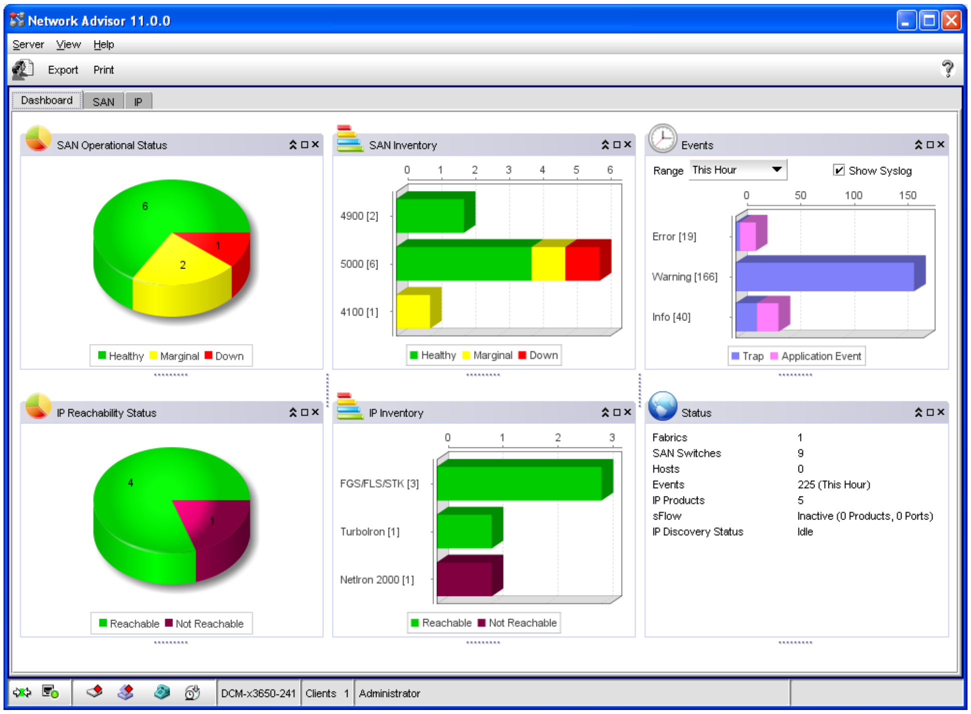
Firewall Considerations

Certain ports must be open between the Brocade Network Advisor client and server processes. Also other ports could optionally be exposed for other services via the intranet connection on the Network Advisor server, that is, SMI-S, SNMP, HTTP, SSL, telnet, SSH, and FTP. If a firewall is put between the Network Advisor server and the managed devices, investigate which ports must be opened and which are optional. Do not consider just day-to-day management, but also the services listed above.

For details, see the *Brocade Network Advisor User Manual*.

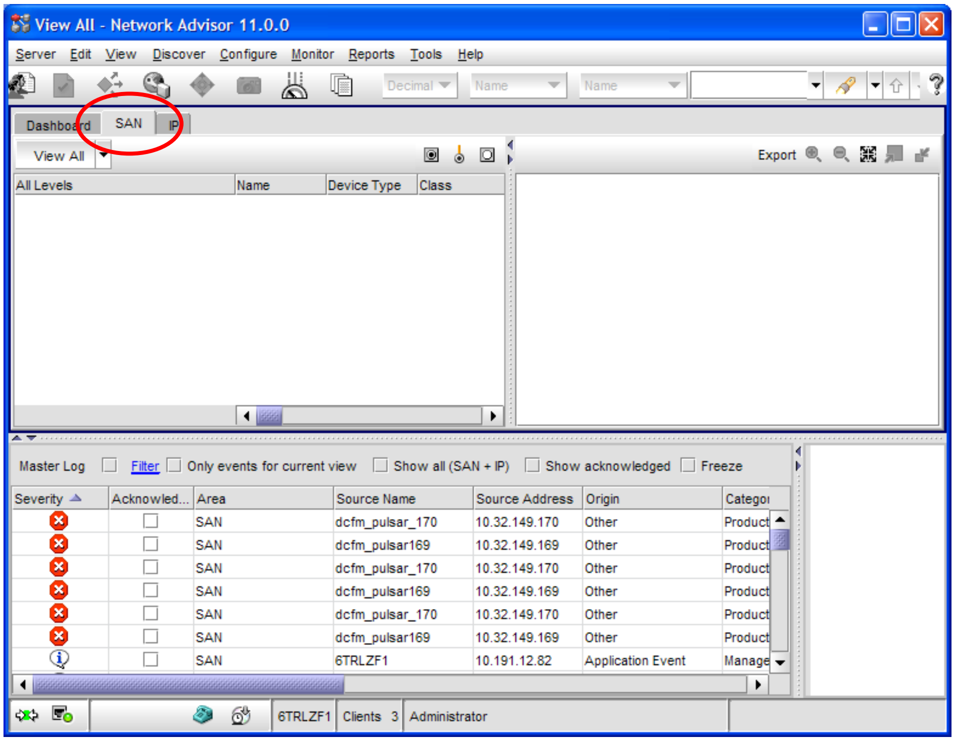
Client Interface

Users of DCFM will be familiar and comfortable with the Network Advisor interface as mentioned earlier. Figure 1 shows the Network Advisor main window—with Dashboard, SAN, and IP tabs. Display of the tabs is controlled by the active licensing option; the Dashboard tab is available in all options.



Fabrics	1
SAN Switches	9
Hosts	0
Events	225 (This Hour)
IP Products	5
sFlow	Inactive (0 Products, 0 Ports)
IP Discovery Status	Idle

Figure 1. Network Advisor main desktop with active SAN and IP licensing


View All - Network Advisor 11.0.0
Server Edit View Discover Configure Monitor Reports Tools Help
Decimal Name Name
Dashboard SAN IP
View All
Export
All Levels Name Device Type Class
Master Log Filter Only events for current view Show all (SAN + IP) Show acknowledged Freeze
6TRLZF1 Clients 3 Administrator

Severity	Acknowled...	Area	Source Name	Source Address	Origin	Categor
☒	□	SAN	dcfm_pulsar_170	10.32.149.170	Other	Product
☒	□	SAN	dcfm_pulsar169	10.32.149.169	Other	Product
☒	□	SAN	dcfm_pulsar_170	10.32.149.170	Other	Product
☒	□	SAN	dcfm_pulsar169	10.32.149.169	Other	Product
☒	□	SAN	dcfm_pulsar_170	10.32.149.170	Other	Product
☒	□	SAN	dcfm_pulsar169	10.32.149.169	Other	Product
ⓘ	□	SAN	6TRLZF1	10.191.12.82	Application Event	Manage

Figure 2: SAN tab in the View All window

Differences to Note

The feature/function differences between DCFM and Network Advisor mentioned earlier are discussed briefly below.

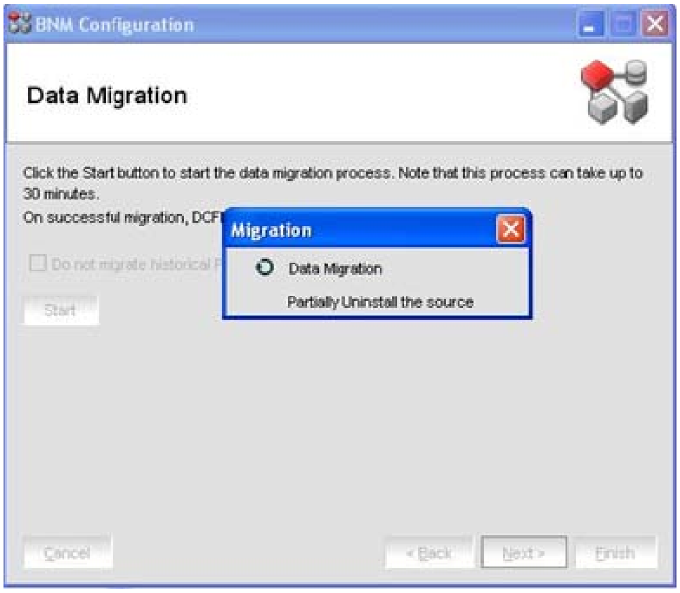
Databases

The path of migrating data and settings from source to destination happen through the Network Advisor 11.0 installer. The configuration wizard auto-detects any earlier installed version path for migration and the installation directory is checked for credentials such as supported version. Once validation is successfully completed, data migration starts.

The prerequisites for database migration from DCFM 10.3.x/10.4.x to Network Advisor 11.0 are:

- Both source and target should be installed on the same system.
- Service of the source version should be running.
- Both remote and local client of source application should be shut down before migration.

Note that you can click the “Do not migrate historical performance data” check box for a faster data migration process and smaller database migrated (check box is shown grayed out in Figure 3).



Click the Start button to start the data migration process. Note that this process can take up to 30 minutes.

On successful migration, DCF

□ Do not migrate historical P

○ Data Migration

Partially Uninstall the source

Figure 3. Data Migration screen in the configuration wizard, showing the progress dialog box

Migration continues even if a minor error occurs, whereas it is aborted if a major error occurs. In either case, errors are logged in a log file located in `<installation dir>/logs/cw.log`. If the migration failed due to a major error, an error dialog is displayed. On successful completion of migration process, a confirmation dialog is displayed in progress dialog of the configuration wizard.

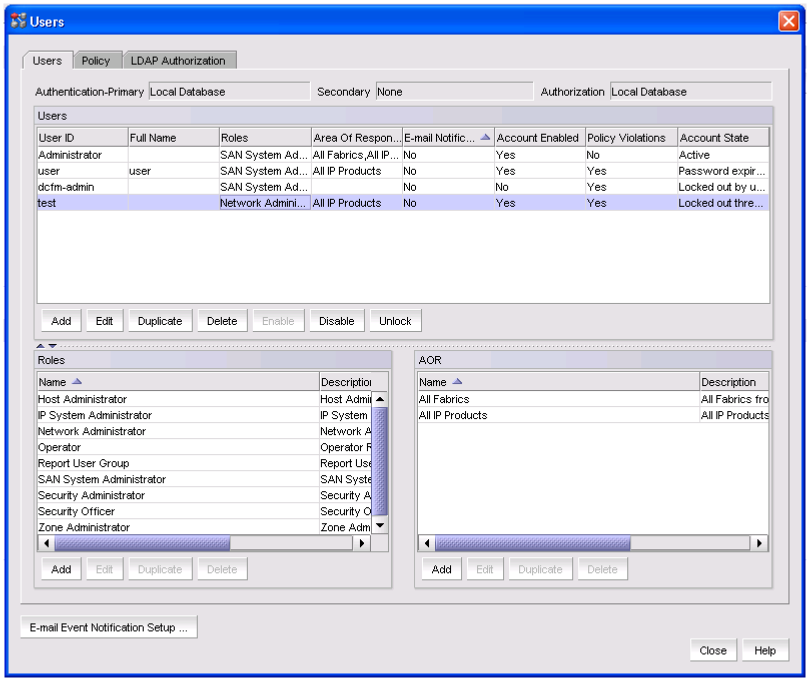
After migration, DCFM 10.3.x/10.4x is partially uninstalled; even if an older version of DCFM is installed on the same machine and you choose not to migrate, legacy DCFM is partially uninstalled on the machine. You can recover DCFM 10.3.x/10.4.x after the migration if you choose to. Consult product documentation for details.

Role-Based Access Control (RBAC)

RBAC, although present in DCFM, is enhanced in Network Advisor in the following areas:

- Unified User Management for IP and SAN environments

  As in DCFM, the user management interface is launched via the Users menu option. In Network Advisor, the Users menu is relocated to the Server menu. Note that the Users menu option is available only for users with the User Management privilege and Read-Only or Read-Write permissions. The Users window has three tabs: Users, Policy, and LDAP Authorization (see Figure 4).



Authentication-Primary: Local Database
Secondary: None
Authorization: Local Database

Users

User ID	Full Name	Roles	Area Of Respon...	E-mail Notific...	Account Enabled	Policy Violations	Account State
Administrator		SAN System Ad...	All Fabrics,All IP...	No	Yes	No	Active
user	user	SAN System Ad...	All IP Products	No	Yes	Yes	Password expir...
dcfm-admin		SAN System Ad...		No	No	Yes	Locked out by u...
test		Network Admini...	All IP Products	No	Yes	Yes	Locked out thre...

Roles

Name	Descriptio
Host Administrator	Host Admi
IP System Administrator	IP System
Network Administrator	Network A
Operator	Operator F
Report User Group	Report Use
SAN System Administrator	SAN Syste
Security Administrator	Security A
Security Officer	Security O
Zone Administrator	Zone Adm

AOR

Name	Description
All Fabrics	All Fabrics fro
All IP Products	All IP Products

Figure 4. Users tab in Users window

- Area Of Responsibility (AOR)

  An AOR Manager allows users to place fabrics, hosts, products, product groups, and port groups in management groups, which can then be assigned to Network Advisor users. Users can manage only the management groups assigned to them. What was called the "resource group" in DCFM is now called the area of responsibility in Network Advisor, and is one of the entities used in defining Network Advisor RBAC. The AOR can contain IP products in addition to all types of SAN products that were assigned to the resource group in DCFM. All available AORs are listed in the AOR table at the bottom right of the Users tab in the Users window (see Figure 4).

- Role /Privilege Management

  All available roles are listed in the Roles table at the bottom left of the Users tab in the Users window (see Figure 4). The Roles table has the following default roles (in addition to user-defined roles) for SAN:

  - SAN System Administrator
  - Network Administrator
  - Security Administrator
  - Zone Administrator

- Operator
- Security Officer
- Host Administrator

In a SAN + IP environment, the system roles are:

- SAN System Administrator
- IP System Administrator
- Network Administrator
- Security Administrator
- Zone Administrator
- Operator
- Security Officer
- Host Administrator
- Report User Group

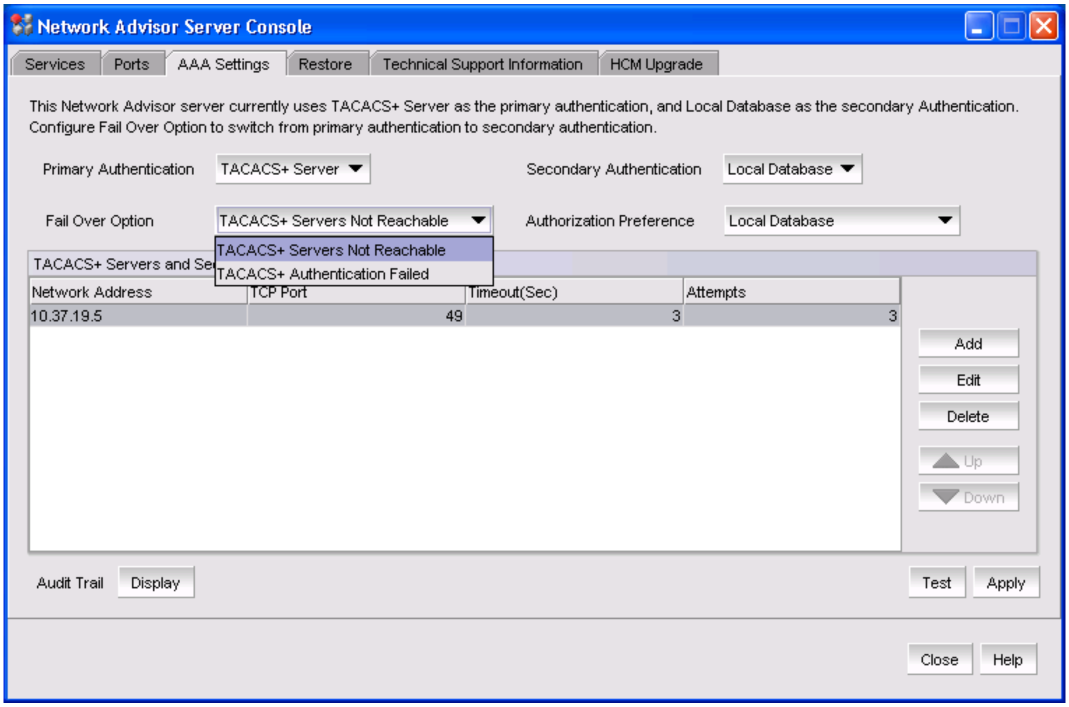
The DCFM default role System Administrator is replaced with SAN System Administrator in Network Advisor 11.0.

- User Account/Role/Resource Group migration
  - Users without roles or resource groups are migrated—however they will have only SAN permissions; IP permissions will need to be added explicitly. All migrated users will have an active state.

    NOTE: IP permissions will be added to roles with “User Management” read-write permissions enabled.
  - After migration, the equal sign (=) in role names will be replaced with the underscore character (_).
  - If any user-defined role is matched with any newly introduced system role in Network Advisor, then it is migrated with name <Role Name>_<Integer Value>_Migrated. The <Integer Value> generated is a random value. If DCFM had a role with the name <Role Name> and the <Role Name> text matches any of the newly introduced default Network Advisor roles, then the respective role is migrated with same name.
  - All resource groups are migrated to AORs; resource groups without any members are migrated as empty AORs. The system resource group, All Fabrics, is migrated. Users assigned to resource groups are migrated.
  - After migration, the equal sign (=) in resource group names will be replaced with the underscore character (_).
  - If any user-defined resource group is matched with any newly introduced system AOR in Network Advisor, then it is migrated with name <Resource Group Name>_<Integer Value>_Migrated. The <Integer Value> generated is a random value. If DCFM had a resource group with the name <Resource Group Name> and the <Resource Group Name> text matches any of the newly introduced default Network Advisor AORs, then the respective resource group is migrated with same name.
  - All members (fabrics and hosts) of migrated resource groups are also migrated.

Authorization, Authentication & Accounting (AAA)

DCFM allows client-to-server authentication through local user accounts or external servers and the authorization is entirely based on local mapping; in Network Advisor, authorization and authentication are optionally externalized. Accounting is still not externalized and referenced from locally available information. Network Advisor provides options for primarily authenticating user accounts against Terminal Access Controller Access-Control System Plus (TACACS+) servers configured externally on server host machines or other hosts reachable from the Network Advisor server. Authentication with TACAcs+, RADIUS, LDAP, and Switch is supported on Windows and Linux platforms. Authentication with Windows domain is supported only on Windows; authentication with an NIS/Password file is supported only on Linux platforms. The tab Authentication is replaced by the name AAA Settings, as shown in Figure 5.



This Network Advisor server currently uses TACACS+ Server as the primary authentication, and Local Database as the secondary Authentication. Configure Fail Over Option to switch from primary authentication to secondary authentication.

Primary Authentication: TACACS+ Server
Secondary Authentication: Local Database
Fail Over Option: TACACS+ Servers Not Reachable
Authorization Preference: Local Database

Network Address	TCP Port	Timeout(Sec)	Attempts
10.37.19.5	49	3	3

Figure 5. AAA Settings tab in the Network Advisor Server Console

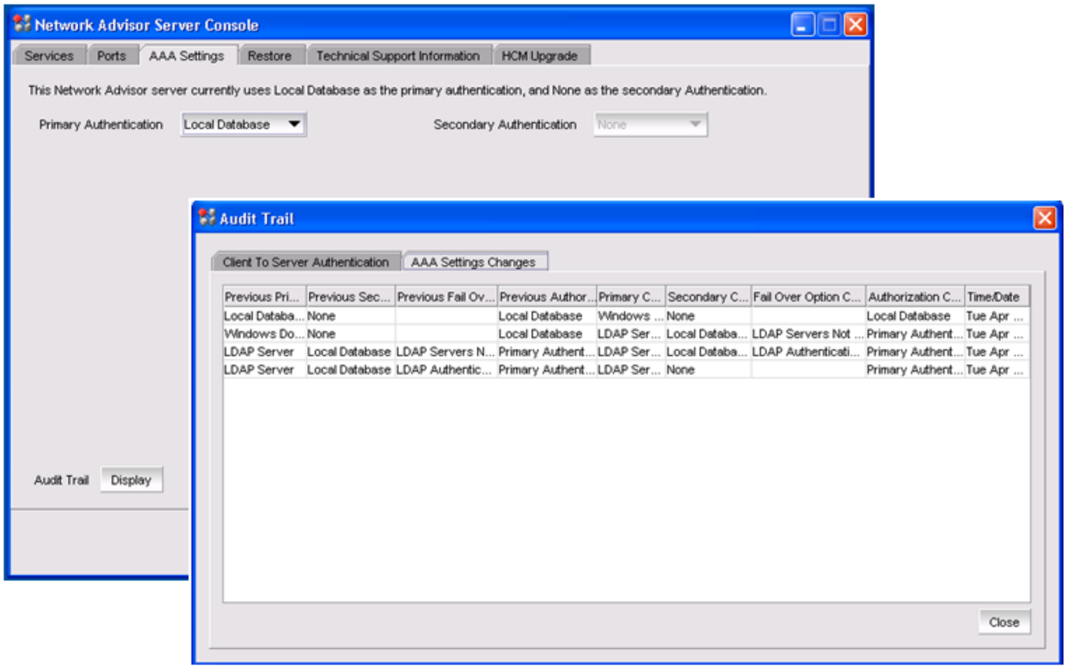
Maintaining DCFM behavior, configuring a local database as a secondary authentication, or failover, is applicable for RADIUS, LDAP, and Switch. Network Advisor 11.0 also supports a local database or none as secondary authentication for TACACS+ servers. In the case of an LDAP server, in addition to “Server not reachable,” one more failover option, “User not found in LDAP,” is addressed.

In Network Advisor, one more failover option, “<RADIUS/TACACS+/LDAP> Authentication Failed,” is introduced for RADIUS, TACACS+, and LDAP servers. Users can configure TACACS+ and RADIUS servers to perform failover to the local database when:

- The <TACACS+/RADIUS> server is not reachable
- <TACACS+/RADIUS> authentication fails

DCFM supports authorization by maintaining configurations in a local database. Network Advisor allows user to authorize with external servers as an option by setting necessary parameters in external servers. Authorization via external server is turned off by default. Authorization via an external server is turned on by setting the Authorization Preference option to Primary Authentication Server.

Enhancements to the audit trail have been added in Network Advisor. As shown in Figure 6, the Authentication Audit Trail (Display) has been renamed Audit Trail (Display) and the Audit Trail dialog box also displays authorization settings for audit purposes. In the Audit Trail window, the Authentication Settings Changes tab has been renamed AAA Settings Changes and the four new columns have been added.



Network Advisor Server Console

This Network Advisor server currently uses Local Database as the primary authentication, and None as the secondary Authentication.

Primary Authentication: Local Database

Secondary Authentication: None

Audit Trail: Display

Audit Trail

Previous Pri...	Previous Sec...	Previous Fail Ov...	Previous Author...	Primary C...	Secondary C...	Fail Over Option C...	Authorization C...	Time/Date
Local Databa...	None		Local Database	Windows ...	None		Local Database	Tue Apr ...
Windows Do...	None		Local Database	LDAP Ser...	Local Databa...	LDAP Servers Not ...	Primary Authent...	Tue Apr ...
LDAP Server	Local Database	LDAP Servers N...	Primary Authent...	LDAP Ser...	Local Databa...	LDAP Authenticati...	Primary Authent...	Tue Apr ...
LDAP Server	Local Database	LDAP Authentic...	Primary Authent...	LDAP Ser...	None		Primary Authent...	Tue Apr ...

Figure 6. AAA Settings tab in the Network Advisor Server Console and the Audit Trail window

Accounting behavior in Network Advisor is the same as it is in DCFM, that is, user actions are accounted as part of application events/internal events. An event is triggered during user authentication and for any application-specific operations. The application events raised by various modules are the way of accounting for user actions in Network Advisor. RBAC does not mandate any such events and it is up to the modules to decide which events to trigger. All accounting-related information is referenced from the Network Advisor local database and not from any configured external server.

In DCFM, security is not enforced nor is there any provision to enforce security in communication between the DCFM and LDAP servers. In order to integrate security between the Network Advisor server and LDAP server, you can enable or disable security while adding or editing a particular LDAP server. The underlying standards used for securing communication are SASL using GSSAPI and TLS is supported. By default the security configuration is disabled. When security is enabled, communication is through the secured channel, however Network Advisor does not perform host name verification and certificate management from Network Advisor is not supported. Network Advisor allows user to configure the authentication protocol between the Network Advisor and LDAP servers. The supported protocols for authentication are MD5 (the default) and Kerberos.

Fault Management

Network Advisor uses the following protocols to communicate to the device being managed to get fault information from both IP and SAN switches:

- Simple Network Management Protocol (SNMP)
- Network Management Request/Response Unit (NMRU) for M-EOS switches
- Network Advisor receives events from managed devices via the following protocols: SNMP traps, Syslog, and NMRU for M-EOS switches.

Master Log

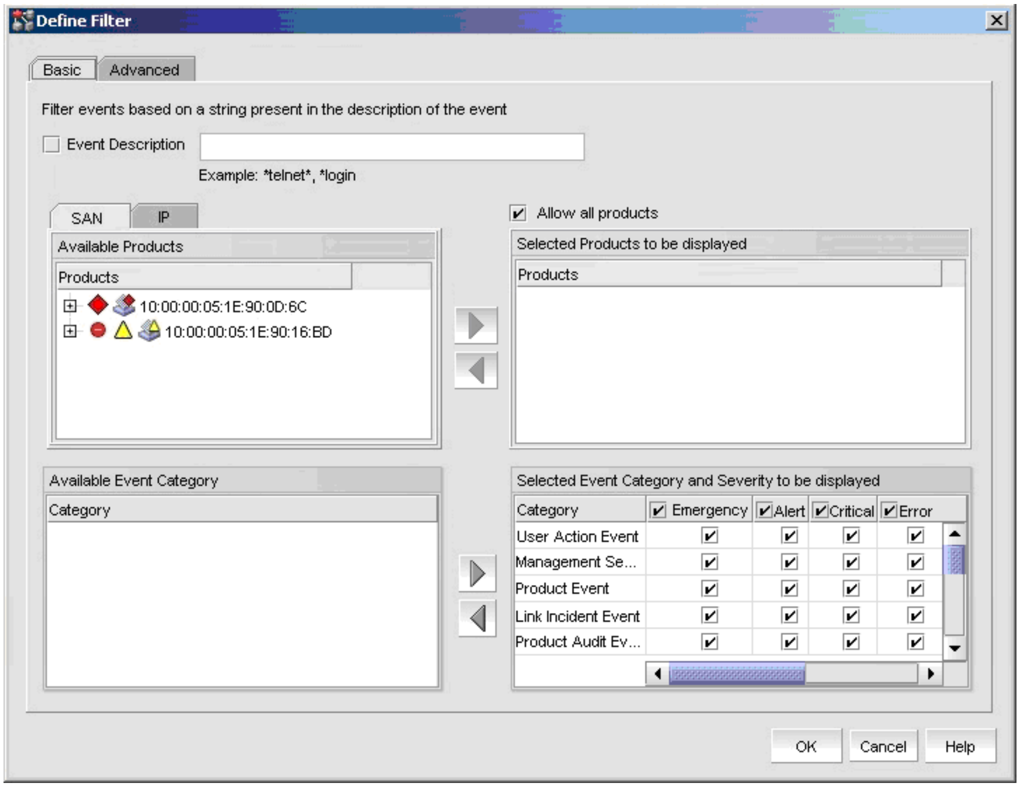
The Master Log displays both IP and SAN events based on the current context (an option to view both SAN and IP events irrespective of the current context is also provided) and no user privileges are required. Events listed are limited to the user's AoR. In Network Advisor, the following features are added to the features from DCFM (only the Pagination feature has been removed):

- User acknowledgement of events
- Show/Hide acknowledged events
- Freezing auto-scrolling of the Master Log
- Events shown are limited to the user's AOR
- Location of the device corresponding to the selected event
- Syslog shown by default for IP devices in the Master Log

The following DCFM right-click menu options have been removed: Hide All, Hide Selection, and Show, E-mail -> Date. The following right-click menu options have been added: Acknowledge, Unacknowledge, and Locate. The Display Details right-click menu option has been renamed Properties.

Filtering

Filters are migrated; the event filters that are configured in a SAN-only installation needs to be modified when upgrading to a SAN + IP installation to include the IP products; otherwise the IP events are not shown. Basic filtering combines the basic filtering options from INM and DCFM. By default basic filtering includes all the products, the entire category and severity, and no filtering on event description. The filter specified is user specific. Based on the license, the SAN or IP or SAN and IP tabs are available in the Define Filter dialog box, the SAN version is shown in Figure 7.



Filter events based on a string present in the description of the event

□ Event Description

Example: *telnet*, *login

☑ Allow all products

Available Products

Products

10:00:00:05:1E:90:0D:6C

10:00:00:05:1E:90:16:BD

Selected Products to be displayed

Products

Available Event Category

Category

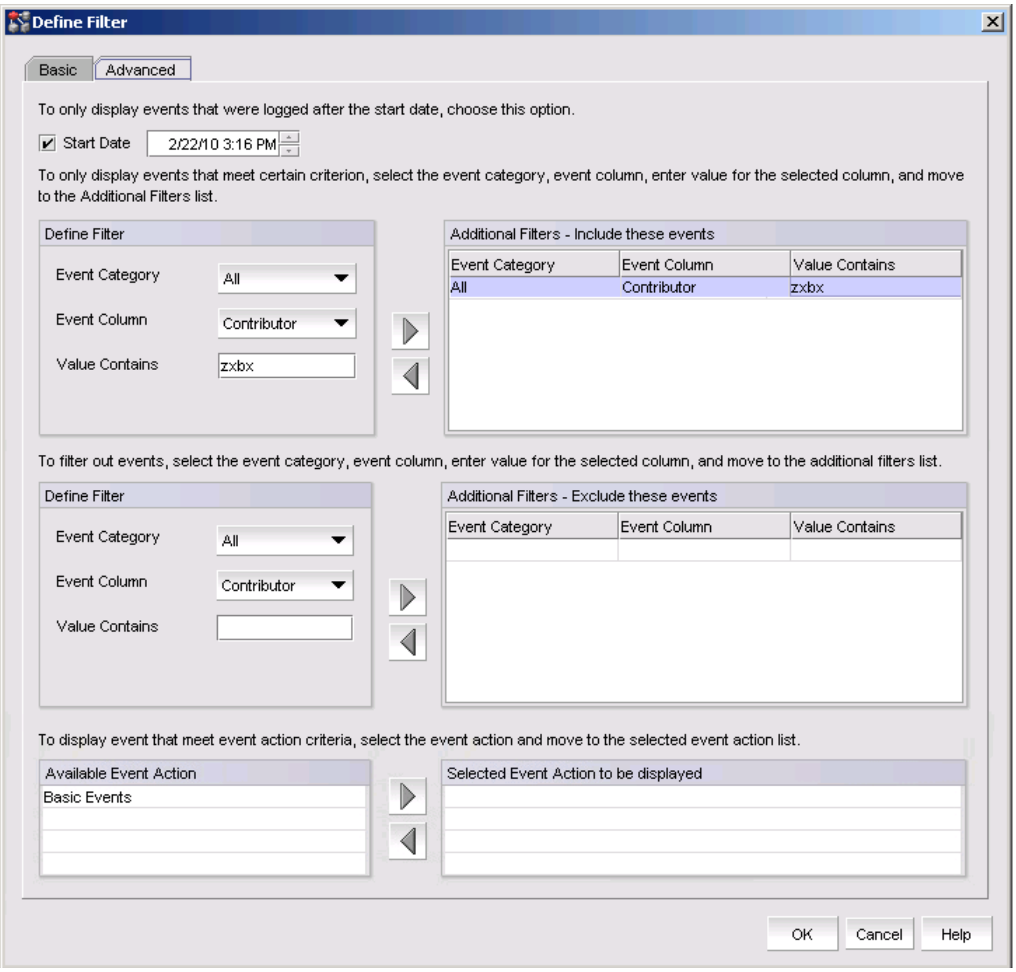
Selected Event Category and Severity to be displayed

Category	☑ Emergency	☑ Alert	☑ Critical	☑ Error
User Action Event	☑	☑	☑	☑
Management Se...	☑	☑	☑	☑
Product Event	☑	☑	☑	☑
Link Incident Event	☑	☑	☑	☑
Product Audit Ev...	☑	☑	☑	☑

Figure 7. Basic (SAN) tab in the Network Advisor Define Filter dialog box

The Advanced tab, shown in Figure 8, is similar to the DCFM Advanced filtering tab. Some of the changes are listed below:

- Start Date can be used to display events that are logged after this date; overrides the basic and other advanced filter settings.
- The event action is defined in the Event Actions dialog box.
- The Include filter allows events in addition to those allowed by the basic filter; the exclude filter excludes events meeting the exclude criteria even when allowed by the basic include filter.
- If the advanced filter event action list is set, then events not selected in the list are disallowed (but can be overridden by setting an include filter).
- Filtering can be based on the following new columns available in the Event Column: Area, Acknowledged, Origin, and Product Address. The Event Column lists all the columns mentioned in the Master Log table.



To only display events that were logged after the start date, choose this option.

☑ Start Date 2/22/10 3:16 PM

To only display events that meet certain criterion, select the event category, event column, enter value for the selected column, and move to the Additional Filters list.

Define Filter

Event Category: All

Event Column: Contributor

Value Contains: zxbx

Additional Filters - Include these events

Event Category	Event Column	Value Contains
All	Contributor	zxbx

To filter out events, select the event category, event column, enter value for the selected column, and move to the additional filters list.

Define Filter

Event Category: All

Event Column: Contributor

Value Contains:

Additional Filters - Exclude these events

Event Category	Event Column	Value Contains

To display event that meet event action criteria, select the event action and move to the selected event action list.

Available Event Action	Selected Event Action to be displayed
Basic Events	

Figure 8. Advanced (SAN) tab in the Network Advisor Define Filter dialog box

Event Migration

The way events are stored in the DCFM server has changed with respect to the database schema in Network Advisor; hence migration needs to address the mapping of DCFM events to the new schema in Network Advisor. All events from the existing DCFM repository are migrated to new database tables with the new schema. DCFM keeps Syslog events (other than audit events) in a separate table compared to other events such as traps and application events. All these events are merged to a single database table in Network Advisor—marking their origin appropriately based on the source of the events: trap, Syslog, and application events. DCFM user-configured event storage values are retained during migration. If the old event storage values are same as the default values, then during migration the default value changes to the new default value.

All the archived data is also migrated when upgrading to Network Advisor 11.0. Since the schema is different, the archived events file is migrated as a new file with a prefix “Migrated_.” There is no impact in migration in severity mapping except that the severity named Panic in DCFM is changed to Emergency in all applicable entities such as events, filters, and policies after migration.

INSTALLATION AND DEPLOYMENT

Installing Network Advisor

Ensure that you have your DCFM serial number or a license key before the installation. You can install Network Advisor by either:

1) Using the DVD

2) Downloading the software from the www.brocade.com (see Appendix A).

Unlike DCFM, Network Advisor 11.0 provides a single installer, which allows configuration options such as choosing packages and installation type via the configuration wizard. For detailed installation procedures, see the product documentation.

Running the Client

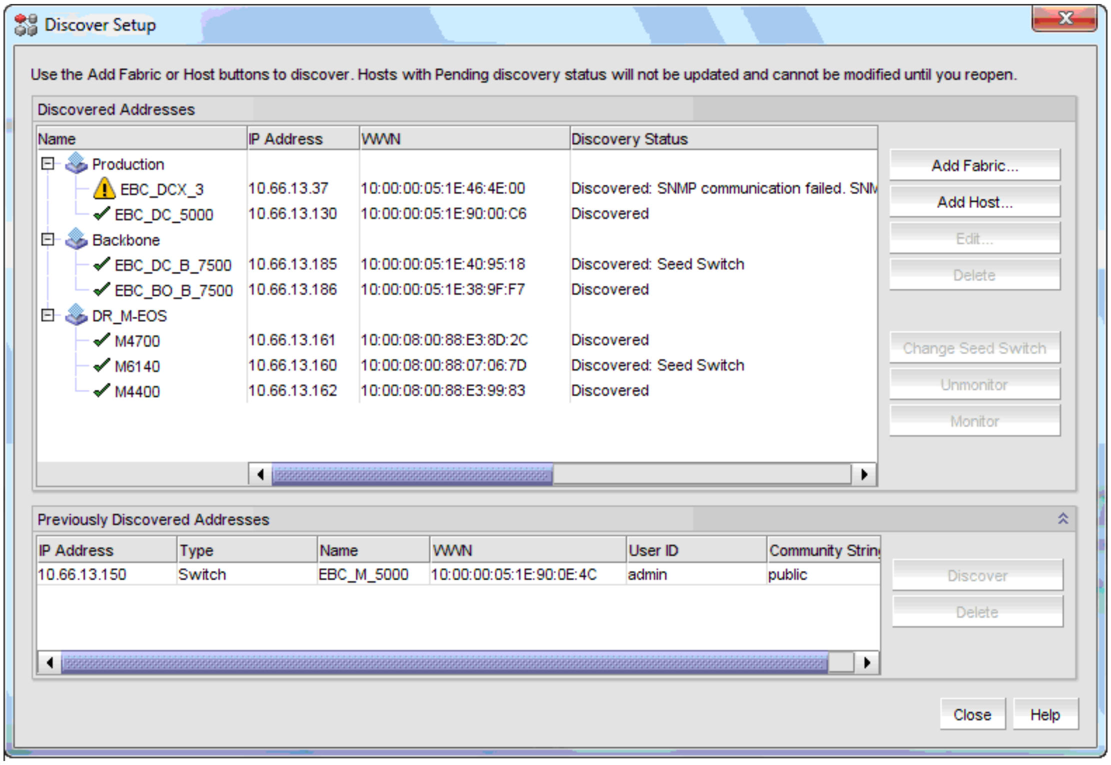
Launch the Network Advisor client either from the Start menu or use the “Web Start the Network Advisor Client” link on the Network Advisor Web page. This displays the login screen. The default user name and password are the same as they were for DCFM: “Administrator” and “password,” which is case sensitive.

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, a set of ports need to be opened up in the firewall.* For a list of these ports, see the *Brocade Network Advisor User in* the section entitled, “Management server and client.”

POST-DEPLOYMENT CONFIGURATION

Discovery of Environment

- To display the Discovery window, choose **Discovery > Setup** in the View All window. 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.
- To find out if a switch has been discovered or not, use the switch’s Properties dialog box.
- 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 (see Figure 9).



Use the Add Fabric or Host buttons to discover. Hosts with Pending discovery status will not be updated and cannot be modified until you reopen.

Discovered Addresses

Name	IP Address	WWN	Discovery Status
Production			
EBC_DCX_3	10.66.13.37	10:00:00:05:1E:46:4E:00	Discovered: SNMP communication failed. SNM
EBC_DC_5000	10.66.13.130	10:00:00:05:1E:90:00:C6	Discovered
Backbone			
EBC_DC_B_7500	10.66.13.185	10:00:00:05:1E:40:95:18	Discovered: Seed Switch
EBC_BO_B_7500	10.66.13.186	10:00:00:05:1E:38:9F:F7	Discovered
DR_M-EOS			
M4700	10.66.13.161	10:00:08:00:88:E3:8D:2C	Discovered
M6140	10.66.13.160	10:00:08:00:88:07:06:7D	Discovered: Seed Switch
M4400	10.66.13.162	10:00:08:00:88:E3:99:83	Discovered

Previously Discovered Addresses

IP Address	Type	Name	WWN	User ID	Community Strin
10.66.13.150	Switch	EBC_M_5000	10:00:00:05:1E:90:0E:4C	admin	public

Figure 9. Network Advisor Discover Setup window

Validation Testing

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

Switch Configuration. All switches discovered in DCFM will be automatically discovered in Network Advisor and the information below is migrated. Right-click on switches in a fabric and choose **Properties** to verify.

- IP Address, WWN, Switch Name
- Contact, Location
- Description, Type, Model
- Firmware Version
- Vendor
- Max Virtual Switch, Num Virtual Switch
- Reachable, Unreachable Time
- Operation Status
- Syslog Registered, SNMP Registered
- Call Home enabled
- Mgmt Server IP

Fabric Information. The fabric information listed below and stored in DCFM will be migrated to Network Advisor. Right-click on a fabric and choose **Properties** to verify.

- Fabric ID, Seed Switch WWN, Fabric Name
- Contact, Location
- Description, Type
- Secure
- Admin Domain ENV
- Managed
- Track Changes
- Active Zoneset Name

FTP Server Information. Internal FTP information such as username, password, home directory, and port number will be saved. External FTP information will include only the IP address of the external FTP server. Verify this through **Server > Options > Software Configuration > SAN FTP/SCP.**

- **Zones.** Network Advisor will populate its database with zoning information retrieved from each discovered fabric. Choose **Configure > Zoning** to see all zoning information.
- **Administrator User Profile.** Network Advisor will import user credentials. Choose **Server> Users** to see registered users and roles.

  NOTE: The system "Administrator" role is not a default role in Network Advisor and is considered as a user defined role after migrating from DCFM to Network Advisor.

Technical Support Information

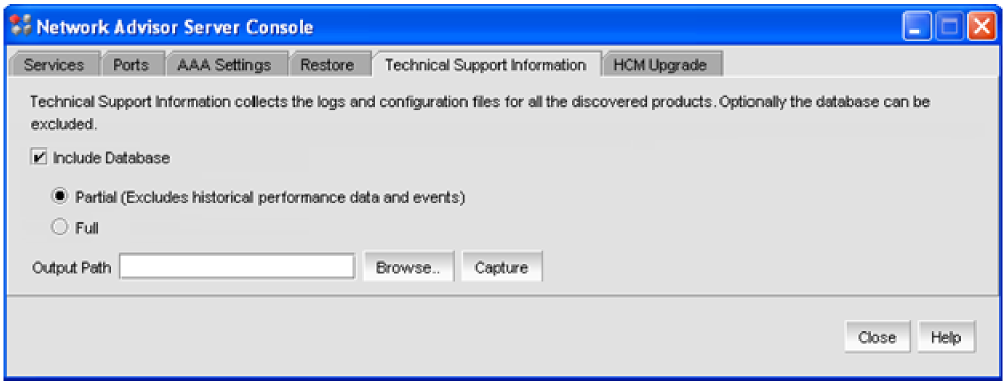
After installing Brocade Network Advisor, take a snapshot to help with potential support issues. Open the Server Management Console to create a snapshot and perform these steps:

1) Click the **Technical Support Information** tab. Note that the Technical Support Information tab is enhanced to provide options to include or exclude the database and to select Full or Partial database.

2) Uncheck the **Include Database** option if you wish. Or if you leave it checked, click **Partial** or **Full** (see details below).

3) In the Output Path text box, specify the path to a location in which to save the Network Advisor server technical support information or browse to a location.

4) Click **Capture** to gather all the information, and then click **Close**.



Technical Support Information collects the logs and configuration files for all the discovered products. Optionally the database can be excluded.

☑ Include Database

● Partial (Excludes historical performance data and events)

○ Full

Output Path

Figure 10. DCFM Technical Support Information screen

Since Brocade Network Advisor manages both SAN and IP, the database size and hence the support save may grow in terms of GBs of size and it may be tedious to get the entire support save for troubleshooting issues. The database occupies the greatest amount of space in Network Advisor support save. In the database, around 80% of the size is due to performance statistics and events data, which typically are not used for troubleshooting. Hence you have the following options for capturing Technical Support information:

- To exclude the database completely if you do not want to send entire database for troubleshooting
- To include the database completely or partially, as required in most cases; this is the default option

Selecting Partial captures the database excluding Historical Performance Statistics data and Events data. However, to get information from recent Events and Stats, Network Advisor would include 5000 and 2000 numbers of records from EVENT_DETAILS_INFO view and Performance stats tables respectively, by default.

Local Client Files

In previous DCFM releases, client log files, support save files, and saved login information for Web-started clients were placed in a folder named: `<user home directory>/<DCFM product name>/<server name>` The equivalent files for a local client were placed in: `<user home directory>/<DCFM product name>`

In Brocade Network Advisor 11.0.0, files for the local client are placed in: `<user home directory>/<Network Advisor>/localhost.` The client file locations are the same for Windows and Linux. Because of the new location, the local client's saved login information (user name and password) is not preserved during migration. You will need to re-enter the user name and password on the first login after upgrading from DCFM to Network Advisor.

APPENDIX A: PURCHASING BROCADE NETWORK ADVISOR

Brocade Network Advisor is available with flexible package and licensing options for a wide range of network deployments and for future network expansion. The no-cost Network Advisor for SAN Professional is included with all Brocade hardware platforms. It includes a subset of features found in the Network Advisor for SAN Professional Plus and is designed to manage Brocade FOS-based switches on a single-fabric basis for up to 1,000 ports.

Brocade Network Advisor software and documentation are shipped on a DVD or available via download (see the *Installation Guide* for details). If you are interested in Network Advisor for SAN Professional Plus or SAN Enterprise, a 75-day trial is available. If you decide to purchase SAN Professional Plus or SAN Enterprise, your data and configurations from SAN Professional can be migrated to SAN Professional Plus or SAN Enterprise. You can upgrade from SAN Professional Plus to SAN Enterprise just by adding a new license key.

- Network Advisor for SAN Professional can be downloaded from www.brocade.com/NetworkAdvisorPro.
- Network Advisor for SAN Professional Plus or SAN Enterprise Trial versions can be downloaded from www.brocadeconnect.com/public/NetworkAdvisorEval.

In addition to managing mixed fabrics, Brocade Network Advisor for SAN Professional Plus and SAN Enterprise have other features not found in Network Advisor for SAN Professional, as detailed in the following tables.

Hardware Platform	Network Advisor for SAN Professional	Network Advisor for SAN Professional Plus	Network Advisor for SAN Enterprise
Brocade 40xx, 54xx Embedded Switch	✓	✓	✓
Brocade 200E, 4x00, 5000, 48000	✓	✓	✓
Brocade 300, 5100, 5300,	✓	✓	✓
Brocade 7500/7500E,/FR4-18i	✓ (a)	✓	✓
Brocade 7600, FA4-18	✓ (b)	✓ (b)	✓ (b)
Brocade FC4-16IP iSCSI Blade (2)	✓	✓	✓
Brocade DCX Backbone	✗	✗	✓
Brocade DCX-4S Backbone	✓	✓	✓
Brocade Encryption Switch	✓	✓	✓
Brocade FS8-18 Encryption Blade	✓	✓	✓
Brocade 8000 Switch	✓	✓	✓
Brocade FCOE10-24 Blade	✓	✓	✓
Brocade 7800 Extension Switch	✓	✓	✓
Brocade FX8-24 Extension Blade	✓	✓	✓
McDATA 4xxx Switches	✗	✓ (c)	✓ (c)
Brocade 6064/M6140 Directors	✗	✓ (c)	✓ (c)
Brocade Mi10K Director	✗	✓ (c)	✓ (c)

a) Limited support
b) Basic Layer 2 configuration
c) Minimum M-EOS 9.6

Feature	Network Advisor for SAN Professional	Network Advisor for SAN Professional Plus	Network Advisor for SAN Enterprise
# of fabrics	1	4	24
Type of fabrics supported	FOS	FOS, M-EOS, Mixed	FOS, M-EOS, Mixed
# of ports	1,000	2, 560	9,000 (FOS) 5,000 (M-EOS, Mixed)
Virtual Fabrics	✓ (Limited support)	✓	✓
FICON	✗	✗	✓
Encryption configuration	✓	✓	✓
Quality of Service (QoS)	✓	✓	✓
Traffic Isolation (TI) zones	✓	✓	✓
FCR/LSAN Zoning	✗	✓	✓
FCIP Tunnels Interface (FOS only)	✓	✓	✓
FCIP configuration	✓	✓	✓
Port fencing	✓ (FOS only)	✓	✓
RBAC and security schemes	✗	✓ (a)	✓ (a)
Real-Time Performance	✓	✓	✓
Historical Performance	✗	✓	✓
DBMS (ODBC and JDBC)	✗	✓ (b)	✓ (b)
Top Talkers	✗	✓	✓
Performance thresholds	✗	✓	✓
HBA/CNA management	✓	✓	✓
Server Virtualization support	✓	✓	✓
Access Gateway	✓	✓	✓
FCoE/DCB	✓	✓	✓
HBA management	✓	✓	✓
Partner software integration	✗	✓	✓
Call Home support	✗	✓	✓
Microsoft SCOM Management Pack	✗	✓	✓
Management Plugin for VMware vCenter	✗	✓	✓
Integrated SMI Agent	✗	✓	✓

(a) Support for Role-Based Access Control (RBAC) and security schemes (RADIUS, LDAP, Active Directory, NIS/NIS+, and more)

(b) Data persistence for up to two years of data, out-of-box Open Database Connectivity (ODBC), and Java Database Connectivity (JDBC) access

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 Network Advisor is designed with open standards interfaces to simplify integration with management frameworks supplied by server, storage, and infrastructure management partners such as VMware vCenter, Microsoft System Center Operations Manager (SCOM), IBM Tivoli, Motorola, and McAfee. The Network Advisor 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, to scale efficiently with storage and virtual server workloads

Microsoft SCOM Management Pack

Microsoft SCOM Management Pack is a Web application hosted on the Network Advisor server that serves Web service end-points and following dynamic HTML content to the SCOM Console:

- Information about fabrics and switches that are managed by Network Advisor
- End-to-End (EE) monitors
- SAN events : critical events for switches (those that trigger Call Home in managed fabrics)

Server administrators can quickly identify SAN-related application performance or other issues by viewing statistics such as Tx/Rx percentage utilization or CRC errors. Access to this statistical information helps administrators improve troubleshooting and resolution, as well as communications between the SAN/storage administrator and the server administrator.

Key benefits of the integrated solution include:

- The System Center Operations Manager plug-in displays fabric inventory information collected by Brocade Network Advisor in the Microsoft SCOM console.
- The SCOM plug-in makes use of Management Pack and SCOM SDK services to extend the SCOM Console UI and present fabric inventory information.
- The SCOM plug-in serves dynamic HTML pages that display fabric inventory data and EE-Monitor Statistics.
- The SCOM plug-in retrieves Call Home events from the Brocade Network Advisor server and periodically checks the health of Network Advisor.

NOTE: Only one SCOM server can be added to Network Advisor for EE or PPE in this release. Also, the SCOM server and Network Advisor server must be on different host systems.

Management Plug-in for VMware vCenter

The management plug-in for VMware vCenter displays SAN connectivity information for managed ESX Server hosts and switch port statistics in the vSphere client. The current plug-in supports CNA and HBA connectivity.

The VMware vCenter plug-in enables proactive SAN monitoring in the following ways:

- Provides Virtual Machine (VM)-to-storage LUN visibility
- Enables VM-to-storage proactive port monitoring
- Provides visibility to SAN performance statistics
- Enables forwarding of SAN performance and fault events
- Empowers vCenter administrators with bottleneck identification

Network Advisor and IBM Integration Solutions

Network Advisor simplifies the management of Brocade switches, directors, and backbone platforms; and Brocade HBAs, and CNAs to help meet Service Level Agreements (SLAs) and reduce costs required for the world's most demanding data centers. Network Advisor also extends seamless management of virtual and physical data center environments through integration with IBM Systems Director and IBM Tivoli Storage Productivity Center.

IBM Systems Director Integration Solution

IBM Systems Director is the systems management foundation that streamlines the way physical and virtual systems are managed across a multi-system environment. It is an easy-to-use, point-and-click, simplified management solution. Through a single user interface, IBM Systems Director provides consistent views for viewing managed systems, determining how these systems relate to one another while showing their individual status.

Key benefits of the integrated solution include:

- Simplifies the management of physical and virtual platform resources
- Provides essential systems management support for all IBM servers, storage, and network devices
- Unifies management of Brocade FOS, M-EOS, and mixed multiprotocol fabrics including support for FCoE and DCB
- Supports Virtual Fabrics and server virtualization, including viewing and setting QoS for virtualized workloads
- Single sign-on and launch-in-context

IBM Tivoli Storage Productivity Center Integration Solution

The Network Advisor and IBM Tivoli Storage Productivity Center solution provides customers with the ability to proactively manage, monitor, and control SAN fabrics. IBM Tivoli Storage Productivity Center helps customers manage the capacity utilization of storage systems, files systems, and databases. It enables customers to automate file-system capacity provisioning, configure and manage multiple devices from a single interface, and tune and proactively manage the performance of storage devices on the SAN.

Key benefits of the integrated solution include:

- Unifies management of Brocade FOS, M-EOS, and mixed multiprotocol fabrics within and across data centers, including support for FCoE and DCB
- Supports Virtual Fabrics and server virtualization, including viewing and setting QoS for virtualized workloads
- Reduces operating expenses and maximizes productivity by automating tasks through easy-to-use, wizard-driven operations
- Monitoring, troubleshooting, diagnostics, and event notification capabilities to enable SLAs
- Secures data flow from applications to storage across data center fabrics by managing user access controls and ensuring consistent security settings
- Delivers real-time and historical performance monitoring to enable proactive problem diagnosis, maximize resource utilization, and facilitate capacity planning
- Helps centralize the management of a customer’s storage infrastructure from a single interface using role-based administration and single sign-on
- Provides a single management application with modular integrated components that are easy to install and provides common services for simple, consistent configuration and consistent operations across host, fabric, and storage systems
- Manages performance and connectivity from the host file system to the physical disk, including in-depth SAN fabric performance monitoring and analysis

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.