HP B-series Network Advisor Enterprise, Professional Plus, and Professional 12.1.5 Release Notes

HP Part Number: 5697-3234
Published: March 2014
Edition: 1

Contents

Version

12.1.5

Description

HP Network Advisor is a software management platform that provides users with a consistent user interface across FC and FCoE / DCB along with custom views and controls based on the users' areas of specialization. Network Advisor provides users with the utmost flexibility in deployment and operational models, including traditional SAN deployments (FC) and end-to-end convergence (FCoE, iSCSI and NAS over DCB). It provides the next evolutionary step from the previous DCFM software management platform, and is required for management of the new hardware platforms highlighted below, and any future hardware platforms, as well as for the new Fabric OS 7.1 and later releases.

HP Network Advisor offers enhancements to flexible SAN performance analysis as well as supporting updated platform firmware versions.

HP Network Advisor 12.1.5 is a software maintenance release based on HP Network Advisor 12.1.1-12.1.4 that include the same hardware support, features, and fixes supported in Network Advisor 12.1.1-12.1.4, plus additional fixes important to HP for 12.1.5.

Key feature enhancements introduced in Network Advisor 12.1.1

- Fabric OS 7.2.0a support
- Fabric Vision Enhancements with MAPS and Flow Vision configuration and dashboard support

Key feature enhancements introduced in Network Advisor 12.1.2

Real Time graphing support for Flow Vision.

Key feature enhancements introduced in Network Advisor 12.1.4

- Historical Graph and Historical Report for GIGE ports.
- FEC measures support in Performance Graphs
- Flow Vision: Frame size support
- vCops SMI Enhancements
- SCOM events enhancements
- D-port support
- Pagination support in Zoning dialog

Migration and upgrades

Network Advisor 11.3.0, 12.0.X (12.0.0 - 12.0.3), and 12.1.X (12.1.1-12.1.4) running on the Linux and Windows operating systems can be upgraded to Network Advisor 12.1.5.

NOTE: Migrations to Network Advisor 12.1.5 from earlier versions, require an earlier version of Network Advisor to be installed and running. Partial and Network path Migrations to Network Advisor 12.1.5 are not supported from prior versions. See the "Application Configuration" chapter in the *Brocade Network Advisor SAN User Manual 12.0.0* for the configuration backup procedure and the "Data Migration" chapter in the *Brocade Network Advisor Installation and Migration Guide 12.0.0* for details about migration.

DCFM 10.4.x running on the Linux and Windows operating systems can be upgraded to Network Advisor 11.1.x (11.1.0 - 11.1.5) first, and then upgraded to Network Advisor 12.0.0 - 12.0.3

and then upgrade to Network Advisor 12.1.5. Network Advisor is not supported on the Solaris platform.

DCFM 10.4.x running on the Solaris platform must first migrate to a supported operating system. Once migration from the Solaris platform to either Linux or Windows is complete, upgrade to Network Advisor 11.1.x and then upgrade to Network Advisor 12.0.0 - 12.0.3 and then upgrade to Network Advisor 12.1.5. Earlier versions of DCFM must first be upgraded to DCFM 10.4.x, then upgraded to Network Advisor 11.1.x, and then upgraded to Network Advisor 12.0.0 - 12.0.3 and then upgrade to Network Advisor 12.1.5. Upgrades from DCFM to Network Advisor 11.1.x do not require a new software license key.

Supported switches and firmware

Table 1 (page 7) and Table 2 (page 8) list switches and firmware families supported with HP Network Advisor 12.1.5. This does not imply that all firmware versions listed in the left column are still supported by HP, but rather that those are the firmware streams on which the corresponding switches are, or were, supported. It also does not imply that all the firmware listed in streams is supported on each of the corresponding switches. HP recommends using the latest software versions to get the greatest benefit from the SAN.

Table 1 Supported switches and firmware

Supported switches and firmware	Switch/Director
Fabric OS 5.0.x, 5.1.x, 5.2.x, 5.3.x, 6.0.x, 6.1.x, 6.2.x,6.3.x, 6.4.x, 7.0.x, 7.1.x, 7.2.x	HP 400 Multiprotocol Router (Brocade 7500)[1] HP 4/8, 4/16 SAN Switch (Brocade 200E) HP SAN Switch 4/64 (Brocade 4900)[2] HP SAN Switch 4/32B (Brocade 5000)[3] HP 8/8, 8/24 SAN Switch (Brocade 300)[5] HP 8/40 SAN Switch (Brocade 5100)[5] HP 8/80 SAN Switch (Brocade 5300)[5] HP 2408 FCoE Converged Network Switch (Brocade 8000)[9] Switch 2/64 (Brocade 12000) HP 1606 SAN Extension Switch (Brocade 7800) [10] HP Encryption SAN Switch (Brocade Encryption Switch)[7] HP 4/256 SAN Director (Brocade 48000) with HP 4/256 SAN Director with 16-Port 4Gb Blade (FC4-16) [2] HP 4/256 SAN Director (Brocade 48000) with HP 4/256 SAN Director 32-Port 4Gb Blade (FC4-32) [2] HP 4/256 SAN Director (Brocade 48000) with HP 4/256 SAN Director 48-Port 4Gb Blade (FC4-48)[2] HP 4/256 SAN Director (Brocade 48000) with HP B-series Multiprotocol Router Blade (FR4-18i)[1] HP 4/256 SAN Director (Brocade 48000) with HP 4/256 SAN Director 48-Port 4Gb Blade (FC10-6)[4] HP DC SAN Backbone Director Switch[6] with HP SAN Director 16-port 8Gb FC Blade (FC8-16) HP DC SAN Backbone Director Switch[6] with HP SAN Director 32-port 8Gb FC Blade (FC8-32) HP DC SAN Backbone Director Switch[6] with HP SAN Director 48-port 8Gb FC Blade (FC8-48)

Table 2 Supported switches and firmware (continued)

Supported switches and firmware	Switch/Director
Fabric OS 5.0.x, 5.1.x, 5.2.x, 5.3.x, 6.0.x, 6.1.x, 6.2.x,6.3.x, 6.4.x, 7.0.x , 7.1.x, 7.2.x	HP DC SAN Backbone Director Switch[6] with HP B-series Multiprotocol Router Blade (FR4-18i) HP DC SAN Backbone Director Switch with HP 4/256 SAN Director 48 Port 4Gb Blade (FC10-6) HP DC SAN Backbone Director Switch[7] with HP DC Switch Encryption FC Blade(FS8-18) HP DC SAN Backbone Director Switch[10] with HP DC SAN Director 10/24 FCoE Blade (FCoe10-24) HP DC SAN Backbone Director Switch[10] with HP DC SAN Director Multiprotocol Extension Blade (FX8-24) HP DC04 SAN Director Switch[8] with HP SAN Director 16-port 8Gb FC Blade (FC8-16) HP DC04 SAN Director Switch[8] with HP SAN Director 32-port 8Gb FC Blade (FC8-32) HP DC04 SAN Director Switch[8] with HP SAN Director 48-port 8Gb FC Blade (FC8-48) HP DC SAN Backbone Director Switch[11] with HP SAN Director 64-port 8Gb FC Blade (FC8-64) HP DC04 SAN Director Switch[8] with HP B-series Multiprotocol Router Blade (FR4-18i) HP DC04 SAN Director Switch[8] with HP 4/256 SAN Director 48 Port 4Gb Blade (FC10-6) HP DC04 SAN Director Switch[8] with HP DC Switch Encryption FC Blade (FS8-18) HP DC04 SAN Director Switch[10] with HP DC SAN Director 10/24 FCoE Blade (FCoe10-24) HP DC04 SAN Director Switch[10] with HP DC SAN Director Multiprotocol Extension Blade (FX8-24) HP DC04 SAN Director Switch[11] with HP SAN Director 64-port 8Gb FC Blade (FC8-64) HP SN8000B 4-Slot SAN Director Switch (DCX8510-4)[12] HP SN8000B 8-Slot SAN Backbone Director Switch (DCX8510-8)[12] HP SN8000B 4-Slot SAN Director Switch (DCX8510-4)[12] and HP SN8000B 8-Slot SAN Backbone Director Switch (DCX8510-8)[12] with HP SN8000B 16Gb 32-port Fibre Channel Blade (FC16-32) HP SN8000B 4-Slot SAN Director Switch (DCX8510-4)[12] and HP SN8000B 8-Slot SAN Backbone Director Switch (DCX8510-8)[12] with HP SN8000B 16Gb 48-port Fibre Channel Blade (FC16-48)[12] HP SN6000B 16Gb FC Switch (6510)[12] HP SN8000B 4-Slot SAN Director Switch (DCX8510-4)[13]and HP SN8000B 8-Slot SAN Backbone Director Switch (DCX8510-8)[13] with HP SN8000B 8Gb 32-port Enhanced Fibre Channel Blade (FC8-32E)[13] HP SN8000B 4-Slot SAN Director Switch (DCX8510-4)[13]and HP SN8000B 8-Slot SAN Backbone Director Switch (DCX8510-8)[13] with HP SN8000B 8Gb 48-port Enhanced Fibre Channel Blade (FC8-48E)[12] HP SN3000B 16Gb FC Switch (6505)[13] HP StoreFabric SN6500B 16Gb FC Switch (6520)[14]
Fabric OS 5.2.x, 5.3.x, 6.0.x, 6.1.x, 6.2.x, 6.3.x, 6.4.0, 7.0.0x, 7.1.x, 7.2.x	Brocade 4Gb SAN Switch for HP c-Class BladeSystem[1] (4024) Brocade 8Gb SAN Switch for HP BladeSystem c-Class[2] (5480) HP EVA4400 embedded switch module, 8Gb Brocade[2] (5410) Brocade 16Gb SAN Switch for HP BladeSystem c-Class (6548) [15]

1. Requires Fabric OS 5.1.0 or later
2. Requires Fabric OS 5.2.0 or later
3. Requires Fabric OS 5.2.1b or later
4. Requires Fabric OS 5.3.0 or later

5. Requires Fabric OS 6.1.0a or later
6. Requires Fabric OS 6.0.0b or later
7. Requires Fabric OS 6.1.1_enc or later
8. Requires Fabric OS 6.2.0 or later
9. Requires Fabric OS 6.1.2_CEE or later
10. Requires Fabric OS 6.3.x or later
11. Requires Fabric OS 6.4.0 or later
12. Requires Fabric OS 7.0.0a or later
13. Requires Fabric OS 7.0.1 or later and Network Advisor 11.1.3 as a minimum version
14. Requires Fabric OS 7.1.0a or later and Network Advisor 12.0.0 as minimum version
15. Requires Fabric OS 7.1.0_blv and Network Advisor 12.0.2 as minimum version

Supported operating systems

Table 3 (page 9) lists the operating systems that support HP Network Advisor 12.1.5.

NOTE: The minimum required system physical memory for running Network Advisor 12.1.5 (server plus one local client) is:

- Network Advisor Professional Edition: 4 GB (32-bit OS), 8 GB (64-bit OS)
- Network Advisor Professional Plus and Enterprise Editions (supported on 64-bit OS only):
  - Small SAN fabric: 8 GB
  - Any combination that includes a medium/large SAN fabric: 16 GB

Table 3 Supported operating systems (64-bit)

Operating System (64-bit) Architecture	Versions
Windows	Windows Server 2008 R2 Standard, Enterprise, Datacenter Windows Server 2012 Standard, Datacenter Windows 7 Enterprise Windows 8 Enterprise
Linux	Red Hat Enterprise Linux 6.1 Adv Red Hat Enterprise Linux 6.2 Adv Red Hat Enterprise Linux 6.3 Adv Oracle Enterprise Linux 6.1 Oracle Enterprise Linux 6.2 Oracle Enterprise Linux 6.3 **NOTE:** Only Network Advisor Professional Edition is supported on 32-bit Operating Systems. Network Advisor Professional Plus and Enterprise Editions require a 64-bit Operating System for installation.

Table 4 Supported operating systems (32-bit)

Operating System (32-bit) Architecture	Versions
Windows	Windows 2008 Standard (x86) Windows 7 Enterprise (x86)
Linux	Red Hat Enterprise Linux 6.1 Adv (x86) Red Hat Enterprise Linux 6.2 Adv (x86) Red Hat Enterprise Linux 6.3 Adv (x86) SUSE Linux Enterprise Server 11 (x86)

Table 4 Supported operating systems (32-bit) *(continued)*

Operating System (32-bit) Architecture	Versions
	Oracle Enterprise Linux 6.1 (x86) Oracle Enterprise Linux 6.2 (x86) Oracle Enterprise Linux 6.3 (x86) **NOTE:** All the above Operating Systems are supported as Guest VMs on VMware ESXi 5.1, KVM (RedHat Enterprise Linux 6.3 Adv) and Microsoft Hyper-V (Hyper-V Server 2008 R2 SP1, Windows Server 2012).

Table 5 Virtual machine management supported versions

Virtual machine	Versions
ESX	4.0, 4.1
ESXi	4.0, 5.0, 5.1
VCenter	4.0, 4.1, 5.0, 5.1

Supported features

Table 6 Supported Network Advisor features

Feature	Network Advisor Professional	Network Advisor Professional Plus	Network Advisor Enterprise
Number of fabrics	1	36	36
Type of fabric supported	Fabric OS	M-EOS, Fabric OS, Mixed	M-EOS, Fabric OS, Mixed
Number of ports	1,000	2,560	9,000 (Fabric OS); 5,000 (M-EOS/Mixed)
4 Gb, 8 Gb, and16 Gb Switches	Yes	Yes	Yes
DC SAN Director 10/24 FCoE Blade/2408 FCoE Converged Network Switch	Yes	Yes	Yes
1606 Extension SAN Switch	Yes	Yes	Yes
4/256 SAN Director	Yes	Yes	Yes
DC04 SAN Director Switch	Yes	Yes	Yes
SN8000B 4-Slot SAN Director Switch	Yes	Yes	Yes
HBA Management (HCM)	Yes	Yes	Yes
Virtualization support	Yes	Yes	Yes
Encryption SAN Switch/Encryption Blade	Yes	Yes	Yes
DC Director Switch MP Extension Blade	Yes	Yes	Yes
Real time stats[1]	Yes	Yes	Yes
Historical stats[2]	No	Yes	Yes
DBMS (ODBC & JDBC)	No	Yes	Yes
Partner software integration	No	Yes	Yes

Table 6 Supported Network Advisor features *(continued)*

Feature	Network Advisor Professional	Network Advisor Professional Plus	Network Advisor Enterprise
Role Based Access Control (RBAC)	No	Yes	Yes
FICON	No	No	Yes
DC SAN Backbone Director	No	No	Yes
SN8000B 8-Slot SAN Backbone director	No	No	Yes

[1] Real-time stats for GE ports. FC ports, E-E Monitors, and TopTalkers

[2] Historical stats for FC ports and E-E Monitors

Installing Network Advisor

This section provides installation instructions for Microsoft Windows and Linux. The Network Advisor Server runs as multiple services on Windows and multiple processes on Linux; they start automatically after installation.

NOTE: All versions of DCFM (Data Center Fabric Manager) have entered EOL (End Of Life) status. Any customers who want to upgrade from DCFM Professional Plus to HP B-series Network Advisor Enterprise will need to upgrade their DCFM to Network Advisor (available at no charge at hp.com), and then apply the Network Advisor Professional Plus Upgrade license, TC354A.

NOTE: Install the Network Advisor application on a dedicated machine that is not running any other server applications, such as another database server.

Installing Network Advisor on Windows (Server)

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

Installing Network Advisor 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 screen instructions to complete the installation.

Launching the Network Advisor Client

To launch the Network Advisor Client on the same local machine as the Network Advisor Server:

For Windows:

1. Select **Start > Programs > Network Advisor 12.1.5 > Network Advisor 12.1.5.**

   The client can be launched using the Desktop icon.

2. At the Windows command prompt, go to the location `<Install_location>/bin`, and enter `dcmclient`.

For Linux:

The client can be launched via Desktop icon.

Launch terminal, go to the location `<Install_location>/bin`, and enter `sh dcmclient`.

For Windows and Linux, follow the steps below on launching the client from a web browser.

Launching the Network Advisor client from a remote host

1. Open a browser window and enter the Network Advisor server hostname or IP address in the Address field. For example:

   http://NetworkAdvisorServerhost1.companyname.com/

   http://192.x.y.z/

2. If a Network Advisor web server port number was specified (instead of the default 80) when the Network Advisor server was installed, you must specify the port number after the hostname or IP address. In the following examples, 8080 is the web server port number:

   http:// NetworkAdvisorServerhost1.companyname.com:8080/

   http://192.x.y.z:8080/

The required Client Oracle JRE version is 1.7.0_25. For remote clients, client Oracle JRE must be installed prior to establishing a server connection.

NOTE:

1. Launching element manager applications within the Network Advisor Client is done using Java Web Start technology. This requires the web browser of the local system to be able to run Java web start applications. This setting might be turned off due to recent Java zero-day vulnerabilities.

   To turn on Java content in the browser:

   a. Launch the Java Control Panel (see http://java.com/en/download/help/win_controlpanel.xml to locate the Java Control Panel application on Windows).

   b. In the Java Control Panel, click **Security**.

   c. Select the check box for Enable Java content in the browser. This enables the Java plug-in in the browser.

   d. Click **Apply**. When the Windows User Account Control (UAC) dialog appears, allow permissions to make the changes. Click **OK** in the Java Plug-in confirmation window.

   e. Launch the Element Manager from the Network Advisor client.

2. On a Windows server, if **Administrators** only have access to a drive, windows does not allow Postgres to create some required directories. As a result, migration from a previous version of Network Advisor to a newer supported version fails. The following procedure is required to resolve the issue:

   a. Make sure that the previous version of Network Advisor is up and running.

   b. Right click on the drive where the new version of Network Advisor is intended to be installed (For example. :D).

   c. Navigate to the **Security tab -> Edit -> Add**.

   d. Add **Authenticated Users** and give full permission, click **Ok**.

   e. Now install the new version of Network Advisor and start the migration progress.

Important notes

Consider the following information before using Network Advisor 12.0.0 or later.

- Host-based standalone SMI agents cannot manage products running Fabric OS 7.0.0a or later. It requires use of the integrated SMI Agent with Network Advisor 12.0.0 or later.
- The supported AG limit for a 64-bit OS is a maximum of 200 AGs.
- Network Advisor cannot manage an ESXi 5.0 host due to a VMware issue (KB 2012672: SFCB CIMOM on ESXi 5.0 is incompatible with JRE 1.6 U29 and later). Users are required to update to ESXi 5.0 update 1 or later to be able to manage the host in Network Advisor through the host adapter discovery.

- If the following error message occurs “Signature could not be validated” during firmware download or technical support data collection using SCP/SFTP, it could be due to a mismatch in the signature key used in the ssh handshake between the switch and SCP/SFTP server. Execute the following CLI command as a work-around to this issue:
    - **For Fabric OS devices**

      ```
      sw0:FID128:admin> sshutil delknownhost
      ```

      IP Address/Hostname to be deleted: `<IP Address of SSH server to be deleted>`
    - **Firmware version 2.1.1b** IP Address/Hostname to be deleted:

      ```
      sw0#execute-script sshdeleteknownhost
      ```

      IP Address/Hostname to be deleted: `<IP Address of SSH server to be deleted>`

      If the above CLI commands do not work, go to **Server > Options > Software Configuration > FTP/SFTP/SCP**, and uncheck the **SCP/SFTP** option.
- The Encryption Smart Card Driver is supported only for 32-bit Linux. It is not supported on 64-bit Linux.
- Firmware Download operation on Fabric OS switches fails via SCP/SFTP when trying to upgrade from Fabric OS 6.3.2b to 6.4.2b4. The workaround is to use the FTP option in Network Advisor to perform the firmware download operation.
- Firmware Download operation on Fabric OS switches fails when trying to upgrade from Fabric OS 6.4.2a to 7.0.2c. The workaround is to use CLI for this operation.
- Trying to move 200+ ports to a Logical Switch with the ‘Reset to Default’ option selected, results in an operation time-out.
- During installation, if Network Advisor database initialization fails on the Windows Operating System, users need to verify access to the drive on which the installation is performed. If user **Administrator** has access only to the drive, the required permissions should also be provided to the **Authenticated Users** and then continue with the installation.
- On devices running Fabric OS 7.1 or earlier, which do not support firmware download via FTP, users get a false notification that the firmware download is successful when trying to download firmware using FTP. For such devices, SCP must be used to download firmware using Network Advisor.
- When the active and defined zone sets have identical zones, which differ only by the case of their names, users will be alerted that the active zone set is different from the defined configuration in the zone database. The workaround is to edit the identical zone names (for such zones) in the defined set, so that after modification, both zone names are identical in active and defined zone sets.
- After upgrading to Network Advisor 12.x from 11.x, SSL-based product communication fails if the devices have ‘weak’ authentication certificates. Users can see a ‘4002’ error on attempting to discover such devices. Devices discovered prior to migration will not be manageable in Network Advisor after migration. Java 1.7 used by Network Advisor 12.x disables the use of certificates with ‘weak’ authentication. The certificates on such devices need to be updated to be compliant with JRE 1.7. See the ‘Secure Sockets Layer protocol’ section of the *Fabric OS Administrator's Guide* for details on updating certificates.
- Receive Throughput measure is not updated in the Flow Vision dialog.
- D-port test fails for F-ports with the result as `null` in the report.

- In Real Time performance graphs, percentage utilization fluctuates between 0 to 100 if a single port is selected. The workaround is to select more than one port while generating Real Time performance graphs.
- By default, Network Advisor uses SNMPv3 to discover SAN products. If required, users can select the 'Manual' option in Discovery dialog and choose SNMPv1 for discovery.
- A delay of 5 to 7 minutes is observed when Web Tools is launched on a system (through Network Advisor or directly in a web browser) where internet access is not available and the network does not return a `destination unreachable` message. This issue occurs as Java tries to validate the SSL certificates with external CAs. To avoid this issue occuring on such systems, modify the following Java properties:

  On Windows: `C:\Users\AppData\LocalLow\Sun\Java\Deployment\deployment.properties`

  On Linux: `home/<` *`logged in user name`*`>/.java/deployment/deployment.properties`

  In the `deployment.properties` file, edit the below parameters and set them to false.

  ```
  deployment.security.validation.ocsp = false
  ```

  ```
  deployment.security.validation.crl = false
  ```

  If these parameters are not present, add them and save the file. Then re-launch Web tools.

Display of Logical switches

If you create logical switches through the Logical Switch dialog box, the logical switch displays under undiscovered Logical Switch in the existing Logical Switches Panel. You must rediscover the newly created logical switch fabric, by going to the discovery dialog, and adding the IP address of the chassis using the add dialog.

Destination columns are blank for HP Encryption SAN Switch in top talkers dialog

When the Top Talkers dialog box is launched for the HP Encryption SAN Switch, the columns **Destination**, **Destination port**, and **Destination switch port** are sometimes empty.

SSL connections using certificates with MD5 signature

To avoid potential security vulnerabilities, Network Advisor versions 12.0 and later do not support SSL connections using certificates with MD5 signatures. If Network Advisor is configured to use HTTPS instead of HTTP when communicating with SAN switches, and the SAN switch has a certificate installed that is signed with an MD5 algorithm, discovery of the switch fails with the following pop-up message: `Authentication failure during discovery operation: 4002.`

The recommended solution is to replace the certificate on the network device with a certificate using the more secure SHA signature. If that is not practical, the Network Advisor server configuration can be changed to accept MD5 signatures. Note that accepting MD5 signatures might result in warnings from network security scanning tools.

To accept MD5 signatures, edit the following text file:

On 32-bit Windows or Linux: <install-dir>/jre/lib/security/java.security

On 64-bit Windows or Linux: <install-dir>/jre64/lib/security/java.security

Remove "MD5" from the following line near the end of the file:

jdk.tls.disabledAlgorithms=MD5, DES, 3DES, RC2

The modified line should appear as:

jdk.tls.disabledAlgorithms=DES, 3DES, RC2

The change takes effect the next time the Network Advisor server is restarted.

Reset Ports operation in Logical switches dialog

NOTE:

1. Reset ports to default operation is applicable only when the ports are moved from one Logical Switch to another Logical Switch through the Right Arrow button i.e., from (Chassis ports Tree/Tree Table) LHS to (Logical Switches Device Tree) RHS device tree.

   It is not applicable when:

   - Ports from a Logical switch are moved to default Logical Switch through Left Arrow button, that is, from (Logical Switches Device Tree) RHS to (Chassis ports Tree/Tree Table) LHS.
   - When a Logical switch is deleted - its ports will not be reset to default before moving to Default Logical switch before its deletion.

   Ports which are moved to the default logical switch can be reset to default, if they are moved from (Chassis ports Tree/Tree Table) LHS to (Logical Switches Device Tree) RHS device tree.

2. Reset ports to default operation does not clear FCIP configurations in the following scenarios:

   - In the HP 400 Multi-protocol Router switch and the HP Multi-protocol Router Blade, VE ports cannot be reset to default unless their corresponding GE ports are cleared of their FCIP configurations.
   - In the HP 1606 SAN Extension switch and HP DC SAN Director Multiprotocol Extension Blade, GE ports cannot be reset to default unless their corresponding VE ports are cleared of their FCIP configurations.

Network Advisor Professional Plus and Enterprise Editions

A 64-bit Operating System is required to run Network Advisor Professional Plus and Enterprise Editions.

McData Switches

Starting with Network Advisor 12.0.0, McData switches are unsupported as seed switches or member switches.

Privilege names

Privilege names are displayed in the Role Management dialog with `SAN` – prefixes. After migration from an older version, new privilege names are displayed in the role Management dialog with these prefixes.

Startup time

Network Advisor server startup and restart can take up to 10 or so minutes to complete.

Configuring SSL

When configuring Network Advisor in SSL enable mode in the application configuration wizard, ensure that both HTTP and HTTPS ports are free and available for Network Advisor. Currently the application checks only if the HTTPS configured port is available and not the HTTP port.

Increase in number of client connections

Starting with Network Advisor 12.0.0, the number of supported client connections has increased to 25. See the installation guide for the details about this feature. In addition to those details, a change to the database memory setting is required.

The PostgreSQL's parameter *shared_buffers* memory allocation should be increased to 1024 MB. This can be done by editing the `<`*installation_directory*`>\data\databases\postgresql.conf` file, changing the *shared_buffers* parameter and then restarting the server. To modify the shared buffers parameter, change the following line:

```
shared_buffers = 256MB
```

To:

```
shared_buffers = 1024MB
```

Connecting to the database

In Linux 64-bit machines, connecting to the database through Open office using ODBC does not work. As a solution, connect from the Windows ODBC Client to the 64-bit Linux machine where Network Advisor is running to view the Database tables.

Remote host connection to ODBC

After migration to Network advisor 12.0.x, remote host connections to an ODBC database are no longer supported. If you want to connect from the remote host, refer to the "Configuring remote client access to the database" section of the *Installation and Migration Guide*.

Linux Server Installation Issues

- During installation on a Linux server, if the user sets the password for the Network Advisor database starting with a '$', installation of the application fails.
- When attempting to install Network Advisor on a Linux Server, if the message `Insert New Media` is displayed, the `ulimit -n 2000` command must be executed from a terminal.

Patch installer troubleshooting

The patch installer may not launch if UAC is enabled on a Windows 7/8/2008/2008 R2/2012 Editions. Users must first disable the UAC using the procedure provided in the troubleshooting section of the *Brocade Network Advisor SAN User Manual 12.0.0* and then launch the patch installer.

Call home

Network Advisor 12.0.0 and later do not support Brocade domestic and international call home centers.

Support Saves may take a long time with large databases

As databases grow larger from Event, sFlow, and Performance Collector data, the support save operation may take a long time to run. Larger databases promote longer support save operations. Make sure you have a minimum of 20 GB disk space for support save and backup operations.

Installation on Network Mounted Drives is not supported.

Installation onto a windows network mounted drive is not supported but installation, if attempted, is allowed and DB fails to start.

Client disconnects

Under heavy server load or degraded network links, there is a potential for the Network Advisor client to disconnect from the server. The workaround is to restart the client.

Virtual Connect Enterprise Manager (VCEM) Support

Below is the list of supported and tested configuration components:

Hardware	Model
Enclosure	HP BladeSystem c3000 or c7000

Servers	Proliant BL465c G7, Proliant BL460c G6
HBA	Brocade 804 8Gb FC HBA, Emulex LPe1205-HP 8Gb FC HBA, QLogic QMH2562 8Gb FC HBA

Software/firmware	**Version**
HP SIM	6.2, 7.1
HP VCEM	6.2, 7.1
Onboard Administrator (OA)	2.41 or later
VC E-net module (HP VC 8Gb 20-Port FC Module & HP VC 8Gb 24-Port FC Module)	3.15

SMI Agent

- For Network Advisor that has more than 30K instances (2 MB zones), the CIMOM takes more memory to generate CIM instances. If users perform Enumerate Instances or Enumerate Instances Names and the total size is more than 2 MB for all managed fabrics, then a CIM_ERROR_FAILED status will be thrown, because the Total Zone DB size is more than 2 MB. For such configurations, users need to use Association calls.

  NOTE: If the total zone DB is more than 1 MB or more than 10000 instances, users should change the max jvm heap size to 2048 MB in order to access the data without failure in a 64-bit machine.

- SMI alert indication BRCD60 is not sent out to SMI clients if Fabric OS switches are discovered but SNMP trap registration has failed. Ensure that the Network Advisor server is successfully registered for traps on all switches.
- If DCB switches are running Fabric OS 6.3.x, VLAN/ACL deployment through SMI-A fails. You must upgrade the DCB Fabric OS to 6.4.x/7.0.0a for VLAN/ACL deployment support through the SMI Agent.

Indications delivery depends on SAN Size and SNMP registration

The time to deliver the indication varies, based on Network Advisor SAN size selected during installation. If a large SAN size is selected, indication delivery time is longer.

Provider classes may take more time to update the fabric changes if the switches managed in Network Advisor are not SNMP registered. All the switches managed in Network Advisor should be SNMP registered to avoid the delay in indication delivery.

Logging for CIMOM

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

The log file size and number of log files can also 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 Configuration Tool through the CIMOM tab.

Service Location Protocol (SLP) support

The Management application SMI Agent uses Service Location Protocol (SLP) to allow applications to discover the existence, location, and configuration of WBEM services in enterprise networks.

You do not need a WBEM client to use SLP discovery to find a WBEM Server; that is, SLP discovery might already know about the location and capabilities of the WBEM Server to which it wants to send its requests. In such environments, you do not need to start the SLP component of the Management application SMI Agent.

However, in a dynamically changing enterprise network environment, many WBEM clients might choose to use SLP discovery to find the location and capabilities of other WBEM Servers. In such environments, start the SLP component of the Management application SMI Agent to allow advertisement of its existence, location, and capabilities.

SLP installation is optional and you can configure it during Management application configuration. Once installed, SLP starts whenever the Management application SMI Agent starts.

Management SMI Agent SLP application support includes the following components:

- The slpd script, which starts the slpd platform
- The slpd program acts as a Service Agent (SA). A different slpd binary executable file exists for UNIX and Windows systems.
- The slptool script, which starts the slptool platform-specific program
- The slptool program can be used to verify whether SLP is operating properly. A different slptool exists for UNIX and Windows.

By default, the Management application SMI Agent is configured to advertise itself as a Service Agent (SA). The advertised SLP template shows its location (IP address) and the WBEM Services it supports. The default advertised WBEM services show the Management application SMI Agent, which:

- Accepts WBEM requests over HTTP without SSL on TCP port 5988
- Accepts WBEM requests over HTTPS using SSL on TCP port 5989

`slptool` commands

Use the following `slptool` commands to verify whether the SLP is operating properly:

- `slptool findsrvs service:service-agent`

  Use this command to verify that the Management application SMI Agent SLP service is properly running as a Service Agent (SA). Example output:
  `service:service-agent://127.0.0.1,65535.`

- `slptool findsrvs service:wbem`

  Use this command to verify that the Management application SMI Agent SLP service is properly advertising its WBEM services. Example outputs:

  - `service:wbem:https://10.0.1.3:5989,65535`
  - `service:wbem:http://10.0.1.3:5988,65535`

This output shows the following functionalities of the Management application SMI Agent:

- It accepts WBEM requests over HTTP using SSL on TCP port 5989.
- It accepts WBEM requests over HTTP without SSL on TCP port 5988.

  - `slptool findattrs service:wbem:http://IP_Address:Port`

    Use this command to verify that Management application SMI Agent SLP service is properly advertising its WBEM SLP template over the HTTP protocol. Example input: `slptool findattrs service:wbem:http://10.0.1.2:5988 .`

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

- ○ `slptool findattrs service:wbem:https://IP_Address:Port`

  Use this command to verify that the Management application SMI Agent SLP service is properly advertising its WBEM SLP template over the HTTPS protocol. Example input: `slptool findattrs service:wbem:https://10.0.1.2:5989`

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

SLP on UNIX systems

This section describes how to verify the SLP daemon on UNIX systems. The following are SLP file locations on UNIX systems:

- `SLP log—Management_Application/cimom /cfg/slp.log`
- `SLP daemon—Management_Application/cimom /cfg/slp.conf`

  The SLP daemon can be reconfigured by modifying `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 see http://www.openslp.org/doc/html/UsersGuide/index.html.

Verifying SLP service installation and operation on UNIX systems:

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

   NOTE: `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. The following are SLP file locations:

- `SLP log—Management_Application\cimom \cfg\slp.log`
- `SLP daemon—Management_Application\cimom\cfg\slp.conf` (the SLP daemon can be reconfigured by modifying this file).
- `SLP register—Management_Application\cimom\cfg\slp.reg`

  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 see http://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. Enter **`cd c:\Management_Application\cimom \bin`** and press `Enter` to change to the directory where `slpd.bat` is located.
5. Enter > **`slptool findsrvs service:service-agent`** and press `Enter` to verify the SLP service is running as a Service Agent.
6. Enter > **`slptool findsrvs service:wbem`** and press `Enter` to verify the SLP service is advertising its WBEM services.
7. Select one of the following options to verify the SLP service is advertising the WBEM SLP template over its configured client protocol adapters.
   - Enter > **`slptool findattrs service:wbem:http://IP_Address:Port`** and press `Enter`.
   - Enter > **`slptool findattrs service:wbem:https://IP_Address:Port`** and press `Enter`.

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

Enumeration issue with HP 2408 FCoE Converged Network Switch running on Fabric OS 6.3.x or earlier

When Network Advisor manages an HP 2408 FCoE Converged Network Switch running Fabric OS 6.3.x or earlier, connected to an FDMI enabled CNA, enumeration instance fails for the following classes:

- Brocade_EthernetPortLANEndPoint
- Brocade_EthernetAdminDomainHostedLanEndPoint
- Brocade_EndpointOfNetworkPipe Brocade_LANEndpoint
- Brocade_EthernetSwitchHostedLANEndPoint
- Brocade_InEthernetLogicalNetwork
- Brocade_PlatformHostedLANEndPoint

Instance class key property with special character

`Getinstance` operation fails if the key property value contains either a semicolon or a non-printable character.

FC port type value for imported HBAs

`Brocade_topologyview.AntecedentFCPortType` property value corresponding to the imported HBA is shown as L_Port.

Documentation Updates

For the most recent Network Advisor documentation, visit the following HP website: http://h18006.www1.hp.com/products/storageworks/dc_fabricmgr/index.html.

Under **Support**, select **HP Support & Documents**, and then select **Manuals**.

HP Network Advisor 12.0.0 fixes

Table 7 (page 21) lists the closed defects for this release.

Table 7 HP Network Advisor 12.0.0 closed defects

Closed fixes summary	Solution
Port numbers overlap when “Link Information Visibility” is enabled in the Options Dialog in L2/IP/VLAN Topology for multiple connections and trunk connections.	Fixed in Network Advisor 12.0.0.
Users are able to see the properties of a device through the static product group properties, which has been removed from an AOR.	**Workaround prior to upgrade:** Re-login into the client. Fixed in Network Advisor 12.0.0.
Users are able to see imported loop devices in the topology even after removing them from the LSAN Zone.	Fixed in Network Advisor 12.0.0.
Unable to disable MSTP on a port level for an MSTP non-instance 0.	**Workaround prior to upgrade:** Use the element manager to perform the disable. Fixed in Network Advisor 12.0.0.
The operation fails when users attempt to de-register the key vault using CLI.	**Workaround prior to upgrade:** Use double quotes around the label in CLI during deregistration. Fixed in Network Advisor 12.0.0.
SAN discovery fails with an incorrect error message when users attempt to discover an SSL-enabled switch, without enabling the SSL option in Network Advisor.	**Workaround prior to upgrade:** Enable the SSL option in the **Product Communication** tab of the **Options** dialog of Network Advisor. Fixed in Network Advisor 12.0.0.
Customers are unable to install the HP Branded SCOM package.	Fixed in Network Advisor 12.0.0.
In the Port Optics dialog, the table cannot be sorted by **Tx Power** or **Rx Power** columns.	Fixed in Network Advisor 12.0.0.
The local LIC client logs (when client is launched through the SMI-A configuration tool) are not collected when the support save operation is triggered from the Server Console.	**Workaround prior to upgrade:** Manually copy the `client.log` file along with client `supportsave` which is generated at the time of LIC client launch. Fixed in Network Advisor 12.0.0.
Customizations made to columns in the Diagnostics Results/Avg Round Trip Delay dialog of the L2 Traceroute dialog are not persisted.	Fixed in Network Advisor 12.0.0.
On NetIron MLX devices, the L3 ACL value is shown as ‘0’ in the port configuration dialog when the IPv6 access list is assigned to the ports.	Fixed in Network Advisor 12.0.0.

Table 7 HP Network Advisor 12.0.0 closed defects *(continued)*

Closed fixes summary	Solution
Cannot set port priority in excess of 240 for ServerIron ports when selected along with other non-ServerIron IOS products.	**Workaround prior to upgrade:** Select ServerIron products only (and not other non-ServerIron IOS products) to set the port priority above 240. Fixed in Network Advisor 12.0.0.
User documentation incorrectly states 'Large' configurations are not supported on a 32-bit OS.	Fixed in Network Advisor 12.0.0.
Changes to L2 links are not reflected when a profile-based re-discovery is performed.	**Workaround prior to upgrade:** Perform a manual re-discovery or wait until the next asset collection for an update to occur. Fixed in Network Advisor 12.0.0.
The Network Advisor client hangs during logical switch configuration.	**Workaround prior to upgrade:** Move the ports one slot at a time. Fixed in Network Advisor 12.0.0.
Network Advisor login through RADIUS requires two attempts.	Fixed in Network Advisor 12.0.0.
The Network Advisor client hangs for operations performed in the product tree and users are blocked to proceed until the client session is terminated manually.	Fixed in Network Advisor 12.0.0.
Periodic scheduled Network Advisor server backup is not working.	**Workaround prior to upgrade:** Perform a manual backup. Fixed in Network Advisor 12.0.0.
The master log description contains the word "FICON " even though it is a non-FICON device.	Fixed in Network Advisor 12.0.0.
The active (occupied) VE ports are not shown in the main Network Advisor display.	Fixed in Network Advisor 12.0.0.
An incorrect switch name appears in the properties tab for a given port.	Fixed in Network Advisor 12.0.0.

HP Network Advisor 12.0.1 fixes

Table 8 (page 22) lists the closed defects for this release.

Table 8 HP Network Advisor 12.0.1 closed defects

Closed fixes summary	Solution
Users may be unable to manage an encryption switch or blade due to a memory leak in the switch/blade. An `EE busy/Operation failed` error may be output.	Fixed in Network Advisor 12.0.1.
FCIP data collection fails for tunnels in a Historical graph	Fixed in Network Advisor 12.0.1.
In the IP Discovery feature, if NOS collection fails, Network Advisor polls the NOS devices at short polling time intervals.	Fixed in Network Advisor 12.0.1.

HP Network Advisor 12.0.2 fixes

Table 9 (page 23) lists the closed defects for this release.

Table 9 HP Network Advisor 12.0.2 closed defects

Closed fixes summary	Solution
RMON alerts for interface CRC errors are incorrectly interpreted by Network Advisor as CPU utilization.	Fixed in Network Advisor 12.0.2.
The Network Advisor Historical Graph option dialog does not allow selection of start date for the previous year historical data. The value set by the user reverts back to the current year.	Fixed in Network Advisor 12.0.2.
Virtualization information is missing from the VDX switches in Network Advisor.	Fixed in Network Advisor 12.0.2.
The Network Advisor server log is filled with invalid credentials errors.	Fixed in Network Advisor 12.0.2.
Stacking ports are not selectable in the Network Advisor Historical Data Collectors.	Fixed in Network Advisor 12.0.2.
Data migration fails from Network Advisor 11.3.0 to 12.0.	Fixed in Network Advisor 12.0.2.
The Power center dialog may not display the correct port information, such as port-name or status.	Fixed in Network Advisor 12.0.2.

HP Network Advisor 12.0.3 fixes

Table 10 (page 23) lists the closed defects for this release.

Table 10 HP Network Advisor 12.0.3 closed defects

Closed fixes summary	Solution
False Offline/Online events reported in Network Advisor due to ICMP processing.	Fixed in Network Advisor 12.0.3.
Client logins may fail following a migration to Network Advisor 12.0.2.	Fixed in Network Advisor 12.0.3.
Migration from Network Advisor 11.2 to 12.0.2 fails if default Event Actions are deleted before the migration. **NOTE:** HP does not support Network Advisor 11.2.	Fixed in Network Advisor 12.0.3.
Historical performance data is not migrated when upgrading to Network Advisor 12.0.1 or 12.0.2 from any prior 12.0 releases.	Fixed in Network Advisor 12.0.3.

HP Network Advisor 12.1.1 fixes

Table 11 (page 23) lists the closed defects for this release.

Table 11 HP Network Advisor 12.1.1 closed defects

Closed fixes summary	Solution
Historical data is not collected and not visible for CPU Utilization, Memory Utilization and System Uptime.	Fixed in Network Advisor 12.1.1.
MLX Discovery of the MLX router fails with PSQL exception.	Fixed in Network Advisor 12.1.1.
On a 64-bit Virtual Machine (VM), users are unable to restore a backup created by the same version of Network Advisor running on a 32-bit VM.	Fixed in Network Advisor 12.1.1.
Host port mapping fails when there is a change in the initiator/target property	Fixed in Network Advisor 12.1.1.

HP Network Advisor 12.1.3 fixes

Table 12 (page 24) lists defects closed in the HP Network Advisor 12.1.3 release.

Table 12 HP Network Advisor 12.1.3 closed defects

Closed defects summary	Solution
Cloning of MAPS policy does not copy all the current rules to the New Policy.	Fixed in Network Advisor 12.1.3.
Distribution of the MAPS 'All Fabrics' policy does not complete and the dialog becomes unresponsive.	Fixed in Network Advisor 12.1.3.

HP Network Advisor 12.1.4 fixes

Table 13 (page 24) lists defects closed in the HP Network Advisor 12.1.4 release.

Table 13 HP Network Advisor 12.1.4 closed defects

Closed defects summary	Solution
Unable to select zone DB when trying to perform zone merge from drop down menu in **Compare/Merge** dialog.	Fixed in Network Advisor 12.1.4.
FCIP compression ratios do not match between Network Advisor and CLI interface.	Fixed in Network Advisor 12.1.4.
Duplicate IP addresses are shown for devices in the Topology display.	Fixed in Network Advisor 12.1.4.
After migration, user is unable to log into the Network Advisor client using LDAP credentials.	Fixed in Network Advisor 12.1.4.
NPIV Port details are not shown in the **Virtual Connect Properties** dialog, and users are not able to perform zoning.	Fixed in Network Advisor 12.1.4.
ConnectivityMemberType is incorrectly displayed for storage with a single port of the same WWN.	Fixed in Network Advisor 12.1.4.
After historical data collectors are disabled, custom dashboard widgets for sFlow cannot be removed. The widget remains and the database continues to grow.	Fixed in Network Advisor 12.1.4.
Users are unable to load/download firmware to Fabric OS switches using an external SCP server.	Fixed in Network Advisor 12.1.4.
SMI Agent shows a remote code execution vulnerability in a Nessus scan report.	Fixed in Network Advisor 12.1.4.
The old Host Name is retained after a restore operation.	Fixed in Network Advisor 12.1.4.
When the SNMP user ID has "!", Network Advisor fails to register as an SNMP Trap recipient, and users will be unable to view the PM statistics.	Fixed in Network Advisor 12.1.4.

HP Network Advisor 12.1.5 fixes

Table 14 (page 24) lists defects closed in the HP Network Advisor 12.1.5 release.

Table 14 HP Network Advisor 12.1.5 closed defects

Closed defects summary	Solution
Fabric watch configurations cannot be done on the HP SN6000B 16Gb FC Switch through Network Advisor. Network Advisor outputs a request for a Fabric Watch license on an HP SN6000B 16Gb FC Switch even though the license is already installed on the switch.	Fixed in Network Advisor 12.1.5.
After an upgrade to Network Advisor 12.0.2 from 11.1.4, users are unable to create SNMP trap filters with all the traps under RASLog Events.	Fixed in Network Advisor 12.1.5.

Table 14 HP Network Advisor 12.1.5 closed defects *(continued)*

Closed defects summary	Solution
Transactions fail with the error: `CIM native error: No Transaction` if zoning operations are done on the Fabric simultaneously by more than one SMI Agent.	Fixed in Network Advisor 12.1.5.
When a filter is applied with virtual Switch IP address, chassis level events are not forwarded for the corresponding virtual switches. The SNMP Filter blocks Chassis level information.	Fixed in Network Advisor 12.1.5.
Migration from Network Advisor 12.0.2 to 12.1.4 is failing when the db password contains a special character. The migration is reported as successful, but at the very end, on the Start Server page, either the window does not close when the **Finish** button is selected or an error message stating `Migration Failure` appears.	Fixed in Network Advisor 12.1.5.
SNMP Traps are not received after the Network Advisor server is restarted. The Master log does not display SNMP traps.	Fixed in Network Advisor 12.1.5.
The Zoning Window displays incorrect FC addresses for ports.	Fixed in Network Advisor 12.1.5.
Users are unable to discover the Fabric because the WWN for Access Gateway (AG) is incorrectly computed which causes device discovery to fail.	Fixed in Network Advisor 12.1.5.

Effective date

March 2014