



IBM System Storage™

IBM Network Advisor v11.1.2 Release Notes

Copyright © 2011 Brocade Communications Systems, Incorporated.

Copyright © IBM Corporation 2011. All rights reserved.

Brocade, and Fabric OS are registered trademarks and the Brocade B-wing symbol and DCX, and are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. All other brands, products, or service names are or may be trademarks or service marks of, and are used to identify, products or services of their respective owners.

IBM, the IBM logo, and [ibm.com](http://www.ibm.com) are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. A complete and current list of other IBM trademarks is available on the Web at <http://www.ibm.com/legal/copytrade.shtml>

Notice: The information in this document is provided "AS IS," without warranty of any kind, including, without limitation, any implied warranty of merchantability, noninfringement or fitness for a particular purpose. Disclosure of information in this material in no way grants a recipient any rights under Brocade's patents, copyrights, trade secrets or other intellectual property rights. Brocade and IBM reserve the right to make changes to this document at any time, without notice, and assumes no responsibility for its use.

The authors, Brocade Communications Systems, Inc., and IBM Corporation shall have no liability or responsibility to any person or entity with respect to any loss, cost, liability, or damages arising from the information contained in this book or the computer programs that accompany it.

Notice: The product described by this document may contain "open source" software covered by the GNU General Public License or other open source license agreements. To find-out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit <http://www.brocade.com/support/oscd>.

Export of technical data contained in this document may require an export license from the United States Government

CONTENTS

Overview	1
Software feature overview	1
SAN Management feature enhancements	1
Migrations & upgrades	1
Operating Systems supported	2
Device platform and firmware requirements	3
Installing IBM Network Advisor	3
To install IBM Network Advisor on Windows (server)	4
To install IBM Network Advisor on Linux (server)	4
To launch the IBM Network Advisor client	4
Installation notes	4
Important SAN Notes	5
Miscellaneous Important Notes that Apply to SAN Installations	5
Removing Switches	5
Secure Fabric OS fabrics cannot be discovered from Network Advisor	5
Display of Logical switches	6
Destination columns are blank for SAN32B-E4 encryption switch in top talkers dialog	6
Firmware download through SCP Server	6
DCFM to Network Advisor remote migration is not supported	6
Common issues for SAN	6
Miscellaneous important notes that apply to SAN installations	6
Patch installer troubleshooting	7
Windows OS: Brocade Domestic Call home center	7
Linux OS: SMC - Restarting services after enabling SSL from Options dialog in RedHat Linux 5	7
Support Saves may take a long time with large databases	7
Performance Counter calculation formulas	7
Other performance counters	9
Installation on network mounted drives is not supported	9
Client disconnects	9
SMI Agent	9
Indications delivery depends on SAN size and SNMP registration	10
Logging for CIMOM	10
Service Location Protocol (SLP) support	10
Enumeration issue with SAN06B-R running on Fabric OS 6.3.x or lower	12
Instance class key property with special character	12
Getinstance operation on Brocade_Ethernetport for Fabric OS 6.1.2_CEE	12
FC port type value for imported HBA's	12
Migration Issue	13
Documentation updates	13
Defects	14
Closed with Code Change in IBM Network Advisor 11.1.2	14
Closed with Code Change in IBM Network Advisor 11.1.1a	15
Closed with Code Change in IBM Network Advisor 11.1.1	16

Overview

IBM Network Advisor 11.1 is a software management platform that unifies network management for SAN networks. IBM Network Advisor uses the best of SAN Management from Data Center Fabric Manager (DCFM) to provide users with an end-to-end view of their entire SAN networking infrastructure. It provides users with a consistent user interface across the FC and FCoE networks along with custom views and controls based on the users' areas of specialization. IBM Network Advisor is licensed and deployed to manage SAN only networks.

Software feature overview

SAN Management feature enhancements

IBM Network Advisor 11.1.2 introduces the following new SAN capabilities:

- **DCB Switches Support:** IBM Network Advisor allows users to discover and manage DCB Switches from SAN tab.
- **Host Views:** Host views are supported on SAN tab. Allows users to discover host either using HCM agent or a Virtual Machine Manager (VMM) like vCenter Server.
- **Virtualization:** Network Advisor now allows users to discover VMs directly from the vCenter.
- **Unified VLAN Management:** Allows users to configure VLANs across all of the devices managed by Network Advisor through a single unified VLAN wizard.
- **Unified ACL Management:** Allows users to consistently define and deploy ACLs across different types of devices.

IBM Network Advisor also brings forward the following capabilities found in Data Center Fabric Manager (DCFM) for SAN management with the following additional features and enhancements:

- **Policy Monitor:** Policy Monitor allows users to set up best practices for their network and run a test manually or on a scheduled basis to make sure the network is conforming to the best practices.
- **Frame Monitor:** Frame monitor provides a monitoring mechanism that allows configuring different thresholds for different type of frames and to report events whenever a count for particular frame type crosses its respective threshold.
- **D-port:** IBM Network Advisor allows users to run optical and electrical loopback and link traffic tests.
- **Bottleneck Detection:** Bottleneck Detection allows users to configure parameters and view statistics. In addition, when a bottleneck is detected, IBM Network Advisor allows users to view the topology as well as receive information on the affected hosts.
- **Microsoft System Center Operations Manager (SCOM) Management Pack:** Populates Microsoft SCOM with fabric details, switch details, statistics, and Call Home events.
- **Selective Server Support Save:** Provides the ability to include or exclude performance and historical events from the database while capturing server support save from SMC.
- IBM Network Advisor also provides digital diagnostic information on 16 G port optics, such as temperature, Rx/Tx power, bias current, and supply voltage.
- **SAN Size Check:** A popup message is displayed when the discovered port/switch/AG count exceeds the SAN size selected (small/medium/large).
- **MD5 Checksum Validation:** MD5 Checksum validation is done before importing firmware files into Repository.

Migrations & upgrades

DCFM Migration: DCFM 10.4.x running on the Linux and Windows operating systems can be upgraded to IBM Network Advisor 11.1.x for SAN. DCFM 10.4.x running on the Solaris platform must first migrate to a supported operating system, and then perform the upgrade to IBM Network Advisor 11.1.x for SAN.

Prior versions of DCFM would need to be first upgraded to DCFM 10.4.x and then perform the upgrade to IBM Network Advisor 11.1.x. Upgrades from DCFM to IBM Network Advisor 11.1.x for SAN do not require a new software license key.

Operating Systems supported

IBM Network Advisor 11.1.x is supported on the following operating systems.

Table 1 Server / Client Operating System Support

Operating System (architecture) / Installer	Versions
Windows	<ul style="list-style-type: none"> • Windows Server 2003 Std SP2 (x86 32-bit) • Windows 2008 Std (x86 32-bit) • Windows XP Pro SP3 (x86 32-bit) • Windows 7 Professional Edition (x86 32-bit)
Windows Server	<ul style="list-style-type: none"> • Windows Server 2008 R2 (x86 64-bit) Data Center, Standard and Enterprise Edition
Linux VMWare	<ul style="list-style-type: none"> • RedHat AS 4.8 (x86 32-bit) • RedHat Enterprise Linux 5.5 Adv (x86 32-bit) • SUSE Linux Enterprise Server 10 SP1, 11 (x86 32-bit) • Oracle Enterprise Linux 5.5 (x86 32-bit) <p>VMWare ESX 4.0, ESX 4.1 and VCenter 4.1 with Guest VMs of:</p> <ul style="list-style-type: none"> • Windows Server 2003 Std SP2 (x86 32-bit) • Windows Server 2008 Std (x86 32-bit) • Windows Server 2008 R2 (x86 64-bit) Data Center, Standard and Enterprise Edition • RedHat Enterprise Linux 5.5 Adv (x86 32-bit) • SUSE Linux Enterprise Server 10 SP1, 11 (x86 32-bit) • Oracle Enterprise Linux 5.5 (x86 32-bit)

Device platform and firmware requirements

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

Operating System	IBM Switch/Director	Brocade Switch/Director
Switch (b-type and B-Model) firmware versions		
FOS 5.0.x, 5.1.x, 5.2.x, 5.3.x, 6.0.x, 6.1.x, 6.2.x, 6.3.x, and 6.4.x	SAN32B-2 (2005-B32, -32B) SAN04B-R (2005-R04) SAN18B-R (2005-R18) SAN16B-2 (2005-B16, -16B) SAN64B-2 (2005-B64) SAN32B-3 (2005-B5K, -5KB) SAN24B-4 Express (2498-B24, -24E) SAN40B-4 (2498-B40, -40E) SAN80B-4 (2498-B80) IBM Converged Switch B32 (3758-B32) ¹ SAN06B-R (2498-R06) VA-40FC SAN256B (2109-M48) SAN384B (2499-192) SAN768B (2499-384) SAN384B-2 (2499-416) SAN768B-2 (2499-816)	Brocade 4100 Brocade 7500E Brocade 7500 Brocade 200E Brocade 4900 Brocade 5000 Brocade 300 Brocade 5100 Brocade 5300 Brocade 7800 Brocade 8000 VA-40FC Brocade 4800 Brocade DCX-4S Brocade DCX Brocade DCX 8510-4 Brocade DCX 8510-8

Operating System	IBM Switch/Director	Brocade Switch/Director
Switch (m-type, M-Model) firmware versions		
M-EOSc 9.6.x, 9.7.x, 9.8.x, and 9.9.x	SAN16M-2 (2026-416, -16E) SAN32M-2 (2027-432, -32E) SAN140M (2027-140)	Spheron 4400 Brocade M4700 Brocade M6140
M-EOSn 9.6.x, 9.7.x, 9.8.x, and 9.9.x	SAN256M (2027-256)	Brocade Mi10K

Installing IBM Network Advisor

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

- Microsoft Windows
- Linux

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

To install IBM 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 instructions to complete the installation.

To install IBM 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 instructions to complete the installation.

To launch the IBM Network Advisor client

- To launch the IBM Network Advisor Client on the same local machine as the Network Advisor Server, launch the client as follows:

Windows: Select **Start > Programs > Network Advisor 11.1.x > Network Advisor 11.1.x**

Windows:

- Client can be launched from the Desktop icon.
- Launch command prompt and go to the location "<Install location>/bin" and enter "**dcmclient**"

Linux:

- Client can be launched from the Desktop icon.
- Launch terminal and go to the location "<Install location>/bin" and enter "**sh dcmclient**"

Windows and Linux: Follow the steps below for launching the client from a web browser.

- To launch the IBM Network Advisor Client from a remote host, launch the client as follows:

Open a browser window and type the IBM Network Advisor server hostname or IP address in the **Address** field; for example:

<http://NetworkAdvisorServerhost1.companyname.com/>

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

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

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

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

Note that the required Client Oracle JRE version has now changed to 1.6.0_24. For remote clients, this JRE needs to be installed prior to establishing a server connection.

Installation notes

- On Linux, the Network Advisor installer becomes unresponsive at the 'Initialize Database' step of the Configuration Wizard, if a value lesser than 1024 is provided for the database port.

Important SAN Notes

This section lists information that you should consider before you use IBM Network Advisor 11.1.x.

Miscellaneous Important Notes that Apply to SAN Installations

1. TSB 2011-106-A has been corrected (Manageability servers running DCFM 10.4.0, 10.4.1, 10.4.2, 10.4.3, 10.4.4 or Network Advisor 11.0.0 run out of application memory if they are managing SAN Switch M14 or SAN256B directors for several weeks. The result is recurring server restarts)
2. DCFM 10.4.x and Network Advisor 11.0.x will not be able to manage products running Fabric OS v7.0 and beyond. To manage those products, customers should upgrade the management application first to IBM Network Advisor 11.1.x before upgrading the products to Fabric OS v7.0.
3. Host based stand-alone SMI agents cannot manage products with Fabric OS v7.0. It requires use of the integrated SMI Agent with IBM Network Advisor 11.1.x.
4. While running diagnostic port test, it is important to note that selecting more than one port from same switch/blade and running diagnosis on them simultaneously might result in failure. It is recommended to choose only one port at a time from any given switch/blade for running the diagnostic port test.
5. If a fabric has a large zone database or effective zone configuration (~1MB), zoning report generation may fail.
6. If IPv6 is enabled on the Fabric OS switch, as well as the Network Advisor server host, then IPv6 will be chosen mode of communication between server and switch.
7. When the user migrates from the DCFM 10.4.x to IBM Network Advisor 11.1.x, it is expected the corresponding DCFM application service to be up and running. The GUI message shown when the DCFM server is not running prompts the user to start the Network Advisor service rather than the DCFM application service.
8. When any FOS switch is upgraded from 6.4.x to 7.x.x firmware and downgraded again to 6.4.x, DCFM 10.4.x servers will show caution badge on switches and Discovery status will not reflect the reason for status.
9. A firmware upgrade to the IBM SAN06B-R (2498-R06) platform using IBM Network Advisor will be disruptive to I/O on the switch.

Removing Switches

If you plan to segment and remove more than two switches from a fabric and you have **Historical performance collection** enabled, then it is recommended that you accept changes after each switch segmentation from the client rather than doing it all at one time; or alternatively, switch off **track fabric changes**.

Secure Fabric OS fabrics cannot be discovered from Network Advisor

Network Advisor does not support Secure FOS (SFOS). If you attempt to discover the fabric, Network Advisor displays an error message that "Discovery Failed". You will have to remove the secure FOS setting and change it back to a normal fabric before discovering the fabric from IBM Network Advisor.

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 have to rediscover the newly created logical switch fabric.

Destination columns are blank for SAN32B-E4 encryption switch in top talkers dialog

When the **Top Talkers** dialog box is launched for the SAN32B-E4 Encryption Switch, the columns, **Destination**, **Destination port**, and **Destination switch port** are sometimes empty.

Firmware download through SCP Server

If you use the Windows-based SCP Server, a firmware download will fail for the switches. It is recommended you use the Linux-based SCP Server.

DCFM to Network Advisor remote migration is not supported

Remote migration is not supported to IBM Network Advisor. It is recommended that you first migrate from DCFM 10.3.x / 10.4.x to another DCFM 10.3.x / 10.4.x server, and then migrate to IBM Network Advisor.

Common issues for SAN

Miscellaneous important notes that apply to SAN installations

1. Privileges related to SAN features are prefixed with 'SAN -' strings. After migration from an older version, new privilege names will be displayed in the **Role Management** dialog with these prefixes.
2. The rollover of wrapper log files may cause the server running on Linux to crash. If this issue is encountered, you must terminate the *dcmsvc* process from task manager and restart the server from the **Server Console**.
3. If a custom AOR without any host included is manually assigned to a defined user, all hosts are displayed in topology to that user. But deleting/updating hosts will not be reflected in the topology for that user until the Client is restarted.
4. IBM Network Advisor server startup and restart can take up to 10+ minutes to complete.
5. Authentication: Fallback authentication may not work when LDAP server running on Windows 2008 R2 is used as the primary authentication and local database is the secondary authentication. This is because the error code returned is the same for both "invalid credential" and "user not found".
6. When configuring IBM Network Advisor in SSL enable mode in the application configuration wizard, ensure that both HTTP and HTTPS ports are free and available for IBM Network Advisor. Currently the application checks only if the HTTPS configured port is available and not the HTTP port.
7. Port disable/enable operation on physical TE-Ports might fail in below scenarios:
 - a. Disabling the virtual FCoE ports of DCB switches of the corresponding physical TE-Ports through **CLI/Web Tools**.
 - b. Removing the FCoE device connected to the ports.

DCB asset collection will fail if the trunks are configured for the TE-ports. The user will not get updates such as port status, lag, and trunk information for the DCB switch. The user will need to delete the fabric and rediscover it from the **Discovery** dialog to overcome this issue.

- An FTP transfer from a Brocade Network Advisor Technical Support Repository dialog to a Cerberus FTP Server and an AIX built-in FTP server, does not work.

Patch installer troubleshooting

Patch installer may not launch if UAC is enabled on a Windows 7/2008/2008R2 Editions. User has to first disable the UAC using the procedure provided in the **Troubleshooting** section of the User Manual, and then launch the patch installer.

Windows OS: Brocade Domestic Call home center

To support Brocade Domestic dial-up Call home center with Windows users, add the below entry in the **hosts** file present in Windows\System32\drivers\etc folder:

“192.168.0.1 Notify1”

Linux OS: SMC - Restarting services after enabling SSL from Options dialog in RedHat Linux 5

When the setting of SSL fails from the Options dialog box, complete the following steps to enable SSL:

- Close the client.
- Stop the services from SMC.
- Relaunch the **Configuration wizard** and enable SSL from the wizard.
- Close and relaunch SMC.
- Start services from SMC.
- Launch the client.

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 will promote longer Support Save operations. Make sure you have a minimum of 20GB disk space for Support Save and Backup operations.

Performance Counter calculation formulas

Counter Name	Type	Protocol used	Source value	Formula
TX	FC	SNMP	.1.3.6.1.3.94.4.5.1.6	$TX = (\text{Delta value}^1 / (1000 * 1000)) / (\text{Polling interval}^2 / 1000)$
RX	FC	SNMP	.1.3.6.1.3.94.4.5.1.7	$RX = (\text{Delta value}^1 / (1000 * 1000)) / (\text{Polling interval}^2 / 1000)$
TX	GE	SNMP	.1.3.6.1.2.1.31.1.1.1.10	$TX = (\text{Delta value}^1 / (1000 * 1000)) / (\text{Polling interval}^2 / 1000)$
RX	GE	SNMP	.1.3.6.1.2.1.31.1.1.1.6	$RX = (\text{Delta value}^1 / (1000 * 1000)) / (\text{Polling interval}^2 / 1000)$
TX	FCIP	SNMP	.1.3.6.1.2.1.31.1.1.1.10	$TX = (\text{Delta value}^1 / (1000 * 1000)) / (\text{Polling interval}^2 / 1000)$

Counter Name	Type	Protocol used	Source value	Formula
RX	FCIP	SNMP	.1.3.6.1.2.1.31.1.1.1.6	$RX = (\text{Delta value}^1 / (1000 * 1000)) / (\text{Polling interval}^2 / 1000)$
TX	EE Monitors	HTTP	PortRX (variable from the return html file)	$TX = (\text{Delta value}^1 / (1000 * 1000)) / (\text{Polling interval}^2 / 1000)$
RX	EE Monitors	HTTP	PortTX (variable from the return html file)	$RX = (\text{Delta value}^1 / (1000 * 1000)) / (\text{Polling interval}^2 / 1000)$
TX	HBA, CNA	HCM API	NA	$TX = (\text{Delta value}1 / (1000 * 1000)) / (\text{Polling interval}2 / 1000)$
RX	HBA, CNA	HCM API	NA	$RX = (\text{Delta value}1 / (1000 * 1000)) / (\text{Polling interval}2 / 1000)$
TX	TE	SNMP	.1.3.6.1.2.1.2.2.1.11 + .1.3.6.1.2.1.31.1.1.1.2 + .1.3.6.1.2.1.31.1.1.1.3	$TX = (\text{Delta value}1 / 1000) / (1000 * 1000)$
RX	TE	SNMP	.1.3.6.1.2.1.2.2.1.17 + .1.3.6.1.2.1.31.1.1.1.4 + .1.3.6.1.2.1.31.1.1.1.5	$RX = (\text{Delta value}1 / 1000) / (1000 * 1000)$
TX% / RX%	FC, GE, FCIP, HBA, CNA	NA	NA	$TX\% \text{ or } RX\% = ((TX \text{ or } RX) / ((105000000 * \text{port speed}) * (\text{Polling interval}2 / 1000.00))) * 100$ If Utilization is less than 1 then the value is it to 0.0
TX% / RX%	TE	NA	NA	$\text{value} = (TX \text{ or } RX) / 10;$ $TX\% \text{ or } RX\% = ((\text{value}) / ((105000000 * \text{port speed}) * (1000 / 1000.00))) * 100$ if Utilization is less than 1 then the value is it to 0.0
Compression Ratio	FCIP		.1.3.6.1.4.1.1588.4.1.1.4	Compression Ratio = current value/ 1000 Since for compression ratio we will take the current compression ratio value
Receive EOF	TE		.1.3.6.1.2.1.16.1.1.1.5	Receive EOF = Delta value1 / (1000 * 1000)
Other Counters				Other counters = Delta value1

- 1) Delta value¹: is the difference of value retrieved between the two consecutive poling cycles.
- 2) Polling interval²: duration between the two polling cycle

Other performance counters

The other counters are listed in the table below

Counter Name	Type	Protocol used	Source value
CRC Errors	FC	SNMP	.1.3.6.1.3.94.4.5.1.40
Signal Losses	FC	SNMP	.1.3.6.1.3.94.4.5.1.43
Sync Losses	FC	SNMP	.1.3.6.1.3.94.4.5.1.44
Link Failures	FC	SNMP	.1.3.6.1.3.94.4.5.1.39
Sequence Errors	FC	SNMP	.1.3.6.1.3.94.4.5.1.42
Invalid Transmissions	FC	SNMP	.1.3.6.1.3.94.4.5.1.41
Rx Link Resets	FC	SNMP	.1.3.6.1.3.94.4.5.1.33
Tx Link Resets	FC	SNMP	.1.3.6.1.3.94.4.5.1.34
C3 Discard	FC	SNMP	.1.3.6.1.3.94.4.5.1.28
Latency	FCIP	SNMP	.1.3.6.1.4.1.1588.4.1.1.5
Dropped Packets	FCIP	SNMP	.1.3.6.1.4.1.1588.4.1.1.3
Link Retransmits	FCIP	SNMP	.1.3.6.1.4.1.1588.4.1.1.2
Timeout Retransmits	FCIP	SNMP	.1.3.6.1.4.1.1588.4.1.1.9
Fast Retransmits	FCIP	SNMP	.1.3.6.1.4.1.1588.4.1.1.10
Duplicate Ack Received	FCIP	SNMP	.1.3.6.1.4.1.1588.4.1.1.11
Window Size RTT	FCIP	SNMP	.1.3.6.1.4.1.1588.4.1.1.12
TCP Out of Order Segments	FCIP	SNMP	.1.3.6.1.4.1.1588.4.1.1.13
SlowStart Status	FCIP	SNMP	.1.3.6.1.4.1.1588.4.1.1.14
CRC Errors	EE Monitors	HTTP	PortCRC (variable from the return html file)

Installation on network mounted drives is not supported

Installation onto a windows network mounted drive is not supported but install is allowed and DB fails to start.

Client disconnects

Under heavy server load or degraded network links, there is a potential for Network Advisor client to get disconnected from the server. Work around is to restart the client.

SMI Agent

1. If SMI client queries CIMOM server for more than one fabric, and if each fabric has a large zone database (~1MB), then Enumerate Instances operation on Brocade_ZonemembershipsettingdataInZone will fail. In this scenario, it is recommended to use the association traversal approach via Brocade_Fabric to retrieve the larger zone databases.
2. 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 Network Advisor server is successfully registered for traps on all switches.
3. If DCB switches are running Fabric OS 6.3.x and 6.3.1_cee, VLAN/ACL deployment through SMI-A will fail. It is required to upgrade the DCB Fabric OS to 6.4.x/6.3.1_dcb/7.0.0 for VLAN/ACL deployment support through SMI Agent.

Indications delivery depends on SAN size and SNMP registration

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

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

Logging for CIMOM

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

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

Logging Level, File size and Number of Log files can be changed by modifying the following fields: "Log Level", "File Size" and "Number of Files" from 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:

- slpd script starts the slpd platform
- slpd program acts as a Service Agent (SA). A different slpd binary executable file exists for UNIX and Windows systems.
- slptool script starts the slptool platform-specific program
- slptool program can be used to verify whether SLP is operating properly or not. 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:

- 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 functionalities of Management application SMI Agent:

- accepts WBEM requests over HTTP using SSL on TCP port 5989
- 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: Where `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: Where `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.

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 SLP APIs by modifying this file. For more information about these files, read the comments contained in them, or refer to <http://www.openslp.org/doc/html/UsersGuide/index.html>

Verifying SLP service installation and operation on UNIX systems:

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

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

SLP on Windows systems

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

SLP file locations:

- SLP log—Management_Application\cimom\cfg\slp.log
- SLP daemon—Management_Application\cimom\cfg\slp.conf

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

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

Enumeration issue with SAN06B-R running on Fabric OS 6.3.x or lower

Enumeration instance fails for the following classes:

Brocade_EthernetPortLANEndPoint, Brocade_EthernetAdminDomainHostedLanEndPoint,
Brocade_EndpointOfNetworkPipe, Brocade_EthernetSwitchHostedLANEndPoint,
Brocade_InEthernetLogicalNetwork, Brocade_LANEndpoint,
Brocade_PlatformHostedLANEndPoint

When Network Advisor manages a SAN06B-R running on Fabric OS 6.3.x or lower, connected to FDMI enabled CNA.

Instance class key property with special character

Getinstance operation fails if the key property value contains semicolon or non printable character.

Getinstance operation on Brocade_Ethernetport for Fabric OS 6.1.2_CEE

Brocade_Ethernetport information could not be fetched through Getinstance operation if CEE switch runs on Fabric OS 6.1.2_CEE

FC port type value for imported HBA's

Brocade_topologyview.AntecedentFCPortType property value corresponding to the imported HBA is shown as L- port.

Migration Issue

Properties configured in the SMI Agent Configuration Tool do not migrate from DCFM 10.4.0 (Solaris) to DCFM 10.4.0 (Windows) through the Copy Data and Settings screen when migrating from DCFM 10.4.0 (Solaris) to DCFM 10.4.0 (Windows) to IBM Network Advisor 11.1.1 (Windows).

Documentation updates

The most recent IBM Network Advisor 11.1.x documentation manuals are available on the IBM Support Portal site: www.ibm.com/supportportal. In the IBM Support Portal, select or enter the product name, and then select **Documentation**. Navigate to the desired publications in the displayed results.

Defects

Closed with Code Change in IBM Network Advisor 11.1.2

This section lists the defects with Critical and High Technical Severity closed with a code change in IBM Network Advisor as of November 18, 2011.

Defect ID: DEFECT000355813	Technical Severity: High
Summary: Call Home notifications are not received for IBM 2499 machine type switches, for events with the ID MS-1009.	
Symptom: For events with the ID MS-1009, user will not receive Call Home notifications.	
Feature: FAULT MANAGEMENT	Function: ENHANCEMENT
Probability: Medium	
Found in Release: DCFM10.4.0	Service Request ID: 631907

Defect ID: DEFECT000364915	Technical Severity: Medium
Summary: Brocade_Switchfcportstats.BBCreditZero property value is incorrectly populated for EOS switches.	
Symptom: Incorrect property value will be shown in the 3rd party management application.	
Feature: SMI Agent	Function: CIMOM
Probability: Low	
Found in Release: DCFM10.4.0	Service Request ID: 644543

Closed with Code Change in IBM Network Advisor 11.1.1a

This section lists the defects with Critical and High Technical Severity closed with a code change in IBM Network Advisor as of October 10, 2011.

Defect ID: DEFECT000362741	Technical Severity: Medium
Summary: "Base Fabric for Transport" in Logical Switches dialog is confusing to the user, it should also mention 'XISL' in the text..	
Symptom: The terminology 'Base Fabric for Transport', used to refer to XISL, can appear to be ambiguous if the text 'XISL' is not specifically mentioned.	
Feature: Virtual Fabrics	Function: Partitioning Dialog
Probability: Medium	
Found in Release: Network Advisor 11.1.2	

Defect ID: DEFECT000362743	Technical Severity: Medium
Summary: An error message is not displayed in the Configure Storage Encryption dialog for targets and Initiators that are not zoned.	
Symptom: Containers can be created even if Initiator and Targets are not in same L2 zone	
Feature: Encryption	Function: ENHANCEMENT
Probability: Medium	
Found in Release: Network Advisor 11.1.2	

Closed with Code Change in IBM Network Advisor 11.1.1

This section lists the defects with Critical and High Technical Severity closed with a code change in Network Advisor as of August 16, 2011

Defect ID: DEFECT000347713	Technical Severity: High
Summary: Allow/Prohibit Matrix – ASM is not set when activating the Active Configuration with Active=Save option enabled in the Active Matrix confirmation dialog.	
Symptom: ASM bit is not set when activating the configuration file.	
Workaround: Close the dialog and reopen it to enable the ASM bit.	
Feature: PDCM	Function: USABILITY
Probability: Low	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000350309	Technical Severity: High
Summary: FICON – Configure cascaded FICON operation failed while setting HIF and no reason is displayed for the failure.	
Symptom: Configure cascaded FICON operation fails.	
Feature: FICON	Function: Cascaded FICON Configuration
Probability: Low	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000350497	Technical Severity: High
Summary: SMIA - ModifyRole() method for DCB devices fails to modify the complete rule of an ACL policy	
Symptom: Unable to modify the ACTION field "Permit/Deny" through ModifyRole() invoke method.	
Feature: SMI Agent	Function: CEE Switch Support SubProfile
Probability: High	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000351606	Technical Severity: High
Summary: Boot image update failed with error message for windows and VMware ESX host.	
Symptom: User will not be able to update boot image.	
Feature: HBA Management	Function: BIOS Mgmt
Probability: Medium	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000351792	Technical Severity: High
Summary: Installer - Installation hangs at 'Initialize Database' when non-default database port number is given in Server Configuration page of Configuration Wizard	
Symptom: User will not be able to complete the installation when the non-default port is used for the database.	
Feature: Installers	Function: USABILITY
Probability: High	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000352404	Technical Severity: High
Summary: Driver Download: Help dialog is not getting launched in driver repository dialog.	
Symptom: User will not be able to launch the Help dialog for the Driver repository.	
Feature: HBA Management	Function: Bulk Driver Configuration
Probability: Medium	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000353970	Technical Severity: High
Summary: Encryption: Add new LUN path does not remember previous settings in the LUN selection screen	
Symptom: User is required to re-apply the LUN setting in the ' LUN view' dialog	
Feature: Encryption	Function: CONFIGURATION
Probability: Low	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000340676	Technical Severity: Medium
Summary: VMM: Duplicate ESX host entries are shown in Product Tree for all the discovered vCenters after the fabric connected to the ESX host is unmonitored and monitored	
Symptom: Duplicate Host entries shown in Product tree	
Feature: VM Support	Function: Host Product Tree UI
Probability: Low	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000342018	Technical Severity: Medium
Summary: FICON – Merge Operation failed with the Error “Internal error occurred - Failed to perform the requested cascaded FICON merge configurations.”	
Symptom: Merge operation fails without appropriate message.	
Feature: FICON	Function: Cascaded FICON Merge
Probability: Low	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000344011	Technical Severity: Medium
Summary: VMM: Deleting a vCenter fails when the fabric is unmonitored but a host is still being managed by the vCenter	
Symptom: vCenter deletion fails and error message “Error during delete discovery Internal error” is displayed.	
Workaround: Relaunch the dialog and delete the vCenter	
Feature: VM Support	Function: VM Discovery Setup
Probability: Low	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000348771	Technical Severity: Medium
Summary: Changing Top Talkers from Tx to Rx fails with error	
Symptom: Error (buffering failed) is displayed when changing Top Talker Flows from Tx to Rx.	
Feature: Performance Management	Function: Top Talkers
Probability: Medium	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000349188	Technical Severity: Medium
Summary: Fabric Binding – Setting SCC policy failed with the reason unable to establish connection to the switch.	
Symptom: SCC policy is not configured on the fabric	
Feature: Fabric Binding & HIF	Function: USABILITY
Probability: Low	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000349291	Technical Severity: Medium
Summary: LSAN Zoning: In LSAN zoning dialog, Alias name is not shown in the WWN-fabric assigned potential member panel	
Symptom: User will not be able to see the alias name in the LSAN Zoning dialog for FAPWWN members	
Feature: ZONING	Function: LSAN Zoning Dialog
Probability: Low	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000349786	Technical Severity: Medium
Summary: Ping or traceroute from FCIP Troubleshooting times out	
Symptom: Ping or traceroute fails when IP interfaces and crossport interfaces are defined on XGE ports.	
Feature: FCIP	Function: USABILITY
Probability: Low	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000350271	Technical Severity: Medium
Summary: Support save collection for HBA/CNA fails when SSL is enabled.	
Symptom: Support save collection fails.	
Workaround: Use without SSL mode or use standalone HCM with SSL mode.	
Feature: HBA Management	Function: HCM Integration
Probability: High	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000351026	Technical Severity: Medium
Summary: Event Actions are getting triggered for both Syslogs as well as SNMP traps.	
Symptom: All raslog based messages will trigger event actions for SNMP Traps and Syslogs.	
Feature: FAULT MANAGEMENT	Function: Event Processing
Probability: Low	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000351441	Technical Severity: Medium
Summary: The product tree in the event actions dialog shows E Trunk Ports even when UseSelfIndex option is not selected.	
Symptom: Cannot create event action while selecting a switch with E Port trunks configured on it.	
Workaround: Provide the IP address in the Provide IP address, WWN, source name text box.	
Feature: FAULT MANAGEMENT	Function: Event Processing
Probability: Medium	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000351688	Technical Severity: Medium
Summary: Master Log – Incorrect Description and details are displayed for the link failure event.	
Symptom: Incorrect details are displayed in the Master Log event description.	
Feature: FAULT MANAGEMENT	Function: Master Log
Probability: Medium	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000351889	Technical Severity: Medium
Summary: Logical Switches – Failed to unbind the addresses from the ports when moved between the logical switches.	
Symptom: Unbind port addresses operation is not successful	
Feature: Virtual Fabrics	Function: Partitioning Dialog
Probability: Medium	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000352018	Technical Severity: Medium
Summary: If LKM certificate has value other than Decru the BES will not accept the certificate from DCFM	
Symptom: When attempting to link the BES to an LKM key vault, if the SSL certificate of the LKM has a value other than Decru, Inc. for the Organization field, the BES will not accept the certificate from DCFM. The following error is displayed by DCFM when attempting to import the certificate: The primary key vault certificate is not issued by the key vault vendor. Either the key vault type is set incorrectly, or the wrong certificate has been loaded for the primary key vault.	
Workaround: Use CLI rather than DCFM to import and register the LKM certificate if the value has been changed from Decru to something else.	
Feature: Encryption	Function: CONFIGURATION
Probability: Low	
Found in Release: DCFM10.4.2	Service Request ID: 601119

Defect ID: DEFECT000352407	Technical Severity: Medium
Summary: Customer's log is flooded by SNMPUSM message.	
Symptom: Customer observes many SNMPUSM messages in the DCFM log. Info sw7B 137.156.140.100 Security Event SNMPUSM stats not in time window on 137.156.140.100 Thu Feb 03 07:15:11 CET 2011 Thu Feb 03 07:15:12 CET 2011 Thu Feb 03 07:15:11 CET 2011 Thu Feb 03 07:15:11 CET 2011 2 10412 20:00:08:00:88:29:B6:20 Info sw7B 137.156.140.100 Security Event SNMPUSM stats not in time window on 137.156.140.100 Thu Feb 03 06:42:10 CET 2011 Thu Feb 03 06:42:11 CET 2011 Thu Feb 03 06:42:10 CET 2011 Thu Feb 03 06:42:10 CET 2011 2 10412 20:00:08:00:88:29:B6:20 Info sw7B 137.156.140.100 Security Event SNMPUSM stats not in time window on 137.156.140.100 Thu Feb 03 06:09:09 CET 2011 Thu Feb 03 06:09:09 CET 2011 Thu Feb 03 06:09:09 CET 2011 1 10412 20:00:08:00:88:29:B6:20	
Feature: UNDETERMINED	Function: UNDER REVIEW
Probability: Low	
Found in Release: DCFM10.4.1	Service Request ID: 599107

Defect ID: DEFECT000352989	Technical Severity: Medium
Summary: Master Log: Invalid characters (series of numbers like OID) is displayed in the Description of Master Log Event	
Symptom: User will be shown incorrect description in the Master Log.	
Feature: FAULT MANAGEMENT	Function: SNMP Registration
Probability: Medium	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000353735	Technical Severity: Medium
Summary: BNA is trying to backup EOS fabrics when backup all fabrics is checked.	
Symptom: BNA will attempt to backup EOS fabrics when backup all fabrics is checked.	
Feature: Configuration Management	Function: SAN - Scheduled Backup
Probability: Low	
Found in Release: Network Advisor11.0.0	

Defect ID: DEFECT000353797	Technical Severity: Medium
Summary: Moving ICL ports to another logical switch reports an "operation not supported" message when unbind option is selected.	
Symptom: An error message "The indicated partition does not support this operation " will be displayed.	
Feature: Virtual Fabrics	Function: USABILITY
Probability: Low	
Found in Release: DCFM10.4.5	

Defect ID: DEFECT000354536	Technical Severity: Medium
Summary: Performance Management - Clear Counters Progress bar does not get closed even after the process is completed	
Symptom: User will be shown the progress bar until the client is closed and relaunched.	
Feature: Performance Management	Function: PMSERVICE
Probability: Low	
Found in Release: DCFM10.4.5	