



IBM System Storage®

IBM Network Advisor v12.1.6

Release Notes (Updated October 14, 2014)

Copyright © 2014 Brocade Communications Systems, Incorporated.

Copyright © IBM Corporation 2014. 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

Release overview	4
Software feature overview	4
SAN Management feature enhancements	4
Migrations & upgrades	4
Operating Systems supported	5
JRE support	6
Device platform and firmware requirements	6
Installing IBM Network Advisor	7
To install IBM Network Advisor on Windows (Server).....	7
To install IBM Network Advisor on Linux (Server).....	7
To launch the IBM Network Advisor client	7
Important SAN Notes	8
Display of Logical switches	10
Destination columns are blank for SAN32B-E4 Encryption Switch in top talkers dialog	10
SSL connections using certificates with MD5 signatures.....	10
Reset Ports operation in Logical Switches dialog	11
Common issues for SAN	11
Miscellaneous important notes that apply to SAN installations.....	11
Patch installer troubleshooting	12
Support Saves may take a long time with large databases	12
Installation on network mounted drives is not supported	12
Client disconnects	12
Performance Statistics Counters - Calculation Formulae	13
SMI Agent	15
Indications delivery depends on SAN size and SNMP registration.....	15
Logging for CIMOM	15
Service Location Protocol (SLP) support	16
Enumeration issue with SAN06B-R running on Fabric OS 6.3.x or lower	18
Instance class key property with special character	18
FC port type value for imported HBA's.....	18
Documentation updates	18
Defects	19
Closed with Code Change in IBM Network Advisor 12.1.6	19

Release overview

IBM Network Advisor 12.1.6 is a software maintenance release based on IBM Network Advisor 12.1.5. All hardware platforms and features supported in IBM Network Advisor 12.1.5 are also supported in IBM Network Advisor 12.1.6. The fixes included in this release are listed in the defect tables at the end of this document.

IBM Network Advisor is a software management platform for SAN networks. IBM Network Advisor uses the best of SAN Management from IBM 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 12.1.6 supports all the same hardware platforms and features and includes the following SAN capabilities and enhancements:

- 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

Migrations & upgrades

IBM Network Advisor Upgrades: IBM Network Advisor 11.1.X (11.1.0 - 11.1.5), 12.0.x (12.0.2 – 12.0.4), and 12.1.x (12.1.3 and 12.1.5) running on the Linux and Windows operating systems can be upgraded to IBM Network Advisor 12.1.6.

Note: Migrations from pre-12.0.2 to 12.1.6, require that the pre-12.0.2 IBM Network Advisor installation be running. Partial and Network path migrations are not supported from pre-12.0.2 to 12.0.6. Refer to “Configuring backup” section of “Chapter 5- Application Configuration” in *IBM Network Advisor User Manual* for the configuration backup procedure. Refer to “Chapter 3 - Data Migration” in the *Installation and Migration Guide* for more details about migration.

DCFM Migration: DCFM 10.4.x running on the Linux and Windows operating systems can be upgraded to IBM Network Advisor 11.1.x (11.1.0 - 11.1.5) for SAN first, then upgraded to IBM Network Advisor 12.0.4, and then to IBM Network Advisor 12.1.6. DCFM 10.4.x running on the Solaris platform must first be migrated to a supported operating system, and then upgraded to IBM Network Advisor 11.1.x for SAN, upgraded to IBM Network Advisor 12.0.4, and then finally to IBM Network Advisor 12.1.6. Prior versions of DCFM would need to be first upgraded to DCFM 10.4.x and then upgraded as listed above. Upgrades from DCFM to IBM Network Advisor 12.1.6 for SAN do not require a new software license key.

Operating Systems supported

IBM Network Advisor 12.1.6 is supported on the following operating systems.

Note: The minimum required system physical memory for running IBM Network Advisor 12.1.6 (server plus one local client) for the different editions is as listed below:

- Pro-plus and Enterprise Editions (supported on 64-bit OS only):
 - Small SAN fabric network: 8GB
 - Any combination that includes a medium/large SAN fabric network: 16GB

Table 1 64-bit Server / Client Operating System Support

Operating System (architecture) / Installer	Versions
Windows	<ul style="list-style-type: none"> • Windows 7 Enterprise • Windows 8 Enterprise
Windows Server	<ul style="list-style-type: none"> • Windows Server 2008 R2 Data Center, Standard, and Enterprise Edition • Windows Server 2012 Standard, Datacenter
Linux	<ul style="list-style-type: none"> • 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

Table 2 32-bit Server / Client Operating System Support

Operating System (architecture) / Installer	Versions
Windows	<ul style="list-style-type: none"> • Windows 2008 Standard (x86) • Windows 7 Professional Edition (x86)
Linux	<ul style="list-style-type: none"> • RedHat Enterprise Linux 6.1 Adv (x86) • RedHat Enterprise Linux 6.2 Adv (x86) • RedHat Enterprise Linux 6.3 Adv (x86) • Oracle Enterprise Linux 6.1 (x86) • Oracle Enterprise Linux 6.2 (x86) • Oracle Enterprise Linux 6.3 (x86) • SUSE Linux Enterprise Server 11 (x86)

JRE support

IBM Network Advisor version	JRE version supported
12.0.2	JRE 1.7u17
12.0.3, 12.1.2, 12.1.3	JRE 1.7u25
12.0.4, 12.1.4, 12.1.5	JRE 1.7u45
12.1.6	JRE 1.7u45 and JRE 1.7u51 [Windows] 1.7u67 [Linux]

Note 1: Web Tools launched from IBM Network Advisor is also supported for the above combinations.

Note 2: On Linux, Oracle enforces the latest JRE patch to be used for web starting the applications. At the time of this release, JRE 1.7u67 is the recommended version which is set to expire on 11/15/2014, beyond which user will see the following error message when launching the client: "Your Java version is out of date"

At that point of time, user needs to download the latest JRE 1.7 patch released by Oracle. Note that the user will see the below warning when launching the client when the latest JRE 1.7 patch is used but this warning can be ignored: "The client is not running the recommended java version 1.7.0_45 or 1.7.0_51. Do you want to continue?"

This is only applicable for clients launched on Linux Operating System. This issue will not be seen on Windows with the recommended JRE (1.7u45 & 51) for 12.1.6.

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, 6.4.x, 7.0x, 7.1.x, and 7.2.x	SAN04B-R (2005-R04) SAN24B-4 Express (2498-B24, -24E) SAN40B-4 (2498-B40, -40E) SAN80B-4 (2498-B80) SAN24B-5 (2498-F24, 249824G, 2498-X24) SAN48B-5 (2498-F48) SAN96B-5 (2498-F96, -N96) SAN06B-R (2498-R06) IBM Converged Switch B32 (3758-B32, -L32) VA-40FC SAN256B (2109-M48) SAN384B (2499-192) SAN768B (2499-384) SAN384B-2 (2499-416) SAN768B-2 (2499-816)	Brocade 7500E Brocade 300 Brocade 5100 Brocade 5300 Brocade 6505 Brocade 6510 Brocade 6520 Brocade 7800 Brocade 8000 VA-40FC Brocade 48000 Brocade DCX-4S Brocade DCX Brocade DCX 8510-4 Brocade DCX 8510-8

Installing IBM Network Advisor

Refer to the *IBM System Storage Network Advisor Installation and Migration 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; 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 12.1.6 > Network Advisor 12.1.6**

Windows:

- Launch the client from the desktop icon.
- Launch command prompt and go to the location "<Install location>/bin" and enter "**dcmclient**"

Linux:

- Launch the client 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.

1. 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:
2. If, when the Network Advisor server was installed, a Network Advisor web server port number was specified (instead of the default 443), you must specify the port number after the hostname or IP address. In the following examples, 8080 is the web server port number:

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

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

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

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

Note 1

Launching element manager applications within Network Advisor Client is done using Java Web Start technology. This requires that the local system's web browser is able to run Java web start applications. This setting may have been turned off in the wake of recent Java zero-day vulnerabilities.

To turn on Java content in the browser, follow the steps below:

1. Launch the "Java Control Panel"
(refer to http://java.com/en/download/help/win_controlpanel.xml to locate the Java Control Panel application on Windows)
2. In the Java Control Panel, click the **Security** tab.
3. Select the check box for **Enable Java content in the browser**. This will enable the Java plug-in in the browser.
4. 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.
5. Now launch Element Manager from the IBM Network Advisor client.

Note 2:

On a Windows server, if only Administrators have access to a drive, Windows will not allow Postgres to create some required directories. As result, migration from a previous version of Network Advisor to a newer supported version fails. Complete the following steps to resolve the issue:

1. Make sure that the previous version of Network Advisor is up and running.
2. Right click on the drive where the new version of Network Advisor will be installed (for example, :D)
3. Select the **Security** tab, and then click **Edit** and then click **Add**.
4. Add "Authenticated Users" and give full permission, click **OK**.
5. Now install the new version of Network Advisor and start the migration progress.

Important SAN Notes

1. Host based stand-alone SMI agents cannot manage products with Fabric OS v7.0 and above. It requires use of the integrated SMI Agent with IBM Network Advisor 12.1.0 and above.
2. Supported AG limits are the following: 64 bit OS - max of 200 AGs
3. 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). The user is therefore required to update to ESXi 5.0 update 1 or later to be able to manage the host in IBM Network Advisor through the host adapter discovery.
4. If you see the following error message "Signature could not be validated" during firmware download or technical support data collection using SCP/SFTP, then it could be due to a mismatch in the signature key used in the ssh handshake between the switch and SCP/SFTP server. Use the following CLI command work-around to address the issue:

- **For Fabric OS devices**

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

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


If this work-around does not work, go to Server > Options > Software Configuration > FTP/SFTP/SCP, and deselect the SCP/SFTP option.

5. The Encryption Smart Card Driver is only supported for 32 bit Linux. It is not supported on 64 bit Linux.
6. Firmware Download operation on Fabric OS switches fails via SCP/SFTP when trying to upgrade from FOS v6.3.2b to v6.4.2b4. The workaround is to use the FTP option in Network Advisor to perform the firmware download operation.
7. Firmware Download operation on Fabric OS switches fails when trying to upgrade from FOS v6.4.2a to v7.0.2c. The workaround is to use CLI for this operation.
8. Trying to move a large number of ports (240+) between logical switches with 'Reset to Default' option selected, results in operation time-out.
9. During installation, if Network Advisor database initialization fails on Windows Operating System, the user needs to verify access to the drive on which the installation is performed. If the user "Administrator" alone has access to the drive, then required permissions should also be provided to "Authenticated Users" and then continue with the installation.
10. There will be a delay in populating the GbE port details in the Network Advisor client if the server IP is not registered on the switch to receive SNMP traps from the switch.
11. On IBM SAN24B-5, firmware upgrade from v7.0 to higher versions is blocked. The work around is to use CLI for the firmware download operation.
12. After upgrading to IBM Network Advisor 12.x from 11.x, SSL-based product communication will fail if the devices have 'weak' authentication certificates. The user will 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 v1.7. Please refer to the 'Secure Sockets Layer protocol' section of *FOS Administrator's Guide* for details on updating certificates.
13. Receive Throughput measure is not updated in Flow Vision dialog.
14. D-port test fails for F-ports with the result as "null" in the report.
15. In Real Time performance graphs, percentage utilization will fluctuate between 0 – 100 if a single port is selected. The workaround is to select more than one port while generating Real Time performance graphs.
16. IBM Network Advisor uses SNMPv3 by default to discover SAN products. If required, user can select the 'Manual' option in Discovery dialog and choose SNMPv1 for discovery.
17. There could be false alarms indicating that the Zone database and the active zone configurations are modified if any of the names of the zoning elements (zones, zone configurations or aliases) contain underscores ('_') in the Zone database that is saved or activated on to a fabric by IBM Network Advisor.
18. A delay of 5 to 7 minutes is seen 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. This problem can be avoided on such systems by modifying the below Java properties:

On Windows: C:\Users\

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'.

If these parameters are not present, add them and save the file.
Then re-launch Web tools.
deployment.security.validation.ocsp = false
deployment.security.validation.crl = false

19. If IBM Network Advisor is installed on Linux Operating System, the Fabric OS Element Manager and HCM cannot be launched if the client is launched using dcmclient script available in Network Advisor installation folder. The Launch in Context (LIC) dialogs from SMIA configuration tool (launched from Server Management Console) also cannot be launched (e.g. Discovery Dialog, Options Dialog etc.). To use the above features on Linux machines, user can launch Network Advisor client from a browser (after installing JRE 7 update 60), pointing to the Network Advisor server installed on that machine.

Workaround

Complete the following two steps to work around this issue.

Step 1) Add following line in the <<User Home>/.java/deployment/deployment.properties file.

deployment.expiration.check.enabled=false

For example, if the user is root then the absolute path of this file would be as follows:

/root/.java/deployment/deployment.properties.

Step 2) Launch the java control panel using then command below and then click the OK button.

<Network Advisor Home>\jre\bin\jcontrol

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 by opening the **Discovery** dialog, and adding the IP address of the chassis using the add dialog.

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.

SSL connections using certificates with MD5 signatures

To avoid potential security vulnerabilities, IBM Network Advisor versions 12.0.x 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 may 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 will take 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, i.e., 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.

Note 2:

Reset ports to default operation will not clear FCIP configurations in the following scenarios:

- In IBM SAN18B-R switches and FR4-18i blades, VE ports cannot be reset to default unless their corresponding GE ports are cleared of their FCIP configurations.
- In IBM SAN06B-R switches and FX8-24 blades, GE ports cannot be reset to default unless their corresponding VE ports are cleared of their FCIP configurations.

Common issues for SAN

Miscellaneous important notes that apply to SAN installations

1. 64 bit OS is required to run Network Advisor Professional-Plus and Enterprise Editions.
2. Privileges related to SAN and IP features are prefixed with ‘SAN –’and ‘IP –’strings. After migration from an older version, new privilege names will be displayed in the Role Management dialog with these prefixes.
3. IBM Network Advisor server startup and restart can take up to 10+ minutes to complete.
4. When configuring IBM Network Advisor in “SSL enable mode” with 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.
5. To avoid excessive telnet/ssh login messages in the IBM Network Advisor master log and event report, and the device CLI console, disable lazy polling by deselecting the “Enable lazy polling” checkbox in **IP Discovery Global Settings > Preferences Dialog**.
6. Starting with 12.0, the number of client connections supported has increased to 25. Refer to the Installation Guide for details. In addition to those details, the following database memory setting is required:

- The PostgreSQL's parameter "shared_buffers" memory allocation should be increased to 1024MB. To change this setting, edit the <installation_directory>\data\databases\postgresql.conf file.
Change the line: shared_buffers = 256MB
To: shared_buffers = 1024MB
 - The server needs to be restarted.
7. In Linux 64 bit machines, connecting to the database through Open Office using ODBC will not work. The solution is to connect from Windows ODBC Client to the 64 bit Linux machine where IBM Network Advisor is running to view the Database tables.
 8. If you are using the ODBC connection from a remote host to the database, after migrating to 12.0.x, you will no longer be able to connect from the remote host. If you want to connect from the remote host, refer to the "Configuring remote client access to the database" section in the Installation and Migration guide.
 9. During installation on a Linux server, if user sets the password for Network Advisor database starting with a '\$', installation of the application will fail.
 10. When attempting to install Network Advisor on a Linux Server, if the message 'Insert New Media' is displayed, the below command needs to be executed from a terminal:
ulimit -n 2000

Technical Support Save files collected from FOS products cannot be unzipped/opened if the FOS product has a lengthy name that results in a file path which is greater than the zipping capability of the Operating System housing the Network Advisor server. For example, Windows 7 supports zipping/unzipping of files only when the full file path is less than or equal to 256 characters.

Patch installer troubleshooting

Patch installer may not launch if UAC is enabled on a Windows 7/8/2008/2008 R2/2012 editions. You must first disable the UAC using the procedure provided in the **Troubleshooting** section of the *User Manual*, and then launch the patch installer.

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.

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 the IBM Network Advisor client to get disconnected from the server. Workaround is to restart the client.

Performance Statistics Counters - Calculation Formulae

For calculating the statistics for FC, GE, FCIP and TE port we use SNMP to query the respective OIDs, mentioned below in the table.

For calculating the HBA and CNA statistics, we use the APIs provided by HCM. And for EE monitors we use HTTP to get the TX, RX and CRC error values.

Polling interval for historical graph is 5 min and for real-time, it changes based on the granularity value selected in the Real Time graph dialog.

Counter Name	Type	Protocol used	Source value	Formula
TX		SNMP	.1.3.6.1.3.94.4.5.1.6	$TX = (\text{Delta value}^1 / (2000 * 1000)) / (\text{Polling interval}^2)$
RX	FC	SNMP	.1.3.6.1.3.94.4.5.1.7	$RX = (\text{Delta value}^1 / (1000 * 1000)) / (\text{Polling interval}^2)$
TX	GE	SNMP	.1.3.6.1.2.1.31.1.1.1.10	$TX = (\text{Delta value}^1 / (1000 * 1000)) / (\text{Polling interval}^2)$
RX	GE	SNMP	.1.3.6.1.2.1.31.1.1.1.6	$RX = (\text{Delta value}^1 / (1000 * 1000)) / (\text{Polling interval}^2)$
TX	FCIP	SNMP	.1.3.6.1.2.1.31.1.1.1.10	$TX = (\text{Delta value}^1 / (1000 * 1000)) / (\text{Polling interval}^2)$
RX	FCIP	SNMP	.1.3.6.1.2.1.31.1.1.1.6	$RX = (\text{Delta value}^1 / (1000 * 1000)) / (\text{Polling interval}^2)$
Uncompressed Tx/Rx MB/sec	FCIP	SNMP	.1.3.6.1.4.1.1588.4.1.1.6	$(\text{Delta value}^1 / (1000 * 1000)) / (\text{Polling interval}^2)$
TX	EE Monitors	HTTP	PortRX (variable from the return html file)	$TX = (\text{Delta value}^1 / (1000 * 1000)) / (\text{Polling interval}^2)$
RX	EE Monitors	HTTP	PortTX (variable from the return html file)	$RX = (\text{Delta value}^1 / (1000 * 1000)) / (\text{Polling interval}^2)$
TX	HBA, CNA	HCM API	NA	$TX = (\text{Delta value}^1 / (1000 * 1000)) / (\text{Polling interval}^2)$
RX	HBA, CNA	HCM API	NA	$RX = (\text{Delta value}^1 / (1000 * 1000)) / (\text{Polling interval}^2)$
TX	TE	SNMP	.1.3.6.1.2.1.31.1.1.1.6	$TX = (\text{Delta value}^1 / (1000 * 1000)) / (\text{Polling interval}^2)$
RX	TE	SNMP	.1.3.6.1.2.1.31.1.1.1.10	$RX = (\text{Delta value}^1 / (1000 * 1000)) / (\text{Polling interval}^2)$
TX% / RX%	FC, GE, FCIP, HBA, CNA	NA	NA	$TX\% \text{ or } RX\% = ((TX \text{ or } RX) / ((105000000 * \text{port speed}) * (\text{Polling interval}^2))) * 100$ If Utilization is less than 1 then the value is it to 0.0
TX% / RX% (Pre 6.4.1 Edison release)	TE	NA	NA	$TX\% \text{ or } RX\% = ((TX \text{ or } RX) / ((105000000 * 10) * (\text{Polling interval}^2))) * 100$ If Utilization is less than 1 then the value is it to 0.0

Cumulative 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 value ¹ / (1000 * 1000)
Other Counters				Other counters = Delta value ¹
Current Compression Ratio	FCIP	NA	NA	(ifHCInOctets + ifHCOctets) / fcipExtendedLinkCompressedBytes

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

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
C3 Discard Rx Timeout	FC	SNMP	.1.3.6.1.4.1.1588.2.1.1.1.27.1.25
C3 Discard Unreachable	FC	SNMP	.1.3.6.1.4.1.1588.2.1.1.1.27.1.26
C3 Discard Tx Timeot	FC	SNMP	.1.3.6.1.4.1.1588.2.1.1.1.27.1.27
C3 Discard Others	FC	SNMP	.1.3.6.1.4.1.1588.2.1.1.1.27.1.28
Encode Error Out	FC	SNMP	.1.3.6.1.4.1.1588.2.1.1.1.27.1.29
Temperature	FC	SNMP	.1.3.6.1.4.1.1588.2.1.1.1.28.1.1.1
Voltage	FC	SNMP	.1.3.6.1.4.1.1588.2.1.1.1.28.1.1.2
Current	FC	SNMP	.1.3.6.1.4.1.1588.2.1.1.1.28.1.1.3
Rx Power	FC	SNMP	.1.3.6.1.4.1.1588.2.1.1.1.28.1.1.4
Tx Power	FC	SNMP	.1.3.6.1.4.1.1588.2.1.1.1.28.1.1.5
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)
Invalid ordered set	FC	SNMP	1.3.6.1.3.94.4.5.1.45
BB credit zero	FC	SNMP	1.3.6.1.3.94.4.5.1.8
Truncated frames	FC	SNMP	1.3.6.1.3.94.4.5.1.47
FEC Corrected Blocks	FC	SNMP	1.3.6.1.4.1.1588.2.1.1.1.27.1.31
FEC Uncorrected Blocks	FC	SNMP	1.3.6.1.4.1.1588.2.1.1.1.27.1.32

SMI Agent

1. For IBM Network Advisor that has more than 30K instances (2 MB zones), the CIMOM takes more memory to generate CIM instances.

If the user performs Enumerate Instances or Enumerate Instances Names and total number of size is more than 2 MB for all managed fabrics, then CIM_ERROR_FAILED will thrown as the "Total Zone DB size is more than 2 MB."

For such configurations, the user needs to use Association calls.

Note: If the total zone DB is more than 1 MB or more than 10000 instances then the user should change the max jvm heap size to 2048MB to fetch the data without failure in 64 bit machine

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.
4. Brocade_AgentProduct class does not return the correct SMI release version details; Brocade_Agent class need can be used for getting the correct SMI version.

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 a 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 the **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 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 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 IBM 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.

FC port type value for imported HBA's

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

Documentation updates

The most recent IBM Network Advisor 12.1.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 12.1.6

This section lists the defects closed with a code change in IBM Network Advisor 12.1.6 as of May 20, 2014.

Defect ID: DEFECT000477274	
Technical Severity: High	Probability: Medium
Product: Network Advisor	Technology: Partner Integration
Reported In Release: Network Advisor 12.1.2	Technology Area: SMI Agent
Symptom: For Brocade_Switch profile, CTP 1.4 execution fails.	
Condition:	
<ol style="list-style-type: none"> 1. The class CIM_ElementStatisticalData expects only one instance in the output whereas it is getting two instances – one for brocade_switchfcportstats and one for brocade_Switchfcporthistoricalstatistics. 2. In the class Brocade_SwitchFCPortHistoricalStatistics, PacketsTransmitted and PrimitiveSeqProtocolErrCount, PacketsReceived - these are the mandatory properties which are currently not implemented in Network Advisor. 	
As a result, CTP 1.4 execution fails for Brocade_Switch profile.	

Defect ID: DEFECT000480568	
Technical Severity: High	Probability: High
Product: Network Advisor	Technology: Application Management
Reported In Release: Network Advisor 12.0.4	Technology Area: Installation & Migration
Symptom: Server does not start when doing silent installation as the console waits for user input and does not exit the process to complete installation.	
Condition:	
Occurs only with silent installation	

Defect ID: DEFECT000485113	
Technical Severity: High	Probability: High
Product: Network Advisor	Technology: Partner Integration
Reported In Release: Network Advisor 12.2.0	Technology Area: SMI Agent
Symptom: Incorrect number of instances are returned for a Meta SAN for the class Brocade_SANInFabric.	
Condition:	
Issue is seen for the class Brocade_SANInFabric.	

Defect ID: DEFECT000491552	
Technical Severity: Medium	Probability: Medium
Product: Network Advisor	Technology: Partner Integration
Reported In Release: Network Advisor 12.0.3	Technology Area: SMI Agent
Symptom: User cannot view all the instances of NPIV CIM_ActiveConnection.	
Condition:	
This issue occurs with NPIV connections.	

Defect ID: DEFECT000497610	
Technical Severity: Medium	Probability: Medium
Product: Network Advisor	Technology: Partner Integration
Reported In Release: Network Advisor 12.1.4	Technology Area: SMI Agent
Symptom: With Network advisor 12.1.4, CPU usage of the application continues to spike when CIMOM is used.	
Condition: Occurs only when CIMOM is used.	

Defect ID: DEFECT000497885	
Technical Severity: High	
Product: Network Advisor	Technology: Partner Integration
Reported In Release: Network Advisor 12.0.2	Technology Area: SMI Agent
Symptom: On Network Advisor, incorrect information is returned by the class Brocade_SwitchInFabric for Access Gateway switches, incorrectly causing Access Gateways to appear to be connected to multiple fabrics.	
Condition: Occurs for Access Gateways when using the class Brocade_SwitchInFabric.	

Defect ID: DEFECT000500674	
Technical Severity: High	
Product: Network Advisor	Technology: Partner Integration
Reported In Release: Network Advisor 12.1.4	Technology Area: SMI Agent
Symptom: User is unable to delete LSAN zones using the SMI Agent.	
Condition: Occurs only when using SMI Agent to delete LSAN zones.	

Defect ID: DEFECT000507408	
Technical Severity: Medium	Probability: Medium
Product: Network Advisor	Technology: Application Management
Reported In Release: Network Advisor 12.1.6	Technology Area: Server Properties
Symptom: Network Advisor is prone to heartbleed vulnerability if the customer enables SSL for postgresql database.	
Condition: This issue occurs when Network Advisor's postgresql configuration is modified to use SSL.	

Defect ID: DEFECT000490449	Technical Severity: High
Summary: SNMP traps are not received after Network Advisor server is restarted.	
Symptom: Master log does not display SNMP traps.	
Risk of Fix: Medium	Probability: High
Feature: UNDETERMINED	Function: UNDER REVIEW
Reported In Release: Network Advisor 12.1.1	Service Request ID: 1275040

Defect ID: DEFECT000490644	Technical Severity: High
Summary: Zoning Window displays incorrect FC Addresses for ports.	
Symptom: User sees incorrect FC addresses for ports in the zoning window.	
Risk of Fix: Low	Probability: High
Feature: ZONING	Function: USABILITY
Reported In Release: Network Advisor 12.1.4	

Defect ID: DEFECT000491804	Technical Severity: High
Summary: WWN for Access Gateway (AG) is incorrectly computed causing device discovery to fail.	
Symptom: User is not able to discover the Fabric to which the AG with incorrect WWN is connected.	
Risk of Fix: Medium	Probability: Medium
Feature: DISCOVERY	Function: SAN Switch Discovery
Reported In Release: Network Advisor 12.1.4	Service Request ID: 1281454