IBM System Storage®

IBM Network Advisor v12.3.4 Release Notes

CONTENTS

Release overview

IBM Network Advisor 12.3.4 is a software maintenance release based on IBM Network Advisor 12.3.3. All hardware platforms and features supported in 12.3.3 are also supported in 12.3.4. These versions include supporting key FC SAN features including support for new 16 Gbps hardware and Fabric OS, increased SAN scalability, a new Web Client and REST API support for accessing Fabric Vision data. Additionally, this release incorporates dashboard enhancements supporting timeline and point-in-time-playback functionality, configuration file and policy manager enhancements. IBM Network Advisor provides support for JBoss Foundation upgrade to v7.2 and around 125 RFEs.

IBM Network Advisor is a software management platform for SAN networks. It provides network administrators the ability to quickly access network topology, health and performance data required to troubleshoot and remediate network issues. IBM Network Advisor is licensed and deployed to manage SAN only networks.

The fixes included in this release are listed in the defect tables at the end of this document.

Software feature overview

SAN Management feature enhancements

IBM Network Advisor 12.3.4 supports the following SAN capabilities and enhancements:

- Platform support
  - FOS 7.3
  - FC16-64 blade for 2499-416 and 2499-816 fabric backbones
  - SAN42B-R (2498-R42)
- Browser based client
  - Dashboard
  - Inventory
  - Reporting
- Dashboard enhancements
  - Timeline and playback support
  - Share, import/export dashboards
- Change Manager
  - Drift detection and audit trail
  - Event based configuration backup collection
  - Device tree support
- Reporting
  - Enhanced SAN reports
  - Scheduling and export capabilities
- Fabric Vision enhancements
  - Support for FOS Fabric Vision enhancements
  - Configure Flow monitor on MAPS threshold violations
  - Auto subflow creation from real time graphs
  - Usability enhancements
- Fault management enhancements
  - Event action support from master log
  - Dynamic content configuration for email event action
  - MIB picker enhancement
- Performance Manager
  - E–port trunks management in real time and historical graphs
  - Clear counter at fabric level
- Architecture enhancements
- REST API

- Customer / OEM RFEs
  - Installer and migration enhancements
  - Auto host enclosure
  - VF configuration backup/restore
  - HTTPS then HTTP product communication mode
  - Trunk level decommission/recommission support for E-port trunks
  - Port decommission: CIMOM recovery support
  - Trial license validity extended to 120 days
- Aruba device management
- Postgres upgrade from 9.2.8.4 to 9.2.9
- Qlogic adapters support
  - Discovery and topology
  - Real time and historical performance monitoring
- MAPS enhancements
  - Test email support
  - Rule assignation to multiple groups
  - Enhanced auto generated rule name option
- Firmware managements enhancements
  - HCL support for SAN42B-R
- SAN historical performance statistics collection for SMIA only flavor of Network Advisor
- PM enhancements for calculating of FC port utilization
- In Flow Vison enhancements
  - Flow Vision templates to support forward and reverse directions when creating flows
- OUI management migration support
- New OS support - Red Hat Enterprise Linux 7.0 Adv
- JRE version update
- IP detailed device report enhancements to allow to filter ports based on the Name field
- Web Client PM Reports enhancements
- "Remote SFP metrics compare check" in Configuration Policy Manager
- Modified pre-defined condition in Configuration Policy Manager for checking SNMP community strings configuration on VCS
- Forward application events and pseudo events as syslog messages
  - Fault management support for forwarding application and pseudo events in syslog filter dialog
  - Application events and pseudo events will be forwarded as syslog message by using the RFC-5424 specification
  - Third party syslog receivers can be used to receive the application events and pseudo events forwarded as syslogs
- Open SSL upgrade from 1.0.0n to v1.0.0o
- SAN Reporting feature enhancements
- Poodle SSL Vulnerability fix in CIMOM (by upgrading server embedded JRE to version 1.7u76)

IBM Network Advisor Upgrades: IBM Network Advisor 12.0.X (12.0.0 – 12.0.4), 12.1.X (12.1.0 – 12.1.6), 12.2.0, and 12.3.3 running on the Linux and Windows operating systems can be upgraded to IBM Network Advisor 12.3.4.

Note 1: Enterprise and Professional Plus editions are not supported on 32-bit servers. To migrate Enterprise and Professional editions to a 64-bit server, refer to the "Pre-migration requirements when migrating from one server to another" section of the *IBM Network Advisor Installation and Migration Guide*.

Note 2: Direct migration from pre-12.0.x releases to 12.3.x is not supported. Refer to Table 13, "Pre-11.1.X release migration path matrix" in the *Installation and Migration Guide* for migration paths from DCFM and Network Advisor 12.3.2 or earlier releases.

Note 3: Refer to Table 15, "SMI Agent only migration paths," in the *Installation and Migration Guide* for SMI Agent only migration paths.

License dialog:

In the License dialog, the maximum limit will be shown as 15000 ports and 100 fabrics.

In the Professional Edition, port count is limited to 300 ports and 2 fabrics.

Migration Impact:

If you migrate from an Enterprise edition with a maximum of 9000 SAN ports and 36 fabrics, then after the migration the maximum limit will be 15000 SAN ports and 100 fabrics. These higher limits will be displayed in the License dialog.

New IBM model names for the IBM switches will not be shown automatically upon migration. To see these new names, edit the existing model name with that of the new name in the "oem-switch-model-mapping.properties" file located in the 'conf' folder of NA home location. Restart the server to make changes take effect.

Operating Systems supported

IBM Network Advisor 12.3.4 is supported on the following operating systems.

Note: The minimum required system physical memory for running IBM Network Advisor 12.3.3 (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	• Windows 8 and 8.1 Enterprise
Windows Server	• Windows Server 2008 R2 Data Center, Standard, and Enterprise • Windows Server 2012 and 2012 R2 Standard, Datacenter
Linux	• Red Hat Enterprise Linux Adv 6.3, 6.4, 6.5, 7.0 • Oracle Enterprise Linux 6.3, 6.4, 6.5 • SUSE Linux Enterprise Server 11. 3

Browser Support

Recommended browser versions for Web Client:

- Internet Explorer 11.0.9 update version RTM (Windows 8.1, Windows Server 2008 R2, Windows Server 2012 R2)
- Internet Explorer 10.0.9 update version RTM (Windows 2012)
- Firefox 24 and later (Windows/Linux)
- Chrome 33 and later (Windows)

Table 2 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] JRE 1.7u67 [Linux]
12.3.2	JRE 1.7u67
12.3.3	JRE 1.7u71, 1.7u72
12.3.4	JRE 1.7u76, 1.8_u31

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

Note 2: Due to java signing certificate expiration the Web Tools launch from IBM Network Advisor will not work with JRE 8 starting from 2/13/2015. An attempt to launch the Web Tools will be blocked and “Failed to validate certificate. The application will not be executed” message will be shown. To work around this issue please uninstall JRE 8, install JRE 7 updates 76 and set the security level to Medium.

For users with JRE 7 installation, an attempt to launch the Web Tools will be blocked and “Application Blocked by Security Settings” message will be shown. To work around this issue, JRE 7 users can simply reduce the security level from High to Medium and continue using JRE 7 update 76.

Note 3: Oracle enforces the latest JRE update to be used to web start the applications. The recommended versions for this release are listed in the JRE support table. Beyond the JRE expiration date, users will see the message “**Your Java version is out of date**” on an attempt to launch the web client.

You can either ignore the message “Your Java version is out of date” by selecting the “**later”** option and and then proceeding with the web start client, or you can install the latest released JRE patch and then web start the client. The following warning will be shown and can be ignored: “The client system has java version <Latest Installed JRE> but the recommended java version is <as noted in the JRE support table>. Do you want to continue?”

Table 3 Supported scalability limits by Network Advisor editions

	Enterprise edition			Professional Plus edition
	Small	**Medium**	**Large**	
SAN switch ports	2000	5000	15000	2560
SAN switches and Access Gateways	40	100	400	100
SAN devices	5000	15000	40000	5000
SAN Fabrics	25	50	100	100
Managed Hosts	20	100	400	100
vCenters	1	5	10	5
VMs (includes powered down VMs)	1000	5000	10000	5000

Note: Virtual Fabrics are counted as fabrics when calculating the managed count limits.

Note: Supported network latency between Network Advisor server and client or server and devices is 100ms.

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, 7.0.x, 7.1.x, 7.2.x, and 7.3.x	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) SAN04B-R (2005-R04) SAN06B-R (2498-R06) SAN 42B-R (2498-R42) 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 300 Brocade 5100 Brocade 5300 Brocade 6505 Brocade 6510 Brocade 6520 Brocade 7500E Brocade 7800 Brocade 7840 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. Run *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. Run *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 12.3.x > Network Advisor 12.3.x**

  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:

     https://NetworkAdvisorServerhost1.companyname.com/

     https://192.x.y.z/
  2. If, when the Network Advisor server was installed, a Network Advisor web server HTTPS 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:8080/

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

Note 1

The web started remote client is supported with JRE versions listed in the JRE support section in this document. The supported JRE version needs to be installed on the remote client system prior to establishing a server connection.

Note 2

The remote client can be launched in the following ways:

1. Enter the server IP in the browser. The page will redirect to web client login page. Select the “Desktop client” option. A page will display with two options to start the remote client:
   - Web start the client
   - Download the client bundle (64-bit OS only). (Supported for the same or cross-OS platforms.)
2. Enter the server IP in the browser. The page will redirect to web client login page. Login to the web client and then select “Desktop Client” menu option for remote client launch

Note 3

Launching the 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, due to 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 **Enable Java content in the browser** check box. This will enable the Java plug-in for 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.

Important SAN Notes

1. For the Professional edition of IBM Network Advisor, the support for SAN fabric count increased from 1 to 2 fabrics and support for switch port count is reduced from 1000 to 300 switch ports.
2. 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 fails if built-in SCP is used as preferred protocol. The workaround is to use the FTP option in IBM Network Advisor.
7. Trying to move a large number of ports (200+) between logical switches with the 'Reset to Default' option selected, results in operation time-out.
8. 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.
9. 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.
10. The FCIP links will not be shown in the topology for tunnels with degraded circuits.
11. IP Sec policy and pre-shared key cannot be viewed for SAN42B-R.
12. IP Ping, IP Route, and Trace route is not supported for SAN42B-R.
13. User cannot edit the tunnel configured without HA circuit for SAN42B-R.
14. IBM Network Advisor uses SNMPv3 by default to discover SAN products. If required, you can select the 'Manual' option in **Discovery** dialog and choose SNMPv1 for discovery, as in case of AG discovery which requires use of SNMPv1 by default.
15. 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\<logged in username>\AppData\LocalLow\Sun\Java\Deployment\deployment.properties

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

    In the 'deployment.properties' file, edit the parameters below and set them to 'false'.
    If these parameters are not present, add them and then save the file. Then re-launch Web Tools.
    deployment.security.validation.ocsp = false
    deployment.security.validation.crl = false

16. **Zone compare/Merge** dialog takes around 30 minutes to load zone DB with 13k nodes.
17. User will not able to configure circuit with MTU setting as Auto from IBM Network Advisor.
18. Real time graph will not display proper data for FCIP tunnels when the polling interval is 10 sec. User need to keep 20 sec polling interval in graph to see the correct data for SAN42B-R.
19. Emulex: HTTPS discovery for ESXi host will work only with certificate import
20. 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 the Network Advisor installation folder. The Launch in Context (LIC) dialogs from the 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, launch IBM Network Advisor client from a browser (after installing the supported JRE version), 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 the command below and then click **OK**.
<Network Advisor Home>\jre\bin\jcontrol

24. FCIP Tunnel creation fails with the message "Internal Error" if a circuit creation failed due to the configuration error and the user attempted to continue the configuration using the **Rollback** configuration dialog.
25. When IBM Network Advisor is installed on Windows 2012 or 2012 R2 platforms, the “Start Server” progress bar remains on the screen even after all services are started, which is indicated in the Server Management Console. The user can proceed with launching the Network Advisor client.
26. Fabrics will auto-collapse in the current view when the Switch Ports count (including the VE ports) exceeds 9000.
27. SAN Configuration Purge Backup is being enabled automatically when “Enable Scheduled Backup” is set and remains enabled after disabling the scheduled backup.
28. Session timeouts observed in Reports page of the Web Client after five minutes. Browser refresh is required to proceed.
29. User should not perform any write operations on FCIP tunnels which have circuits with different IDs.
30. When CIMOM server is bound to host name, SLP service fails to get registered. Workaround: To overcome this issue user can bind the CIMOM server to IP Address instead of host name.

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 add the IP address of the chassis using the **Add** dialog.

SSL connections using certificates with MD5 signatures

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 “Fabric Discovery failed because SSL certificate of the seed switch uses a weak algorithm. Install SSL Certificate with strong authentication algorithm on the switch and try again” for devices with weak certificates. Devices discovered prior to migration will not be manageable in IBM Network Advisor after migration. Java 1.7 used by IBM 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 Admin guide for details on updating certificates

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 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 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.
- Switch reset to default operation on IBM SAN42B-R switches may fail due to GE port sharing or if the associated VE port exists in another LS.

Additional important notes for SAN

1. 64 bit OS is required to run Network Advisor Professional-Plus and Enterprise Editions.
2. User role 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. 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**.
5. Starting with 12.0, the number of client connections supported has increased to 25. Refer to the *Installation and Migration 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 1024 MB. 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.

6. 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.
7. 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*.
8. Technical Support data collection for discovered Products fails through an external Linux FTP server on a Windows installation of Network Advisor. To successfully collect support save data for NOS and FOS devices, the following configuration needs to be done in the VSFTPD FTP server before triggering the support save by setting external VSFTPD FTP Linux server (other than NA FTP server):

   /etc/vsftpd.conf file and set "chroot_local_user=YES"
9. The client only application can be installed on a machine other than the server (without using a web browser) by creating a client bundle on the server, then copying and installing that client on another machine. Refer to the 'Client only installation' section of the *Installation and Migration Guide* for details.
10. Event Action from Master Log fails for Source Name as Local Host in master log.
11. "Server is not available" message will be displayed in the **login** dialog when user changes the default server port [24600] and tries to launch a remote client from client bundle. It is recommended to use the default server port.
12. Intermittently HTTP 500 error message is displayed when launching the Web Client. Server restart will fix the issue.
13. Error code 10003 reads "Common DCFM error". Instead it should read "10003: [..] Another transaction in progress'.
14. User needs to run the "sanperformancestatenable" script from NA home utilities folder to enable/disable performance statistics collection for SMIA only package installation. Following are the steps to execute the script.
    - Windows: Open cmd prompt and move to <BNA_HOME>\utilities and run sanperformancestatsenable.bat dbusername dbpassword enable|disable
    - Linux: Open terminal and move to <BNA_HOME>\utilities and run sanperformancestatsenable dbusername dbpassword enable|disable
15. User needs to use a different name (non-default) for the widget when attempting to add "Top Product Response Time" widget to avoid this error "Monitor could not be added. Duplicate monitor name".
16. Intermittently the Port Traffic/SFP/Error Time Series Report generation may fail when the port count is greater than 50 and the Time Scope is greater than 3 days.
17. REST API does not provide FCIP circuit measures for the GigE port.
18. Pre-defined condition for checking SNMP Community string configurations on the VCS would fail on the run of corresponding Policy Monitor.
19. "CLI through server" for FC/LC mode cluster and CLI Template based deployments for LC mode cluster will not function when product communication is set to "SSH Only".
20. IBM Network Advisor is now enforcing minimum disk space requirements during migration. When the disk space requirements are not met, IBM Network Advisor displays an error message prompting the user to use the script to delete performance data and retry migration.

21. The following step from the “Migration Data” section of the *Installation and Migration Guide* is no longer applicable and can be ignored during the migration: “To migrate historical performance data, select the SAN and IP check boxes, if necessary.”
22. SNMP Trap auto-registration does not happen for a discovered VCS which is configured with ‘Read Only’ community string alone. Registration can be done manually post discovery through **Product Trap Recipients** dialog.
23. When IBM Network Advisor is managing more than 1500 IP products, you may experience some performance degradations such as delays while launching some dialogs.
24. Due to Microsoft Windows operating system restriction which does not allow services logged in as Local System user to interact with the desktop, the GUI application cannot be launched using “Launch a Script” option of **Add Event Action**.

    Refer the following link for more information:
    http://msdn.microsoft.com/en-us/library/windows/desktop/ms683502%28v=vs.85%29.aspx
25. LDAP users have to provide usernames with case sensitivity, as defined in LDAP server, to successfully login into Network Advisor client.
26. During migration, if insufficient space is detected, then a warning message will be displayed with an option to rollback. If user chooses "No", then migration will be aborted. As a result, the source version services will remain uninstalled. Please refer to the Installation and Migration Guide for instructions to install the source version services manually.
27. The firewall ports listed in the Installation and Migration guide need to be open bidirectionally for all the bi-directional protocols.

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 Appendix G: **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. Work around 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 = (Delta value[1] / (1000 * 1000)) / (Polling interval[2])
RX	FC	SNMP	.1.3.6.1.3.94.4.5.1.7	RX = (Delta value[1] / (1000 * 1000)) / (Polling interval[2])
TX	GE	SNMP	.1.3.6.1.2.1.31.1.1.1.10	TX = (Delta value[1] / (1000 * 1000)) / (Polling interval[2])
RX	GE	SNMP	.1.3.6.1.2.1.31.1.1.1.6	RX = (Delta value[1] / (1000 * 1000)) / (Polling interval[2])
TX	FCIP	SNMP	.1.3.6.1.2.1.31.1.1.1.10	TX = (Delta value[1] / (1000 * 1000)) / (Polling interval[2])
RX	FCIP	SNMP	.1.3.6.1.2.1.31.1.1.1.6	RX = (Delta value[1] / (1000 * 1000)) / (Polling interval[2])
Uncompressed Tx/Rx MB/sec	FCIP	SNMP	.1.3.6.1.4.1.1588.4.1.1.6	(Delta value[1] / (1000 * 1000)) / (Polling interval[2])
TX	EE Monitors	HTTP	PortRX (variable from the return html file)	TX = (Delta value[1] / (1000 * 1000)) / (Polling interval[2])
RX	EE Monitors	HTTP	PortTX (variable from the return html file)	RX = (Delta value[1] / (1000 * 1000)) / (Polling interval[2])
TX	HBA, CNA	HCM API	NA	TX = (Delta value[1] / (1000 * 1000)) / (Polling interval[2])
RX	HBA, CNA	HCM API	NA	RX = (Delta value[1] / (1000 * 1000)) / (Polling interval[2])
TX	TE	SNMP	.1.3.6.1.2.1.31.1.1.1.10	TX = (Delta value[1] / (1000 * 1000)) / (Polling interval[2])
RX	TE	SNMP	.1.3.6.1.2.1.31.1.1.1.6	RX = (Delta value[1] / (1000 * 1000)) / (Polling interval[2])
TX% / RX%	FC	NA	TX = .1.3.6.1.3.94.4.5.1.6 RX = .1.3.6.1.3.94.4.5.1.7	TX% or RX% for FC = ((delta value1 of TX or RX) / ((Bytes transmitted * port speed)*(polling interval2)) * 100 where Bytes transmitted for 1G,2G,4G,8G and 6G port speed is 106250000 and Bytes transmitted for 10G port speed is 127500000. If utilization is less than 1, the value is 0.0.

TX% / RX%	GE	SNMP	TX = .1.3.6.1.2.1.31.1.1.1.10 RX =.1.3.6.1.2.1.31.1.1.1.6	TX% or RX% for FC = ((delta value1 of TX or RX) /((125000000* port speed)*(polling interval2))) * 100. If utilization is less than 1, the value is 0.0.
TX% / RX%	FCIP	SNMP	TX = .1.3.6.1.2.1.31.1.1.1.10 RX =.1.3.6.1.2.1.31.1.1.1.6	TX% or RX% for FCIP = ((delta value1 of TX or RX) /(maximum bytes transmitted))*polling interval2))) * 100, where maximum bytes transmitted = tunnel speed
TX% / RX% (Pre 6.4.1 Edison release)	TE	SNMP	TX = .1.3.6.1.2.1.31.1.1.1.10 RX =.1.3.6.1.2.1.31.1.1.1.6	TX% or RX% for TE = ((delta value1 of TX or RX) /((125000000* 10)*(polling interval2)))* 100. If utilization is less than 1, the value is 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 + ifHCOutOctets) / fcipExtendedLinkCompressedBytes

1) Delta value[1]: is the difference of value retrieved between the two consecutive polling cycles.
2) Polling interval[2] : duration between the two polling cycle in seconds

SMI Agent

1. For IBM Network Advisor that has more than 30K instances, the CIMOM takes more memory to generate CIM instances
2. If the user performs Enumerate Instances and the total size is more than 2 MB for all managed fabrics, it may result in out of memory issue. In this case, the user has to increase the CIMOM heap size to fetch zone database size of 2 MB.
   Note: For 1.6 MB of zone database (144600 zone members), with 9 GB of heap size the Brocade_zonemembershipsettingdata instances are retrieved.

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 IBM Network Advisor are not SNMP registered. As this would cause a delay in indication delivery, all the switches managed in IBM Network Advisor should be SNMP registered

CIMOM heap size

The CIMOM heap size has been increase for small, medium, and large SAN network sizes:

Old heap sizes:
small

platform.64.cimom.conf.set.MAX_HEAP_SIZE = 1024m

medium

platform.64.cimom.conf.set.MAX_HEAP_SIZE = 1536m

large

platform.64.cimom.conf.set.MAX_HEAP_SIZE = 2048m

Current heap sizes:

small

platform.64.cimom.conf.set.MAX_HEAP_SIZE = 1536m

medium

platform.64.cimom.conf.set.MAX_HEAP_SIZE = 2048m

large

platform.64.cimom.conf.set.MAX_HEAP_SIZE = 3072m

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*>\c*onf* 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 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 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 reconfigured by modifying this file.
- SLP register—`Management_Application\cimom\cfg\slp.reg`
  statically register an application that does not dynamically register with SLP using SLPAPIs by modifying this file. For more information about these files, read the comments contained in them, or 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 **Ente**r.
   - 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.

.

Documentation updates

The most recent IBM Network Advisor 12.3.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 **Product documentation** under the **Product support content** heading. Navigate to the desired publications in the displayed results.

IBM Network Advisor Installation and Migration Guide refers to 'Professional Plus Trial' license (Tables 1, 12, and 14). This license is no longer valid and reference to this license will be removed in a subsequent version of Network advisor documentation.

Defects

12.3.4 Open defects

Defect ID: DEFECT000548764	
Technical Severity: High	**Probability:** High
Product: Network Advisor	**Technology:** Application Management
Reported In Release: Network Advisor 12.3.4	**Technology Area:** Options Dialog
Symptom: Remote Client or Web Tools proxy fail to launch with “Unable to launch application” error after changing the “Redirect HTTP Requests to HTTPS” setting via Server > Options dialog.	
Condition: The issue is observed only when “Redirect HTTP Requests to HTTPS” checkbox is unselected in Server > Options > Server Port dialog. The issue persists after re-selecting the checkbox and restarting the services.	
Workaround: To avoid the issue use Network Advisor Configuration wizard, instead of Server > Options dialog, to check or uncheck “Redirect HTTP Requests to HTTPS” checkbox. However, if the **Server > Options** dialog was used, do the following: 1. To launch Remote Client use the remote client bundle. For this enter the IP address or host name of the Management application server in the browser in the Address bar. Then click the "Download client bundle" hyperlink,extract the downloaded client bundle zip file and launch client login dialog. 2. Launch Web Tools directly from the browser.	

Defect ID: DEFECT000548050	
Technical Severity: High	**Probability:** High
Product: Network Advisor	**Technology:** Other
Reported In Release: Network Advisor 12.3.4	**Technology Area:** Other
Symptom: SLP Service fails to start upon Network Advisor installation. An attempt to restart SLP service from SMC console fails as well.	
Condition: The issue is observed on Red Hat 7.0, OEL 6.4 and OEL 7.0 platforms.	

Defects closed with code change in IBM Network Advisor 12.3.4

Defect ID: DEFECT000531936	
Technical Severity: High	**Probability:** High
Product: Network Advisor	**Technology:** Security
Reported In Release: Network Advisor12.3.3	**Technology Area:** Security Vulnerability
Symptom: SSL (Poodle) vulnerability is partially addressed in NA 12.3.3. Except for SMI access to CIMOM over HTTPS, all other vulnerabilities have been addressed.	
Condition: Network Advisor servers’ SMI Agent using HTTPS is exposed to SSL (Poodle).	
Workaround: Deploy BNA server and SMI clients behind a firewall for HTTPS access. Also, make sure to block port 24605 in the firewall.	

Defect ID: DEFECT000547647	
Technical Severity: High	**Probability:** High
Product: Network Advisor	**Technology:** Security
Reported In Release: Network Advisor 12.3.3	**Technology Area:** Security Vulnerability
Symptom: Authentication failure errors observed in Network Advisor for VF switches after changing switch password from CLI.	
Condition: The issue occurs after changing VF switch(es) password from CLI. In this case Network Advisor makes continuous unsuccessful attempts to collect switch assets using old login information.	
Workaround: After changing switch password from CLI rediscover the fabric in Network Advisor to update switch login information.	

Defect ID: DEFECT000539284	
Technical Severity: High	**Probability:** High
Product: Network Advisor	**Technology:** Security
Reported In Release: Network Advisor12.3.3	**Technology Area:** Security Vulnerability
Symptom: Migration of Network Advisor failed and rolled back to the previous version.	
Condition: Issue observed if performance custom reports were run in pre-12.3.4 Network Advisor prior to migrating to 12.3.4.	
Workaround: Prior to performing Network Advisor migration, delete performance custom reports.	

Defect ID: DEFECT000542610	
Technical Severity: High	**Probability:** High
Product: Network Advisor	**Technology:** Security
Reported In Release: Network Advisor12.3.3	**Technology Area:** Security Vulnerability
Symptom: Deployment of switch username and password via Network Advisor failed and corresponding errors shown in switch console.	
Condition: Issue observed on FI/NI devices if deployment performed in migrated Network Advisor server.	