



IBM Storage Network®

IBM Network Advisor v14.2.2

Release Notes

Copyright © 2018 Brocade Communications Systems, Incorporated.

Copyright © IBM Corporation 2018. All rights reserved.

Brocade, the B-wing symbol, MyBrocade are trademarks of Brocade Communications Systems, Inc., in the United States and in other countries. Other brands, product names, or service names mentioned of Brocade Communications Systems, Inc, are listed at www.brocade.com/en/legal/brocade-Legal-intellectual-property/brocade-legal-trademarks.html. Other marks may belong to third parties.

Broadcom, the pulse logo, Connecting everything, and Brocade are among the trademarks of Broadcom in the United States, certain other countries and/or the EU.

Broadcom Proprietary. Copyright © 2017 Broadcom. All Rights Reserved.

The term "Broadcom" refers to Broadcom Limited and/or its subsidiaries. For more information, please visit www.broadcom.com.

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

IBM, the IBM logo, and 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: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade or IBM. Brocade and IBM reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact an IBM representative for information on feature and product availability.

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	5
Software feature overview	5
SAN Management feature enhancements	5
Operating Systems supported	8
Browser support	8
Device platform and firmware requirements	10
Supported Adapters.....	11
Installing IBM Network Advisor.....	12
To install IBM Network Advisor on Windows (Server).....	12
To install IBM Network Advisor on Linux (Server).....	12
To launch the IBM Network Advisor client	12
System Requirements	14
Memory, host, and disk space requirements	14
Minimum system requirements for server (plus 1 client) installation	14
Recommended system requirements for server (plus 1 client) installation.....	14
Operating system cache requirements	15
Client and server system requirements	16
Upgrade and Migration considerations.....	16
Migration Impact	17
Configuration Considerations.....	17
Limitations and Restrictions	18
Important Notes for managing Analytics Platform (Only for AMP users)	18
Upgrading the License	20
License Upgrade procedure in Network Advisor	21
Downgrading the license	21
Defects	22
Defects closed with code change in IBM Network Advisor 14.2.2	22
Known Issues.....	22
Important SAN Notes.....	22
Display of Logical Switches	24
SSL connections using certificates with MD5 signatures.....	25
Important Notes common for SAN and IP	25
Domestic and International Modem based Call Home is no longer supported for Call Home	28
Support Saves and server backup may take a long time with large databases	28
Installation on Network Mounted Drives is not supported.....	28
Client disconnects	28
Cross-flavor Migration.....	29
Migrating same version of NA (14.2.1) from OEM1 version to OEM2 version:.....	29
Migrating NA (pre-14.2.1) OEM1 version to NA 14.2.1 OEM2 version:.....	30
Virtual Connect Enterprise Manager (VCEM) Support	30
Performance Statistics Counters - Calculation Formulae	30
SMI Agent	32
Indications delivery depends on SAN Size and SNMP registration.....	33

CIMOM Heap Size	33
Logging for CIMOM	33
Service Location Protocol (SLP) support.....	34
Management SMI Agent SLP application support.....	34
SLP on UNIX systems	35
SLP on Windows systems	36

Release overview

IBM Network Advisor 14.2.2 is a software maintenance release based on IBM Network Advisor 14.2.1. This release addresses the Java signing certificate expiry issue. All hardware platforms and features supported in IBM Network Advisor 14.2.1 are supported in 14.2.2.

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 14.2.2 supports the following SAN capabilities and enhancements:

- Java signing certificates have been renewed.
- Defect fixes.

IBM Network Advisor 14.2.1 supports the following SAN capabilities and enhancements:

- Fabric OS Platform Support
 - Fabric OS 8.1.0x
- IOS Firmware Support
 - FI 8.0.60
 - ICX 7150
- Network OS Firmware support
 - NOS v7.2.0
- MAPS
 - Rule on Rule monitoring (requires Fabric OS v 8.1.0a or later)
 - Deprecation of Uninstall vTap Action feature
- REST API Enhancements
 - Port Persistent Enable/Persistent Disable operation support
- EMC Call Home – Send Test functionality
- Defect fixes provided

IBM Network Advisor 14.2.0 provided the following SAN capabilities and enhancements:

- Platform support
 - Fabric OS 8.1.0
 - SAN24B-6 switch
- VM Insight support
 - Identify and track VMs within a fabric
 - Provide VM visibility in Fabric Vision technology for monitoring and diagnostics

- Flow Monitoring
- Flow Vision enhancements
 - Top N Flows/Bottom N Flows – Dashboard widget - Entity ID, VM Name and Application name added to the Top N /Bottom N Flows widgets
 - Flow Vision IOS Measures support in Historical Graph and Dashboard
- MAPS Enhancements
 - VM Insight based flows
 - Alert Severity Support for MAPS Rule
 - Enhancement in MAPS Policy Creation
 - New default Rules to Monitor Rx, TX & UTIL Measures
 - New default Rules to Monitor ERR_PORTS measures
 - Fabric Performance Impact (FPI) Monitoring Feature Enhancements
 - MAPS Rule Name Limitations
 - Monitor Front end Encryption port
 - Support for uninstalling vTAPs when threshold of 250K IOPS is exceeded
 - User defined policies and rules limits
 - Quiet time support for SNMP
 - Restriction of Orphan rules creation
- Web UI Enhancements
 - AMP Enhancements
- CLI Reports
 - Restriction of Orphan rules creation
- Zoning
 - Alias Support in Peer Zoning
 - Enhanced Zone Name Support
 - Zone DB size restriction based on per chassis limit
 - Alias/Zone creation by Port WWN instead of Node WWN
- Virtual Fabric
 - Offline LISL state at Logical Switch creation
 - FICON LS support
 - 16 LS support for Gen 6 chassis
- FCIP
 - 10 circuits/tunnel support
 - Circuit measures in performance graphs and dashboard
 - WAN Vision Dashboard
- COMPASS Enhancements
 - Track Switch User Accounts

- Track Switch User Account Credential
- Web Client
 - Unified Inventory
 - PM support for NOS and IP
- Campus Enhancements
 - Campus Dashboard
 - New Syslog Formatting
 - sFlow support for Campus Fabric
 - Stack ISSU Support
- REST API
 - Port enable/disable, Port name settings
 - Peer zoning and zone alias support (Read-only)
- TRILL trunk alerting for trunk members
- Infrastructure upgrade
- JRE upgraded to 1.8.0u112
 - PostgreSQL updated to v9.5.4
- Analytics Monitoring Platform support
 - ampos2.0.0a
- Monitor DB data migration from 14.1.x to 14.2.0
- Support for JRE 1.8.0u121

Deprecated and retired features

- Bottleneck detection

For switches running FOS v8.0.0 and above Bottleneck configuration through the legacy Bottleneck Detection dialog is not allowed. For these switches Bottleneck conditions/thresholds configuration as well as bottleneck widgets and ports' bottleneck status will be supported through MAPS FPI. Bottleneck configuration and detection dialogs will still be supported for switches running FOS version prior to v8.0.0.

- For switches running FOS v8.1.0a and above the Uninstall vTap action will not be available in MAPS Policy Actions dialog starting from Network Advisor v14.2.1.
- Starting with FOS v7.4.2 release the following switches and blades are no longer supported:
 - Encryption Switch
 - FS8-18 blade

Therefore, in the Firmware Download dialog the Network Advisor does not list FOS versions v7.4.2 and above for the Encryption Switch. And for the director switch with FS8-18 blade the Network Advisor shows the error: "FS8-18 blade is not supported by the targeted firmware. Please remove the blade before upgrading."

Migration Impact:

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 14.2.x is supported on the following operating systems.

- Windows Server 2008 R2 SP1 Datacenter, Standard and Enterprise
- Windows Server 2012 R2 Standard, Datacenter
- Windows 7 Enterprise (Client only)
- Windows 8.1 Enterprise (Client only)
- MAC OS 10.12 (Sierra) (Fabric Insight Portal only)
- Windows 10 Enterprise
- Red Hat Enterprise Linux 6.8
- Red Hat Enterprise Linux 7.1
- Red Hat Enterprise Linux 7.2
- Red Hat Enterprise Linux 7.3
- SUSE Linux Enterprise Server 11.3
- SUSE Linux Enterprise Server 12.0
- Oracle Enterprise Linux 7.1
- Oracle Enterprise Linux 7.2
- Oracle Enterprise Linux 7.3

Browser support

Recommended browser versions for Web client:

- Internet Explorer 11 and later (Windows only, except Windows 8 and Windows 2012)
- Edge 13 (Windows 10 only)
- Firefox 41 and later (Windows/Linux)
- Chrome 46 and later (Windows)

JRE support

IBM Network Advisor version	JRE version supported
14.2.2	JRE 1.8u152

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

Note 2: (Applicable only to Web Tools from FOS releases done before 2/13/2015.) Due to java signing certificate expiration, Web Tools launched from IBM Network Advisor will not work with JRE. An attempt to launch the Web Tools will be blocked and “Failed to validate certificate. The application will not be executed” message will display. To work around this issue, uninstall JRE 8, install JRE 7 updates 79/80 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 display. To work around this issue, JRE 7 users can simply reduce the security level from High to Medium and continue using JRE 7 update 79/80.

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 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 display 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?”

Note 4: JRE 1.7.0 update 51 and later support begins with the following Fabric OS versions:

- Fabric OS v6.4.3f
 - Fabric OS v7.0.2e
 - Fabric OS v7.1.1c
 - Fabric OS v7.1.2
 - Fabric OS v7.2.1
 - Fabric OS v7.3.0
 - Fabric OS v7.4.0
 - Fabric OS v8.0.0
 - Fabric OS v8.0.1
 - Fabric OS v8.1.0x
 - Fabric OS v8.1.1
- a. Apply the following workaround when launching Web Tools using a browser or Network Advisor Remote client for all Fabric OS versions earlier than the ones listed above:
- On Windows:
Go to C:\Program Files\Java\jre7\lib\security
 - On Linux:
Go to <jre install directory>/lib/security
 - Edit java.security file and change the value to 256 from 1024
forjdk.certpath.disabledAlgorithms=MD2, RSA keySize< 1024
- b. Apply the following workaround on the Network Advisor server when launching Element Manager from the Network Advisor client for all Fabric OS versions earlier than the ones listed above:
- On Windows:
Go to <Network Advisor install directory>\jre64\lib\security

- On Linux:
Go to <jre install directory>/lib/security
- Edit java.security file and change the value to 256 from 1024
forjdk.certpath.disabledAlgorithms=MD2, RSA keySize< 1024

Device platform and firmware requirements

The following table lists the versions of 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 v8.0.1x, v8.0.2x, v8.1.0x, v8.1.1	SAN256B-6 SAN512B-6 SAN24B-6 SAN64B-6 SAN128B-6	Brocade X6-4 Director Brocade X6-8 Director Brocade G610 Brocade G620 Brocade G630
FOS v8.0.0	SAN64B-6 SAN128B-6	Brocade G620 Brocade G630
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, 7.3.x, and 7.4.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) SAN06B-R (2498-R06) SAN 42B-R (2498-R42) IBM Converged Switch B32 (3758-B32, -L32) VA-40FC 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 7800 Brocade 7840 Brocade 8000 VA-40FC Brocade DCX-4S Brocade DCX Brocade DCX 8510-4 Brocade DCX 8510-8

Supported Adapters

For Windows, the Emulex and QLogic adapter discovery is based on Windows Management Instrumentation (WMI).

For ESXi host, the Emulex adapter discovery is based on CIM provider.

For Brocade adapters, HCM 3.2.4 version is integrated with NA.

	Adapter Types	Driver/Firmware versions
Brocade	Brocade 415,425,815,825	<u>Driver/Firmware Versions:</u> 1.1, 2.0, 2.1, 2.2, 3.0, 3.1, 3.2, 3.2.4 <u>CIM Provider version:</u> cpba3.2.3
	Brocade 804 ¹	
	Brocade 1010,1020,1007 ²	
	Brocade 1741 ³	
	Brocade 1860 ⁴	
	Brocade 1867 ⁵	
	Brocade 1869 ⁶	
Emulex	LPe12002-M8 8Gb 2-port PCIe Fibre Channel Adapter	<u>Driver Versions:</u> ESXi: 10.0.727.44 Windows: 10.0.720.0 <u>Firmware Versions:</u> ESXi: 1.1.43.3 Windows: 1.1.43.3 <u>CIM Provider Version:</u> ESXi 5.1 and 5.5: 10.0.774.0 <u>Boot Code and firmware version:</u> 11.0.2.243.19 (LPE32002 only)
	LPe16000 16Gb PCIe Fibre Channel Adapter	
	LPe32002-M2 32Gb 2-port PCIe Fibre Channel Adapter	
QLogic	QLE2562-CK 8Gb, Dual Port, FC HBA, x4 PCIe	<u>Boot Code Version:</u> 01.01.38 (multi-bot image with FCode for QLE269x/27xx Series Adapters) <u>Driver Versions:</u> Windows: 9.1.13.20 <u>Firmware Versions:</u> Windows: 8.00.00 <u>CIM Provider Version:</u> ESX-5.5.0-qlogic-cna-provider-1.5.7
	QLE2672-CK - Host bus adapter - PCI Express 3.0 x4 / PCI Express 2.0 x8 low profile - 16Gb Fibre Channel x 2	
	Corp ISP2532-based 8Gb Fibre Channel to PCI Express HBA	
	QLE2742 PCIe 3.0 x8 (dual-port) 32G FC HBA QLE2740 Single-port PCIe 3.0 x8 to 32Gb Fibre Channel Adapter – SFP+	
	QLE2764 Quad-port PCIe 3.0 x8 to 32Gb Fibre Channel Adapter	

Footnotes:

¹ Requires v2.1.1.0 or later

² Requires v2.0 or later

³ Requires v2.2 or later

⁴ Requires v3.0 or later

⁵ Requires v3.0.3 or later

⁶ Requires v3.2.3 or later

Supported vCenter Versions

Virtual Machine Management: vCenter and ESXi Supported Versions	
ESXi	5.5, 6.0
VCenter	5.5, 6.0

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 14.2.x > Network Advisor 14.2.x**
- 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"**

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

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:

Remote Host:

To launch the IBM Network Advisor client from a remote host, do the following:

1. 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/>

The web client login page displays.

- Click **Desktop Client**.
The Network Address web start page displays.
- Choose one of the following options:
 - o Click **Web Start the Client** link.
The Log In dialog box displays.
- Click the **Download client bundle** link.

Web browser:

To launch the Network Advisor Client from a web browser, do the following:

1. Open a browser window and enter the Network Advisor IP address in the Address bar.

For example:

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

3. Click **Desktop Client** to launch the Java client from any page of the web client. The Log In dialog box displays.

Note 3: Launching element manager applications within Network Advisor Client is done using Java Web Start technology. This requires the local system's web browser to be 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 **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.

System Requirements

Memory, host, and disk space requirements

Memory requirements are only applicable when there are no other applications running on the Network

Advisor server. Paging space should be equal to or exceed the physical memory size.

Note: When Network Advisor is installed on VM the system resources have to be dedicated to the VM.

The following table summarizes the memory, host, and disk requirements for a remote client.

Resources	Small	Medium	Large
Installed Memory	4 GB	4 GB	4 GB
Processor Core Count (including physical and logical cores)	2 (1 physical and 1 virtual)	4 (2 physical and 2 virtual)	4 (2 physical and 2 virtual)
Disk Space	1 GB	1 GB	1 GB

Minimum system requirements for server (plus 1 client) installation

The following table summarizes the memory system requirements for server (plus 1 client) installation.

Resources	Professional Edition	Professional Plus or Enterprise Edition
Installed Memory	6 GB	6 GB
Processor Core Count (including physical and logical cores)	2	2
Disk Space	10 GB	20 GB

Recommended system requirements for server (plus 1 client) installation

The following table summarizes the recommended system requirements for server (plus 1 client) installation.

Resources	Small	Medium	Large
Installed Memory	16 GB	16 GB	16 GB

Processor Core Count (including physical and logical cores)	2 (1 physical and 1 virtual)	4 (2 physical and 2 virtual)	8 (4 physical and 4 virtual)
Disk Space	20 GB	80 GB	100 GB

NOTES:

1. To efficiently manage more than 9000 SAN ports or 200 IP devices, the recommended memory allocation is 16 GB. The minimum memory allocation is 2 GB for the client and 6 GB for the server.
2. If you use sFlow, it is recommended that you add an additional 100 GB of disk space.
3. It is recommended that you add an additional 40 GB of disk space for the default temporary directory.
4. If you enable periodic supportSave or configure the Network Advisor server as the Upload Failure Data Capture location for monitored switches, you must add additional disk space. Each switch supportSave file is approximately 5MB and each Upload Failure Data Capture file is approximately 500 KB. To determine the disk space requirements, multiply the frequency of scheduled supportSave files by 5 MB and the expected Upload Failure Data Capture files by 500 KB before the planned periodic purge activity.

Recommended system requirements for server managing Analytics Monitoring Platform

Installation resources	20K Flows	40K Flows	60K Flows
Installed Memory	32 GB	32 GB	32 GB
Processor Core Count (physical + logical)	24	24	24
Disk Space	1 TB	2 TB	3 TB
Server Heap	6 GB	6 GB	6 GB
Client Heap	2 GB	2 GB	2 GB

NOTES:

1. It is recommended to use only the remote client for the Network Advisor server when managing Analytics Monitoring Platform with more than 20K Flows.
2. SSD storage is strongly recommended for better performance when managing Analytics Monitoring Platform. Future releases of Network Advisor when supporting Analytics Monitoring Platform will require the use of SSD and the storage space requirements may increase due to additional capabilities.
3. When managing Analytics Monitoring Platform, it is recommended to use a server with a minimum of two Processors/CPU's with each Processor/CPU having a minimum of six Physical cores with two or more threads (logical cores) per core, resulting in a minimum total of 24 logical cores.
4. When managing Analytics Monitoring Platform, the Network Advisor supports a maximum of 8K switch ports in a fabric.

Operating system cache requirements

It is recommended that you use the System managed size (the OS allocates the required cache); however, if you choose to use a custom size, make sure you use the following memory settings for your operating system.

The virtual memory requirements for Windows system is 1 GB for minimum paging file size and 4 GB for maximum paging file size.

Linux swap space requirements

Installed physical memory (RAM) size	Recommended swap size
Greater than 6 GB and less than 8 GB	Equal to the amount of RAM
Greater than or equal to 8 GB and less than 64 GB	5 times the amount of RAM

Client and server system requirements

Note: Network Advisor is not supported in a Network Address Translation (NAT) environment where the server and client are on different sides of the NAT Server.

Network Advisor has the following client and server system requirements:

1. In the Professional edition, a single server supports a single client, which must be a local client only.
2. In Professional Plus and Enterprise editions, a single server supports a maximum of 25 clients, which can be local or remote on 64-bit servers. To support more than 8 clients, you must make the following changes to your configuration:
 - a. Increase the server memory size. You can configure the server memory size from the Options dialog box, Memory Allocations pane. For instructions, refer to the Network Advisor User Manual or online help.
 - b. Increase the PostgreSQL database shared buffers memory allocation to 1024 MB by editing the *Install_Home\data\databases\postgresql.conf* file.

Upgrade and Migration considerations

Migration is supported from the following previous releases.

Pre-14.2 release	Versions
Network Advisor 14.0.x	14.0.0, 14.0.1, 14.0.2, 14.0.3
Network Advisor 14.1.x	14.1.0, 14.1.1

Note 1: Network Advisor 14.0.x (14.0.0, 14.0.1, 14.0.2, 14.0.3) and 14.1.x (14.1.0, 14.1.1) running on the Linux and Windows operating systems can be upgraded to Network Advisor 14.2.x

Note 2: All Network Advisor editions are supported only on 64-bit servers. To migrate Enterprise and Professional editions to a 64-bit server, refer to 'Pre-migration requirements when migrating from one server to another' section of the Installation and Migration Guide.

Note 3: Direct migration from pre-14.0.0 releases to 14.2.x is not supported. Refer to Supported migration paths in the Installation and Migration Guide for migration paths from DCFM, INM and pre-14.0.0 releases.

Note 4: Refer to Supported migration paths in the Installation and Migration Guide for SMI Agent only migration paths.

Note 5: SAN users may add IP management to Network Advisor 14.2.x for SAN+IP network management with the procurement of the IP functionality. Also, IP users may add SAN management to Network Advisor 14.2.x for SAN+IP network management with the procurement of the SAN functionality.

Note 6: Make sure minimum of free space is 1.5 times the size of the Network Advisor data folder (<Install_Home>\data) available for performing migration for the servers with large amount of Performance, Events, and Flow Vision data in the database.

Note 7: Network migration is not supported from 14.0.x releases to the 14.2.x release.

Note 8: Network migration is supported from 14.1.x releases to the 14.2.x release.

Note 9: Cleanup the monitor entries in NA Database during the Migration case (pre-14.1.x)

- When customer migrates from pre-14.1.x release to 14.2.x, following AMP related data would be removed in 14.2.x after migration:
 - Flows retrieved from AMP in pre 14.1.x release
 - Dropping all statistics retrieved from AMP in pre 14.1.x release
 - Out of the box dashboards, added in 12.4.2 and 12.4.3 release for AMP
 - o SAN Analytics Monitoring: Top Flows
 - o SAN Analytics Monitoring: Summary
- There are no changes made to the source (pre 14.1.x release) database. Customer can install respective pre 14.1 release and consume this data.

Note 10: Monitor entries migration from 14.1.x releases to 14.2.x release is supported.

Note 11: Migration/upgrade from Network Advisor v14.2.1 to 14.3.0 is not supported. Network Advisor v14.3.0 is recommended only for customers who have Analytics Monitoring Platform (AMP) in their Fabrics.

Migration Impact

If the OEM name for any of the switch models has changed from one release to another, then you will need to change the properties file after 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 and restart the server for changes to take effect.

Network Advisor downgrade to previous versions is not supported.

Configuration Considerations

Supported scalability limits by Network Advisor edition:

	Enterprise edition			Professional Plus edition	Professional edition
	Small	Medium	Large		
SAN switch ports	2000	5000	15000	2560	300
SAN switches and Access Gateways	40	100	400	40	15
SAN devices	5000	15000	40000	5000	1000
SAN Fabrics	25	50	100	36	2
MPLS switches	1	10	100	1	Not supported
VDX switches	50	100	400	50	50
Managed Hosts	20	100	400	100	20
vCenters	1	5	10	5	1

VMs (includes powered down VMs)	1000	5000	10000	5000	1000
ESX Hosts	200	1000	2000	1000	200

Notes:

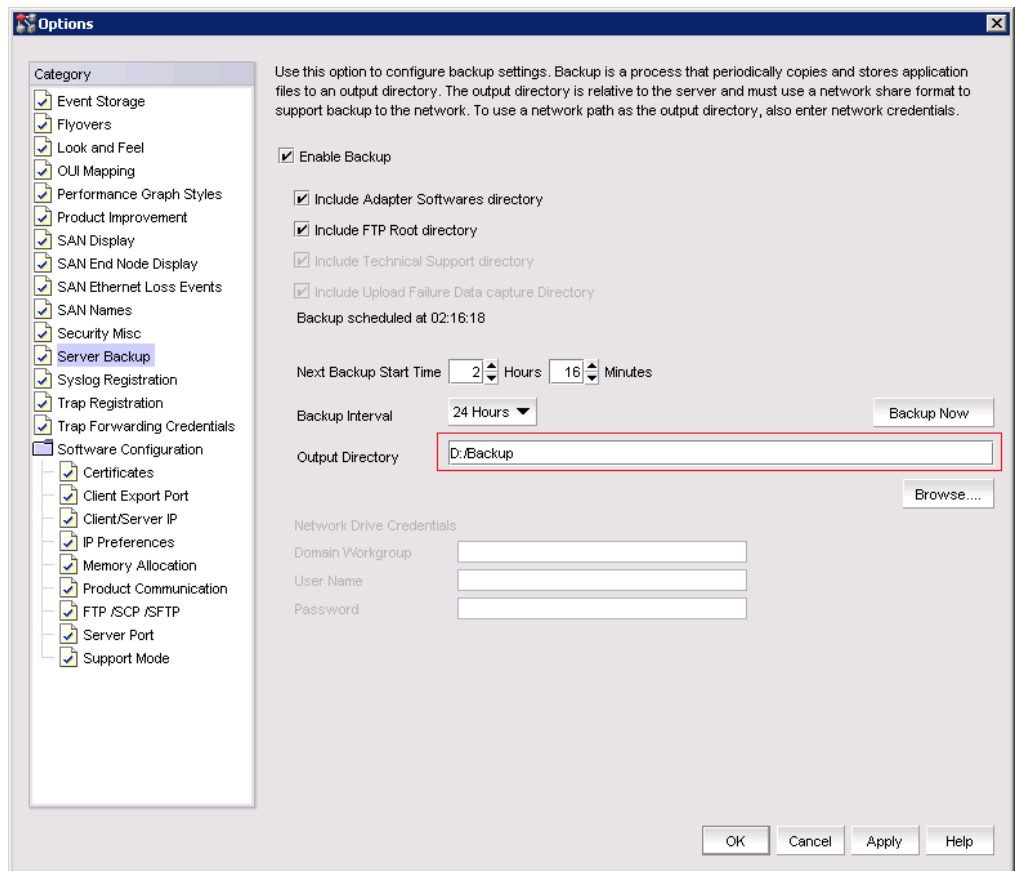
1. Virtual Fabrics are counted as fabrics when calculating the managed count limits.
2. Supported network latency between Network Advisor server and client or server and devices is 100ms.
3. Professional Plus edition is not supported for the IP package.
4. Supported network latency between Network Advisor server and client or server and devices is 100ms.

Limitations and Restrictions

QLogic branded adapters are not supported for discovery.

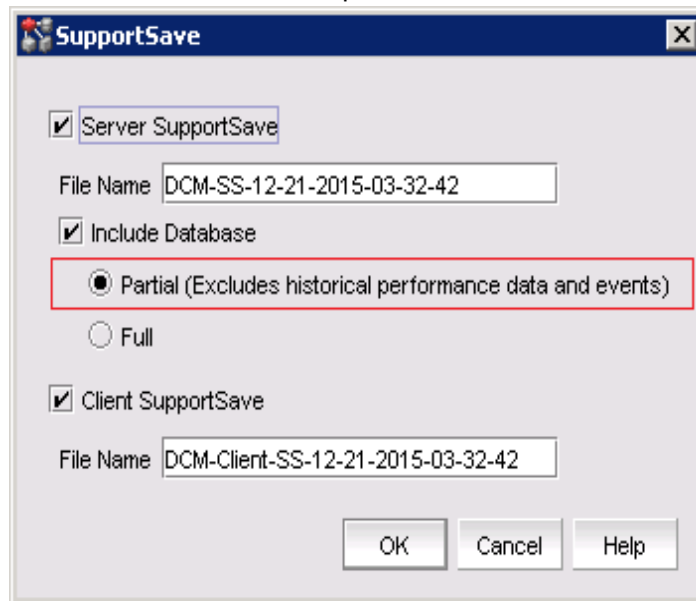
Important Notes for managing Analytics Platform (Only for AMP users)

- **Backup and restore recommendations**
 - a) With AMP discovered in NA 12.4.4, for Back up, it is recommended to use with External device with since backing up to CD is not the recommended method. The usable capacity of a CD is
 - i. Approximately 700 MB and needs to be replaced when full. It is recommended that you configure the backup system to target a hard drive or a network drive.
 - ii. Note that: The amount of space required for each backup is 1/10th of the size of NA installation directory and the backup process takes about 1.5 hours for 100GB of data.
 - b) By default, the NA server backup is scheduled for every day - a backup every 24hrs. With AMP discovered in NA 12.4.4, since the data size will be huge,
 - i. If user needs better NA performance, it is recommended to disable the default scheduled back by disabling the “Enable Backup” option (also shown in the figure below) and trigger a manual backup on a weekly basis or based on the need, by enabling the “Enable Backup” check box and selecting “Backup Now” button.
 - ii. If user needs the data back up every day, then the performance of the NA will be impacted due to the backup process. Based on the need, the backup can be planned.



- **Support save recommendations**

- a) With AMP discovered in NA 12.4.4, for capturing the Server and Client support save data, it is recommended to select the Partial option, this would exclude historical performance data and events from the database capture.



- **Disk space recommendation in case of migration**

- a) It is recommended to have free disk space of 3 times the size of “NA installation folder/data”. Note that it would take approximately 2 hours to complete the migration for 100G of data folder size.

Example:

Size of the “NA installation folder/data” is – 500 GB

Additional free disk space required is - 1000 GB (1.5 TB)

Time that will take for completing migration would be – 10 hours approximately.

- **Performance considerations for Dashboard**

- a) When there are more than 30k flows monitored in NA

- i. It is recommended to select the 30 minutes or 1 hour time scope for better performance of the drill down graphs/dialogs
- ii. The drill down graph/dialog launch will take around 5 minutes when user selects 6 hours/12 hours/1 day time scope.

- **Any AMP device should be discovered only by one NA server**

Upgrading the License

The quickest and simplest method of moving from one package to another is to enter the new license information on the Network Advisor License dialog box. The following tables list the available upgrade paths.

SAN Upgrade Paths

Current software release	To software release
SAN Professional	SAN Professional Plus or Licensed version SAN Enterprise Licensed version
San Professional Plus Licensed version	SAN Enterprise Licensed version
SAN Enterprise Trial	SAN Enterprise Licensed version

License Upgrade procedure in Network Advisor

1. Select **Help > License**.
The Network Advisor License dialog box displays.
2. Browse to the license file (.xml) and click **Update**.
3. Click **OK** on the Network Advisor License dialog box.
4. Click **OK** on the message.
The Client closes after updating the license successfully. Restart the Server from the Server Management Console for the changes to take effect.
5. Open the application (double-click the desktop icon or open from the Start menu). The Log In dialog box displays.
6. Enter your user name and password.
The defaults are Administrator and password, respectively. If you migrated from a previous release, your user name and password do not change.
7. Select or clear the **Save password** check box to choose whether you want the application to remember your password the next time you log in.
8. Click **Login**.
9. Click **OK** on the Network Advisor Login Banner.

Downgrading the license

User can downgrade from a higher Trial configuration to a licensed version with a lower Configuration. User can perform the following types of downgrade:

- Edition
- Package
- MPLS
- IP Product Count

Notes:

1. Downgrade to Professional Edition is not supported.
2. Downgrading to a Trial version is not supported.
3. Downgrade during migration (Configuration Wizard) is not supported.
4. License downgrade operation will not run when IP Profile discovery and Server Backup are in progress.
5. If you combine more than one downgrade option, you must meet the requirements for all downgrade options.

Edition downgrade paths

Current software release	To software release
Enterprise SAN	Professional Plus SAN

Defects

Defects closed with code change in IBM Network Advisor 14.2.2

This section lists the defects with Critical, High and Medium Technical Severity closed with a code change as of January 05, 2018 in Network Advisor 14.2.2.

Defect ID: DEFECT000657589	
Technical Severity: High	Probability: High
Product: Network Advisor	Technology: Security
Reported In Release: Network Advisor 14.0.1	Technology Area: Security Vulnerability
Symptom: Network Advisor remote client launch will fail showing a message that certificate has expired (Application Blocked by Java Security)	
Condition: When launching the remote client on Network Advisor 14.3.1 or earlier versions after February 18th, 2018.	
Recovery: Users that wish to continue using a Network Advisor with an expired certificate in remote client mode can perform the following steps: 1. Add the Network Advisor URL to an Exception Site List under the "Security" tab of the Java Control Panel 2. Disable signed code certificate revocation checks.	

Defect ID: DEFECT000629457	
Technical Severity: High	Probability: Medium
Product: Network Advisor	Technology: Partner Integration
Reported In Release: Network Advisor 14.2.0	Technology Area: SMI Agent
Symptom: Intermittently a "java.lang.NoClassDefFoundError" is shown and indications are not received with neither http or https.	
Condition: Issue seen when attempting to create indication subscription in SMIA client bundled within the Network Advisor.	

Known Issues

Important SAN Notes

- While pushing larger zone configurations, make sure to reserve enough space in zoneDB to accommodate hdr size of all the LS and actual committed configuration within the zoneDB max size. It is recommended to add zones gradually. Pushing Zone DB of size more than max zone DB size, will set available zone DB size to negative value which in turn causes a deadlock where any zone operation will not work.
- FOS 8.1.0x and NA 14.2.x support a total of 16 LS on each X6 Director. For Creation, Modification, or Deletion of Logical Switches in FICON environments, it is highly recommended to limit these operations from Network Advisor's Logical Switches dialog to less than 4 LS at-a-time to avoid timeout issues. For non-FICON environments, a limit of 8 LS at-a-time is enforced.
- Firmware Download fails if built-in SCP is used as preferred protocol. The workaround is to use the FTP/SFTP option in NA
- SNMPv3 using AES256 algorithm may not work with certain passwords as there could be some mismatch for encryption/decryption of passwords. For example: "pass1", "xyz12mo" fails whereas "xyz12" works. This is because AES256 algorithm is not a standard implementation

- Trying to move 200+ ports to a Logical Switch with 'Reset to Default' option selected, results in operation time-out.
- During installation, if Network Advisor database initialization fails on Windows Operating System, 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.
- The FCIP links will not be shown in the topology for tunnels with degraded circuits
- IP Ping, IP Route and Trace route is not supported for 7840/SX6
- 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, as in case of AG discovery which requires use of SNMPv1 by default.
- 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 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

- 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 7840/SX6
- Emulex: HTTPS discovery for ESXi host will work only with certificate import
Workaround
Perform the following two steps to work around this issue.

Step 1) Add following line in <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 below:

/root/.java/deployment/deployment.properties

Step 2) Launch the java control panel using below command and click on Ok button <Network Advisor Home>\jre\bin\jcontrol

- If Network Advisor is installed on Linux Operating System, the Fabric OS Element Manager and HCM cannot be launched when the client is launched using the 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, launch the Network Advisor client from a browser (after installing supported JRE 7 version), pointing to the Network Advisor server installed on that machine.

Workaround

Perform the following steps to work around this issue.

Step 1) Add following line in <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 below:

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

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

`<Network Advisor Home>\jre\bin\jcontrol`

- Secure Syslog is not supported from Network Advisor
- SAN Configuration Purge Backup is being enabled automatically when “Enable Scheduled Backup” is set and remains enabled after disabling the Scheduled Backup.
- User is not recommended to perform write operations such as delete or enable/disable on FCIP tunnels which have circuits with different IDs.
- 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.
- Firmware upgrade will happen serially for B7840's with HA configured tunnels between them. For parallel download on B7840's use CLI.
- FCIP circuit trace route verification fails when attempted from Network Advisor
- Web tools launch is not supported for Analytics Monitoring Platform
- HTTP TRACK/TRACE methods are not blocked in NA 14.2.0 JBoss (v 8.2) Webserver. If a web application server has TRACE enabled, attacker (Cross-Site Tracing attack) can just send Http request to the target server and in turn attackers will be able to hijack the session.
- SAN Inventory widget in default dashboard shows ‘Error loading the data’ on creating and deleting custom dashboards inconsistently when managing more than 9000 ports. User has to re-launch the client to see the data again.
- Do not enable “Use SSL 2.0 compatible ClientHello format” setting in Java Control Panel on the Network Advisor Client machine as it will interfere with the remote client launch.
- For AMP users with scaled number of AMP flows, it is recommended that you disable daily database backups for better Network Advisor performance with the AMP case. If local server has JRE version 1.8u112, the links in Configure SMIA Agent dialog in Server Management Console, will not launch.
Workaround:
Uninstall the JRE version 1.8u112 or install JRE version 1.8u111.
- While generating reports from Microsoft Windows command prompt and saving the report in non-default location, the report output directory path should not end with the backslash (“\”), or the backslash character should be prefixed with forward slash (“/”). For example: –o “c:\V”.
- As per the Fabric OS design, all three AAA servers (RADIUS, ADLDAP, TACACS+) have to be configured together. All three AAA server settings should be present in the configuration file (from COMPASS), when we want to add any one server additionally (RADIUS, ADLDAP, TACACS+). This can be achieved in COMPASS using “Import from Switch” and “Edit” options.

For example, let's say all the three AAA servers are configured on switch. From COMPASS, if we try to push only ADLDAP configuration during sync operation then already configured RADIUS and TACACS+ configurations on switch will get removed. The template configuration present in the configuration file will get downloaded to switch replacing the existing configuration.

- Make sure that the Management application server and the Fabric Insight Portal system clocks are synchronized even if they are in different time zone.

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 going to the discovery dialog and add the IP address of the chassis using the Add dialog.

SSL connections using certificates with MD5 signatures

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. Java 1.8 used by NA 12.x disables the use of certificates with 'weak' authentication. The certificates on such devices need to be updated to be compliant with JRE v1.8. Please refer to the 'Secure Sockets Layer protocol' section of Fabric OS 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:

- a. 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.
- b. 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:

- a. In 7800, 7840 and FX8-24, GE ports cannot be reset to default unless their corresponding VE ports are cleared of their FCIP configurations
- b. Switch reset to default operation on SAN42B-R may fail due to GE port sharing or if the associated VE port exists in another LS

Important Notes common for SAN and IP

1. In rare cases, due to some interactions with virus scan software, Network Advisor Server Start process might go on 10 to 12 minutes, or may fail to start the server. If this happens, then configure the virus scans to skip scanning Network Advisor files.
2. 64 bit OS is required to run any edition of Network Advisor - Professional, Professional-Plus and Enterprise.
3. Network Advisor server startup and restart may take up to 10+ minutes to complete.
4. To avoid excessive telnet/ssh login messages in the Network Advisor master log and event report, and the device CLI console, disable lazy polling by un-checking the "Enable lazy polling" checkbox in **IP Discovery Global Settings > Preferences Dialog**.
5. Starting 12.0, the supported number of client connections has increased to 25. Please refer to the installation guide for the 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. [This setting can be done by editing <installation_directory>\data\databases\postgresql.conf file.]

Change following line:

```
From: shared_buffers = 512MB
To:   shared_buffers = 1024MB
```

- Server needs to be restarted.
6. In Linux 64 bit machines, connecting to the database through Open office using ODBC will not work. Solution is to connect from Windows ODBC Client to the 64 bit Linux machine where Network Advisor is running to view the Database tables.
 7. 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 Network OS and Fabric OS devices the below 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"
 8. 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 'Client only installation' section of the Installation and Migration guide for details.
 9. "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.
 10. Intermittently HTTP 500 error message is displayed when launching the Web Client. Server restart will fix the issue.
 11. User needs to run the "sanperformancestatenable" script from NA home utilities folder to enable/disable performance statistics collection for SMIA only package installation. Below are the steps to execute the script,

Windows:

Open cmd prompt and move to <NA_HOME>\utilities and run
sanperformancestatenable.bat dbusername dbpassword enable|disable

Linux: Open terminal and move to <NA_HOME>\utilities and run
sanperformancestatenable dbusername dbpassword enable|disable

12. 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.

13. REST API does not provide FCIP circuit measures for the GigE port.
14. NA is now enforcing minimum disk space requirements during migration. When the disk space requirements are not met, NA display a message prompting the user to use the script to delete performance data and retry migration.
15. 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.
16. MAPS Compare Help dialog is not launching, user has to search the Help contents from **Help menu > Contents**
17. When Network Advisor is managing more than 1500 IP products, user might experience some performance degradations such as delays while launching some dialogs.
18. 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.

Please refer the following link for more information:

<http://msdn.microsoft.com/en-us/library/windows/desktop/ms683502%28v=vs.85%29.aspx>

19. 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 Guide for the instructions to install the source version services manually.
20. The ports listed in Network Advisor Installation and Migration guide need to be open bi-directionally for all the bi-directional protocols in the firewall where the server is installed.
21. If source Network Advisor has more products discovered then it is recommended to stop all the services manually from Network Advisor Server Management Console of the older version before initiating migration from the Configuration Wizard.
22. Reports: The user is recommended to run not more than 50 schedules at the same time to avoid performance issues.
23. Service start up failure can be seen in Windows 2008 R2 OS and the recommendation is to apply this hot fix from <http://support.microsoft.com/kb/2577795>
24. If you see the following error message "Signature could not be validated" during firmware download or technical support data collection (Fabric OS and Network OS devices only) or configuration backup/restore (Network OS devices only) 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. Try 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>
```

For Network OS devices

Firmware version 3.0 and later

```
sw0# clear ssh-key <IP Address of SSH server to be deleted>
```

Firmware version 2.1.1b

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

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

If the above does not work, go to Server > Options > Software Configuration > FTP/SFTP/SCP, and uncheck the SCP/SFTP option.

25. You need to use a different (non-default) name for the widget when attempting to add “Top Product Response Time” widget to avoid this error “Monitor could not be added. Duplicate monitor name”.
26. Patch Installer troubleshooting – The 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 “Chapter G: Troubleshooting - Patch troubleshooting” Section of the User Manual and then launch the patch installer.

Domestic and International Modem based Call Home is no longer supported for Call Home

Alternatively, customers using Domestic or International Call Home Modem feature can reconfigure their Call Home to utilize the Email option for continued Call Home notifications in the event of a system problem. Please refer to the Call Home section of the Network Advisor User Manual for more configuration details. Note that **EFCM** and **DCFM** customers will also be affected by this change and need to reconfigure their call home to utilize the Email option for continued Call Home notifications in the event of a system problem.

Support Saves and server backup may take a long time with large databases

As databases grow larger from Event, sFlow, and Performance Collector data, support save and server backup operation may take a long time to run. Larger databases will promote longer support save/ server backup operations.

For server backup, make sure you have free disk space equivalent to “total of twice the <Install_Home>\data folder (except databases folder) and 30% of <Install_Home>\data\databases folder”.

For support save collection, make sure you have free disk space equivalent to a “total of <Install_Home>\logs folder and 30% of <Install_Home>\data\databases folder”

Note:

For networks with large amounts of data to backup, the Management application's performance is degraded during the daily scheduled backup. To avoid performance degradation, configure backup to an external hard drive or use Backup Now on demand.

Installation on Network Mounted Drives is not supported

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

Client disconnects

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

Cross-flavor Migration

Migrating same version of NA (14.2.1) from OEM1 version to OEM2 version:

- a. Partially uninstall the source NA 14.2.1 OEM1 version
- b. Now install NA 14.2.1 OEM2 version

- c. In the 'copy data and settings' page, browse to the NA 14.2.1 OEM1 version and continue with the migration.

Migrating NA (pre-14.2.1) OEM1 version to NA 14.2.1 OEM2 version:

- a. Install the source NA pre-14.2.1 OEM1 version
- b. Now install NA 14.2.1 OEM2 version
- c. In the 'copy data and settings' page, browse to the NA 14.2.1 OEM1 version and continue with the migration.

Virtual Connect Enterprise Manager (VCEM) Support

The supported and tested versions are listed below:

HP SIM Version	v7.4.0
HP VCEM version	v7.4.1
OA firmware	Onboard Administrator (OA) v2.41 or later
VC E-net module firmware(HP VC 8Gb 20-Port FC Module & HP VC 8Gb 24-Port FC Module)	v3.15
Hardware	HP BladeSystem c3000 or c7000
Servers	Proliant BL465c G7, Proliant BL460c G6
HBA	Brocade 804 8Gb FC HBA, Emulex LPe1205-HP 8Gb FC HBA, QLogic QLE2562 8Gb FC HBA, QLogic QLE2672-CK 16Gb FC HBA

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.

Name			Source value	Formula
TX	FC	SP	.1.3.6.1.3.94.4.5.1.6	$TX = (\Delta \text{valueP1P} / (1000 * 1000)) / (\text{Polling intervalP2P})$
RX	FC	MP	.1.3.6.1.3.94.4.5.1.7	$RX = (\Delta \text{valueP1P} / (1000 * 1000)) / (\text{Polling intervalP2P})$
TX	G	SP	.1.3.6.1.2.1.31.1.1.1.10	$TX = (\Delta \text{valueP1P} / (1000 * 1000)) / (\text{Polling intervalP2P})$
RX	GE	SNMP	.1.3.6.1.2.1.31.1.1.1.6	$RX = (\Delta \text{valueP1P} / (1000 * 1000)) / (\text{Polling intervalP2P})$
TX	FCIP	SNMP	.1.3.6.1.2.1.31.1.1.1.10	$TX = (\Delta \text{valueP1P} / (1000 * 1000)) / (\text{Polling intervalP2P})$

RX	FCIP	SNMP	.1.3.6.1.2.1.31.1.1.1.6	$RX = (\Delta \text{valueP1P} / (1000 * 1000)) / (\text{Polling intervalP2P})$
Uncompressed Tx/Rx MB/sec	FCIP	SNMP	.1.3.6.1.4.1.1588.4.1.1.6	$(\Delta \text{valueP1P} / (1000 * 1000)) / (\text{Polling intervalP2P})$
TX	EE Monitors	HTTP	PortRX (variable from the return html file)	$TX = (\Delta \text{valueP1P} / (1000 * 1000)) / (\text{Polling intervalP2P})$
RX	EE Monitors	HTTP	PortTX (variable from the return html file)	$RX = (\Delta \text{valueP1P} / (1000 * 1000)) / (\text{Polling intervalP2P})$
TX	HBA, CNA	HCM API	NA	$TX = (\Delta \text{valueP1P} / (1000 * 1000)) / (\text{Polling intervalP2P})$
RX	HBA, CNA	HCM API	NA	$RX = (\Delta \text{valueP1P} / (1000 * 1000)) / (\text{Polling intervalP2P})$
TX	TE	SNMP	1.3.6.1.2.1.31.1.1.1.10	$TX = (\Delta \text{valueP1P} / (1000 * 1000)) / (\text{Polling intervalP2P})$
RX	TE	SNMP	.1.3.6.1.2.1.31.1.1.1.6	$RX = (\Delta \text{valueP1P} / (1000 * 1000)) / (\text{Polling intervalP2P})$
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 = $((\Delta \text{value1 of TX or RX}) / ((\text{Bytes transmitted} * \text{port speed}) * (\text{polling interval2}))) * 100$ where Bytes transmitted for 1G,2G,4G,8G and 16G 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 = $((\Delta \text{value1 of TX or RX}) / ((125000000 * \text{port speed}) * (\text{polling interval2}))) * 100$. If the 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 = $((\Delta \text{value1 of TX or RX}) / (\text{maximum bytes transmitted}) * \text{polling interval2})) * 100$, 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 = .1.3.6.1.2.1.31.1.1.1.1.6	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 valueP1P / (1000 * 1000)
Other Counters				Other counters = Delta valueP1P
Current Compression Ratio	FCIP	NA	NA	(ifHCInOctets + ifHCOctets) / fcipExtendedLinkCompressedBytes

1. Delta valueP¹: is the difference of value retrieved between the two consecutive polling cycles.
2. Polling intervalP²: duration between the two polling cycle in seconds

SMI Agent

- For Network Advisor that has more than 30K instances, the CIMOM takes more memory to generate CIM instances.
- If user performs Enumerate Instances and total number of size is more than 2 MB for all managed fabrics, it may result in out of memory issue. In this case, 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 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 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.

CIMOM Heap Size

The CIMOM heap size has been increase for small, medium and Large SAN Network Sizes:

Old heap size:

small

platform.32.cimom.conf.set.MAX_HEAP_SIZE = 768m
platform.64.cimom.conf.set.MAX_HEAP_SIZE = 1024m

medium

platform.32.cimom.conf.set.MAX_HEAP_SIZE = 768m
platform.64.cimom.conf.set.MAX_HEAP_SIZE = 1536m

Large

platform.32.cimom.conf.set.MAX_HEAP_SIZE = 1024m
platform.64.cimom.conf.set.MAX_HEAP_SIZE = 2048m

Current Heap Size:

small

platform.32.cimom.conf.set.MAX_HEAP_SIZE = 1024m
platform.64.cimom.conf.set.MAX_HEAP_SIZE = 1536m

medium

platform.32.cimom.conf.set.MAX_HEAP_SIZE = 1024m
platform.64.cimom.conf.set.MAX_HEAP_SIZE = 2048m

Large

platform.32.cimom.conf.set.MAX_HEAP_SIZE = 1024m
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 <Installation Dir>\conf folder.

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

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

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:

1. accepts WBEM requests over HTTP using SSL on TCP port 5989
 2. accepts WBEM requests over HTTP without SSL on TCP port 5988
 3. slptool findattrs service:wbem:http://IP_Address:Port
 - a. Use this command to verify that Management application SMI Agent SLP service is properly advertising its WBEM SLP template over the HTTP protocol.
 - b. 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.
4. slptool findattrs service:wbem:https://IP_Address:Port
 - a. Use this command to verify that the Management application SMI Agent SLP service is properly advertising its WBEM SLP template over the HTTPS protocol.
 - b. 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:

1. SLP log—Management_Application\cimom\cfg\slp.log
2. SLP daemon—Management_Application\cimom\cfg\slp.conf
The SLP daemon can be reconfigure the by modifying this file.
3. SLP register—Management_Application\cimom\cfg\slp.reg
statically register an application that does not dynamically register with SLP using SLPAPIs by modifying this file. For more information about these files, read the comments contained in them, or refer to <http://www.openslp.org/doc/html/UsersGuide/index.html>

Verifying SLP service installation and operation on Windows systems:

1. Launch the Server Management Console from the Start menu.
2. Click Start to start the SLP service.
3. Open a command window.
4. Type `cd c:\Management_Application\cimom \bin` and press **Enter** to change to the directory where slpd.bat is located.
5. Type `> slptool findsrvs service:service-agent` and press **Enter** to verify the SLP service is running as a Service Agent.
6. Type `> slptool findsrvs service:wbem` and press **Enter** to verify the SLP service is advertising its WBEM services.
7. Choose one of the following options to verify the SLP service is advertising the WBEM SLP template over its configured client protocol adapters.

Type `> slptool findattrs service:wbem:http://IP_Address:Port` and press **Enter**.

Type `> slptool findattrs service:wbem:https://IP_Address:Port` and press **Enter**.

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