Network Advisor 14.2.1 Release Notes

Contents of this file:

HPE B-series Network Advisor 14.2.1 Release Notes

Brocade Network Advisor 14.2.1 Release Notes v1.0

HPE B-series Network Advisor Enterprise, Professional Plus, and Professional 14.2.1
Release Notes

Description

HPE B-series Network Advisor Release Notes have been posted on HPE's web site at the HPE Support Center.
See the Brocade Network Advisor Release Notes for general information and details on fixes as well as other important information pertinent to this release. The HPE B-series Network Advisor Release Notes only contain HPE specific information related to this release.

Update recommendation

HPE strongly recommends that you upgrade to this version as soon as possible to take advantage of the latest fixes and features.

To access the latest HPE B-series Network Advisor software:

- Select "Support" from the hpe.com home page
- Select "HPE Support Center" under "Product Support".
- Enter your B-series switch model into "Get drivers, manuals, parts & solutions", then select your specific switch from the next screen.
- Under "Download options" select "Get drivers, software and firmware"
- Click on your specific B-series switch model
- With Driver Language selected as "English", select "OS Independent" under "Operating systems in English"
- Click "Application" under "OS Independent Downloads"
- To read the Network Advisor Release Notes, find the firmware version you are looking for in the "Current version" column, click the link under "Description" for that version, then click the "Release Notes" tab on the next page.
- To download the Network Advisor, click the "Download" button

Standards compliance

This software conforms to the FC standards and accepted engineering practices and procedures. In certain cases, HPE might add proprietary supplemental functions to those specified in the standards. For a list of standards conformance, see the HPE website: http://www.HPE.com.

Supported product models

For the latest product support information, see the Single Point of Connectivity Knowledge (SPOCK) on the HPE website: http://www.HPE.com/storage/spock.

Under "Other Hardware", select "Switches". You must sign up for an HPE Passport to access this website.

Fibre Channel and Fibre Channel Routing scalability

For the latest information about Fibre Channe and Flibre Channel Routing (FCR) scalability support, see the *HPE StorageWorks SAN Design Reference Guide*, available on the HPE website, at: http://www.HPE.com/go/sandesignguide.

Brocade Network Advisor 14.2.1

GA Release Notes v1.0

May 31, 2017

Document History

Version of Document	Summary of Changes	Publication Date
v1.0	Initial Draft	5/31/17

Contents

Overview

Brocade Network Advisor Version 14.2.0

Brocade Network Advisor 14.2.0 is a major release supporting Fabric OS 8.1.0, NOS 7.1.0, FI 8.0.50, NI 6.1, VM insight, various enhancements to MAPS, Flow Monitoring, FCIP, Usability and troubleshooting areas.

This release inherited the Fabric Insight Portal web client (designed in Network Advisor 14.1.x release for AMP users only) for general SAN users to provide the user with an easy to use and intuitive interface for monitoring IO level and fabric behavior in a Brocade Fibre Channel SAN fabric. The Network Advisor Fabric Insight Portal also introduces Flow Collections and Flow Filtering for Analytics Monitoring Platform flow management, and custom Rules Sets for use with MAPS for more flexible and granular flow monitoring.

New Enhancements

- Fabric OS platform support
  - o Fabric OS 8.1.0
  - o Brocade G610 switch
- VM Insight support
  - o Identify and track VMs within a fabric
  - o Provide VM visibility in Fabric Vision technology for monitoring and diagnostics
  - o Flow Monitoring
- Flow Vision enhancements
  - o Top N Flows/Bottom N Flows – Dashboard widget - Entity ID, VM Name and Application name added to the Top N /Bottom N Flows widgets
  - o Flow Vision IOS Measures support in Historical Graph and Dashboard
- MAPS Enhancements
  - o VM Insight based flows
  - o Alert Severity Support for MAPS Rule

- o Enhancement in MAPS Policy Creation
- o New default Rules to Monitor Rx, TX & UTIL Measures
- o New default Rules to Monitor ERR_PORTS measures
- o Fabric Performance Impact (FPI) Monitoring Feature Enhancements
- o MAPS Rule Name Limitations
- o Monitor Front end Encryption port
- o Support for uninstalling vTAPs when threshold of 250K IOPS is exceeded
- o User defined policies and rules limits
- o Quiet time support for SNMP
- o Restriction of Orphan rules creation
- Web UI Enhancements
- AMP Enhancements
- CLI Reports
  - o Various reports for AMP users and general FC
- Zoning
  - o Alias Support in Peer Zoning
  - o Enhanced Zone Name Support
  - o Zone DB size restriction based on per chassis limit
  - o Alias/Zone creation by Port WWN instead of Node WWN
- Virtual Fabric
  - o Offline LISL state at Logical Switch creation
  - o FICON LS support
  - o 16 LS support for Gen-6 chassis
- FCIP
  - o 10 circuits/tunnel support
  - o Circuit measures in performance graphs and dashboard
  - o WAN Vision Dashboard
- COMPASS Enhancements
  - o Track Switch User Accounts
  - o Track Switch User Account Credential
- Web Client
  - o Unified Inventory
  - o PM support for NOS and IP
- Campus Enhancements
  - o Campus Dashboard
  - o New Syslog Formatting
  - o sFlow support for Campus Fabric
  - o Stack ISSU Support
- REST API
  - o Port enable/disable, Port name settings
  - o 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
- Brocade 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

Brocade Network Advisor Version 14.2.1

Brocade Network Advisor 14.2.1 is a software maintenance release based on Brocade Network Advisor 14.2.0. All hardware platforms and features supported in Brocade Network Advisor 14.2.0 are also supported in Brocade Network Advisor 14.2.1.
The fixes included in this release are listed in the defect tables below in this document.

New Enhancements
- Fabric OS platform support
  - Fabric OS 8.1.0x
- IOS Firmware support
  - FI 8.0.60
  - ICX 7150
- 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
- Brocade Analytics Monitoring Platform support
  - Filter management – support for specifying range of LUN
  - Support wildcard in Filter definitions
  - Support SRDF (replication) flow
  - Ability to add collection as filter in filter bar
  - UI enhancements - menu launch points, metrics selection, view refresh
  - Collection Management enhancements - Ignore Default Rules, Create New Custom Rulesets, Configure Rule dialog
  - ampos 2.0.1 support
- Defect fixes provided

Important considerations for web client users

This release introduces a new improved web client design - Fabric Insight Portal - replacing the web client supported in releases BNA versions 14.0.x and earlier. The Fabric Insight Portal uses new design paradigms for ease of use and will be enhanced going forwards. In this release the web client functionality fully replaces the earlier web client with the following caveats:

- SAN Report Builder – this functionality is deprecated and replaced with a command line driven set up reports for SAN FC environments.
- Global search - In this release is restricted to searches within a single instance of BNA and not across BNA instances.
- Supportsave for NOS is not included in the new web client.

Deprecated Web Client (14.0.x)

In Network Advisor releases 14.0.x and earlier, when pointed the browser at the Network Advisor server hostname or IP address, you were directed to a Web Page where you could access some functionality of the Java based client through a browser. The functions, such as Dashboards, Inventory, Events, Reports, were provided mainly in read-only mode. This client was based on software technology that is deprecated and no longer supported. It is replaced with the Fabric Insight Portal, a browser accessible User Interface based on cutting edge User Interface technology and modern web-based applications workflows and paradigms.

Fabric Insight Portal (new)

The new Fabric Insight Portal provides the user with an optimized interface for monitoring and accessing the detailed IO-level flow information provided by the Analytics Monitoring Platform. This interface was designed to match common workflow processes users will follow when investigating application performance, understanding workload behaviors, troubleshooting performance issues, or tuning and optimizing a SAN environment.

Now, when the user specifies the IP address or hostname of a Network Advisor server from a standard web browser, they will be directed to the new Network Advisor Fabric Insight Portal UI. The same credentials used in the traditional Network Advisor client are used to login to the server.

In addition to the new interface design of the Fabric Insight Portal, the database and back-end architecture has been redesigned in Network Advisor to provide better performance when managing a SAN with AMP. This new architecture enables highly responsive updates in the Fabric Insight Portal, whether for bringing up a dashboard view, drilling down into detailed information in the new Investigation Mode, or examining lists of flows from one or multiple AMP appliances in the environment. The new architecture and UI design also allow Network Advisor to scale and support even more AMP flows than in previous releases.

With the introduction of the Fabric Insight Portal, some functionality that was available in the legacy web client has been changed or removed. The following sections summarize key new features

introduced in the Fabric Insight Portal and also note functionality that has changed or is not supported in this new interface. For details of the supported features and functions, please refer to the 14.2 User Documentation.

Fabric Insight Portal Filters (new)

In Network Advisor 14.2, Fabric Insight Portal introduces support for Filters, a new capability that allows user to zero in on specific AMP flows of interest. Filters allow users to quickly and easily investigate behaviors related to a specific application, host device, or storage array and retain their filter configuration for future use. Filters can be applied to templates, dashboards, and detailed Network Flows information and support zones and zone aliases for easy identification of devices in a SAN.

Fabric Insight Portal Collections (new)

The Fabric Insight Portal in Network Advisor 14.2 also introduces support for collections, logical groupings of flows identified and tracked by the Analytics Monitoring Platform. Users can define Flow Collections to fit their needs for monitoring, performance optimization, investigation, troubleshooting, reporting, and a variety of other purposes.

Flow Collections also support the ability to establish custom Rule Sets for the flows in a collection, allowing users to specify IO performance and latency thresholds at unique levels for different applications or types of storage devices. The Flow Collection Rule Sets are managed in the Fabric Insight Portal and sent to AMP appliances to monitor the unique rules in real time and for every IO operation.

Users can also choose to create aggregate Flow Collection metrics, providing a look at IO level performance and behaviors for the Flow Collection as a whole. This allows the SAN Administrator to understand performance behaviors and investigate an entire storage array, application, business group, department, or other logical grouping as a complete entity, instead of the individual flow components of the group.

SAN Dashboards and AMP Dashboards (new)

The Network Advisor Fabric Insight Portal provides the SAN Dashboards that are most useful in managing the SAN. In addition it provides two new Dashboards and widgets to manage, investigate, and troubleshoot environments using AMP.

Note. Dashboards for IP Port Health are not available in the Fabric Insight Portal in Network Advisor 14.2. If your deployment contains Brocade's IP switches and Routers, please use the standard Java client to access the IP Dashboards or use Network Advisor versions other than 14.2.

SAN Inventory

The SAN Inventory web pages are replaced with a new and redesigned look in the Fabric Insight Portal in 14.2.

IP Inventory

IP Inventory web pages are replaced with a new and redesigned look in the Fabric Insight Portal in 14.2.

Events

The Events page is supported in the Fabric Insight Portal in Network Advisor 14.2.

Reports

The Reports capability available in the web client in previous versions of Network Advisor is not supported in Network Advisor 14.2.   Using the Fabric Insight Portal, users are able to easily export any widget available in any dashboard or template in seconds.

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:
  - Brocade 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 Brocade 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."

Supported OS, Browsers, JRE

Supported 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

Supported Browsers

Recommended browser versions:

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

Supported JRE versions

Network Advisor version	JRE version supported
14.2.1	JRE 1.8u131

Note 1: Web Tools launch from Network Advisor is also supported for the above combination.

Note 2: Applicable **only to WebTools from Fabric OS releases done before 2/13/2015**. Due to java signing certificate expiration, the Web Tools launch from Network Advisor will not work with JRE 8. 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 79/80 and set the security level to Medium. If you have 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, 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 JRE versions for this release are listed in JRE Support table. Beyond JRE expiration date you will see the message "Your Java version is out of date" on attempt to launch the web client.

You can either ignore the message "Your Java version is out of date" by selecting a later option and proceed with the web start client, or 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 JRE Support table>. Do you want to continue?"

Note 4. JRE 1.8.0 update 66 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

- Apply the following workaround on a computer when launching WebTools using a browser or the Network Advisor Remote client for all Fabric OS versions earlier than the above listed:
  a. Navigate to the jre installation directory.
     On Windows, navigate to C:\Program Files\Java\jre8\lib\security
     On Linux, navigate to <jre install directory>/lib/security

  b. Open the java.security file and change the jdk.certpath.disabledAlgorithms=MD2, RSA keySize < 1024 value from 1024 to 256.
     For example, jdk.certpath.disabledAlgorithms=MD2, RSA keySize < 256

- Apply the following workaround on the Network Advisor server when launching Element Manager from Network Advisor client for all Fabric OS versions earlier than the above listed:
  a. Navigate to the Network Advisor installation directory.
     On Windows, navigate to <Network Advisor install directory>\jre64\lib\security
     On Linux, navigate to <Network Advisor install directory>/jre/lib/security
  b. Open the java.security file and change the jdk.certpath.disabledAlgorithms=MD2, RSA keySize < 1024 value from 1024 to 256.
     For example, jdk.certpath.disabledAlgorithms=MD2, RSA keySize < 256

Supported Hardware

Supported SAN Devices

The following table lists the versions of Brocade firmware supported in this release. Brocade recommends using the *latest* firmware versions in order to get the greatest benefit from the network and network management.

Fabric OS version	Switch or Director Type SAN Devices
FOS v8.0.1x, v8.0.2x, 8.1.0x	Brocade X6-4 Director[20]

Fabric OS version	Switch or Director Type SAN Devices
	Brocade X6-8 Director[20]
	Brocade G620 switch[17]
	Brocade G610 switch[22]
FOS v8.0.0	Brocade G620[17]
FOS v5.0.x, v5.1.x, v5.2.x, v5.3.x, v6.0.x. v6.1.x, v6.2.x, v6.3.x, v6.4.x, v7.0.x, v7.1.x, v7.2.x, v7.3.x, v7.4.x v8.0.1x, v8.0.2x, v8.1.0x	Brocade 3250
	Brocade 4100
	Brocade 7500[1]
	Brocade 200E
	Brocade 4900[2]
	Brocade 5000[3]
	Brocade AP7600[4]
	Brocade 300[5]
	Brocade 5100[5]
	Brocade 5300[5]
	Brocade 6505[13]
	Brocade 6510[12]
	Brocade 6520[14]
	Brocade 7840[15]
	Brocade 8000[9]
	Brocade 12000
	Brocade 7800[10]
	Brocade VA40-FC
	Brocade Encryption Switch[7]
	Brocade 48000 with FC4-16, FC4-32 and FC4-482 blades
	Brocade 48000 with FR4-18[1]
	Brocade 48000 with FC4-16[2]
	Brocade 48000 with FC10-6[4]
	Brocade 48000 with FA4-18
	Brocade DCX[6] with FC8-16, FC8-32,FA4-18, and FC8-48 blades
	Brocade DCX[6] with FR4-18i blades
	Brocade DCX with FC10-6 blades
	Brocade DCX[7] with FS8-18 blades
	Brocade DCX[10] with FCoE10-24 blades
	Brocade DCX[10] with FX8-24 blades
	Brocade DCX-4S[8] with FC8-16, FC8-32,FA4-18, FC8-48 and FC8-64 blades
	Brocade DCX[11] with FC8-64 blades

Fabric OS version	Switch or Director Type SAN Devices
	Brocade DCX-4S[8] with FR4-18i blades
	Brocade DCX-4S[8] with FC10-6 blades
	Brocade DCX-4S[8] with FS8-18 blades
	Brocade DCX-4S with FA4-18
	Brocade DCX-4S[10] with FCoE10-24 blades
	Brocade DCX-4S[10] with FX8-24 blades
	Brocade DCX-4S[11] with FC8-64 blades
	Brocade DCX 8510-4[12] and DCX 8510-8[12]
	Brocade DCX 8510-4[12] and DCX 8510-8[12] with FC16-32 , FC16-48 blades and FC8-64
	Brocade DCX 8510-4[13] and DCX 8510-8[13] with FC8-32e and FC8-48e blades
	Brocade DCX 8510-4[15] and DCX 8510-8[15] with FC16-64 blade
	Brocade Analytics Monitoring Platform[21]

Fabric OS version	Blade Type SAN Devices
FOS v5.2.x, v5.3.x, v6.0.x, v6.1.x, v6.2.x v6.3.x, v6.4.0, v7.0.x, v7.1.x, v7.2.x, v7.3.x	Brocade 3014
	Brocade 3016
	Brocade 4020
	Brocade 4016
	Brocade 4024[1]
	Brocade 4018
	Brocade 4012
	Brocade 4424
	Brocade 5410[2]
	Brocade 5450[2]
	Brocade 5460[2]
	Brocade 5424[2]
	Brocade 5470[2]
	Brocade 5480[2]
	Brocade M6505
	Brocade 6547
	Brocade 5430
	Brocade 5431
	Brocade 5432
	Brocade 6546
	Brocade 6548
	Brocade 6558[16]
	Brocade 6543[19]

	Brocade 6542[18]

Footnotes:
[1] Requires FOS v5.1.0 or later
[2] Requires FOS v5.2.0 or later
[3] Requires FOS v5.2.1 or later
[4] Requires FOS v5.3.0 or later
[5] Requires FOS v6.1.0 or later
[6] Requires FOS v6.0.0 or later
[7] Requires FOS v6.1.1_enc or later
[8] Requires FOS v6.2.0 or later
[9] Requires FOS v6.1.2_CEE or later
[10] Requires FOS v6.3.x or later
[11] Requires FOS v6.4.0 or later
[12] Requires FOS v7.0.0 or later
[13] Requires FOS v7.0.1 or later
[14] Requires FOS v7.1.0 or later
[15] Requires FOS v7.3.0 or later
[16] Requires FOS v7.3.0_cng or later
[17] Requires FOS v8.0.0 or later
[18] Requires FOS v7.4.0_ins or later
[19] Requires FOS v7.3.0_hur or later
[20] Requires FOS v8.0.1 or later
[21] The minimum recommended compatible version of AMP OS for sustained use is v2.0.0a. AMP OS v2.0.0 is the minimum supported version for compatibility with BNA 14.2.0. AMP OS v1.5.0 is only supported for temporary use to facilitate AMP migration to AMP OS v2.0.0 or later. Please refer to AMP OS Release Notes for additional migration and compatibility information.
[22] Requires FOS v8.1.0a or later

Supported NOS Devices

Network OS version	NOS Device Type
Network OS v7.0.0, v7.0.1, 7.1.0x	VDX 6940-144S, VDX 6740, 6740T, 8770, 6740T-1G, 6940-36Q, 2746, 2741
Network OS v6.0.1, v6.0.1x, v6.0.2, v6.0.2x	VDX 6940-144S, VDX 6740, 6740T, 8770, 6740T-1G, 2740, 6940-36Q
Network OS v6.0.0	VDX 6740, 6740T, 8770, 6740T-1G, 2740, 6940-36Q
Network OS v5.0.0, v5.0.1x	VDX 6740, 6740T, 8770, 6740T-1G, 2740
Network OS v5.0.1_tcn	VDX 2741
Network OS v4.0.1_hit1, v6.0.1 , v6.0.1x	VDX 2746
Network OS v3.0.0_dcb3, v3.0.0_dcb4, v4.1.2, v4.1.2a, v4.1.3, v4.1.3a, v4.1.3b	VDX 6746

Network OS version	NOS Device Type
Network OS v4.1.0, v4.1.1, v4.1.2, v4.1.3	VDX 6740, 6740T, 8770, 6710, 6720, 6730, 6740T-1G, 2740
Network OS v4.0.0 &v4.0.1	VDX 6740, 6740T, 8770, 6710, 6720, 6730
Network OS v3.0.0, v3.0.0a, v3.0.0b, v3.0.1, v3.0.1a	VDX 8770, 6710, 6720, 6730
Network OS v2.1P[1]P , v2.1.1, v2.1.1a, v2.1.1b, v2.1.2a	VDX 6710, 6720, 6730
Network OS v2.1.1_fuj, v3.0.0dcb5	VDX 2730

Supported IP Devices

FI/NI Versions	IP Device Type
8.0.60	FastIron ICX 7150
8.0.40, 8.0.40a, 8.0.50, 8.0.60	FastIron ICX 7450-32ZP, 7450, 7250, 7750
8.0.2x, 8.0.3x	FastIron ICX 7450, ICX 7750
8.0.1x	FastIron ICX 7750
2.7.02x, 2.7.03x, 2.8.x, 2.9.x	BigIron RX
7.1.x, 7.2.x	FastIron FGS, FGS-STK, FLS, FLS-STK, SuperX
7.1.x, 7.2.x, 7.3.x, 7.4.x	FESX, FWS
7.1.x, 7.2.x, 7.3.x, 7.4.x, 8.0.x	FastIron CX, FCX-STK
7.1.x, 7.2.x, 7.3.x, 7.4.x, 8.0.x	FastIron SX
8.0.xx	FastIron ICX 6610, 6450, 6430,
7.4.x, 8.0.x	FastIron ICX 6430, 6450
7.5x, 8.0.01x, 8.0.1x, 8.0.2x, 8.0.3x	Brocade 6650
5.0.x , 5.1.x, 5.2.x, 5.3.x, 5.4.x, 5.5x, 5.6.x, 5.7.x, 5.8.x, 5.9.x, 6.0.0, 6.1.0	NetIron CES, CER, MLX, XMR, MLXe
2.0.x, 2.1.x, 2.2.x	Brocade 6910
12.1. x[2], 12.2. x[2], 12.3.x, 12.4.x, 12.5.0x	ServerIron ADX
10.2.01x , 11.0.x	ServerIron
4.1.x, 4.2.x, 7.3.x, 7.4.x, 8.0.x, 8.0.01x	TurboIron 24X
4.1.x , 4.1.01x	FastIron FES

Footnotes:

[2]12.1.0f and 12.2.1 are not supported

Supported Wireless Devices

Wireless Controllers	Access Points	FW version

		ZoneFlex ZF7372	
Ruckus	SmartZone 100 Virtual SmartZone - Essentials (vSZ-E) Virtual SmartZone – High Scale (vSZ-H) SmartCell Gateway 200 (SCG200)	ZoneFlex ZF7982 ZoneFlex R300 ZoneFlex R310 ZoneFlex R700 ZoneFlex R710 ZoneFlex R720 ZoneFlex R500 ZoneFlex R600 ZoneFlex H500	3.5.0.0.808 3.5.0.0.1345 3.2.1.0.659 3.1.2.0.134
Aruba*	7010	AP124	6.4.1.0
	7210		6.4.2.2_46307
	7220	AP125	
	7240	AP224	
	3200XM	AP135	
	3400XM	AP225	
	3600XM	AP124	
Motorola	RFS 4000	AP7131	WiNG 5.4, 5.5
	RFS 6000	AP 7131N	
	RFS 7000	AP 5181	

* Aruba Instant Access Points are supported in Network Advisor.

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 BNA.

Adapter Types		Driver/Firmware versions
Brocade	Brocade 415,425,815,825	Driver/Firmware Versions: 1.1, 2.0, 2.1, 2.2, 3.0, 3.1, 3.2, 3.2.4 CIM Provider version: cpba3.2.3
	Brocade 804[1]	
	Brocade 1010,1020,1007[2]	
	Brocade 1741[3]	
	Brocade 1860[4]	
	Brocade 1867[5]	
	Brocade 1869[6]	

		Driver Versions: ESXi: 10.0.727.44 Windows: 10.0.720.0
Emulex	LPe12002-M8 8Gb 2-port PCIe Fibre Channel Adapter LPe16000 16Gb PCIe Fibre Channel Adapter LPe32002-M2 32Gb 2-port PCIe Fibre Channel Adapter	Firmware Versions: ESXi: 1.1.43.3 Windows: 1.1.43.3 CIM Provider Version: ESXi 5.1 and 5.5: 10.0.774.0 Boot Code and Firmware Version: 11.0.243.19 (LPe32002 only)
Qlogic	QLE2562-CK 8Gb, Dual Port, FC HBA, x4 PCIe 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 ×8 (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	Boot Code Version: 01.01.38 (multi-bot image with FCode for QLE269x/27xx Series Adapters) Driver Versions: Windows: 9.1.13.20 Firmware Versions: Windows: 8.00.00 CIM Provider Version: ESX-5.5.0-qlogic-cna-provider-1.5.7

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 Network Advisor

Installation instructions are provided for the following operating systems:
1. Microsoft Windows
2. Linux

Note: The 32 Bit installer is no longer supported for any edition of the Network Advisor.

The Network Advisor Server runs as multiple services on Windows and multiple processes on Linux. They all start automatically after the installation.

To install Network Advisor on Windows (Server)
1. Download and extract the zip archive.
2. Navigate to the Windows folder.
3. Execute *install.exe.*
4. Follow the instructions to complete the installation. For details refer to the *Installation and Migration Guide*.

To install Network Advisor on Linux (Server)
1. Download and extract the tar.gz archive
2. Navigate to the Linux_64 folder.
3. Execute *Install.bin* from the File Manager window.
4. Follow the instructions to complete the installation. For details refer to the *Installation and Migration Guide*.

To launch the Network Advisor Client

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

On Windows:
- Select Start > Programs > Network Advisor 14.2.x > Network Advisor 14.2.x.
- Click the Desktop icon.
- Launch command prompt, navigate to <Install Home>/bin, type dcmclient and press Enter.

On Linux:
- Click the Desktop icon.
- Launch terminal, navigate to "<Install Home>/bin, type sh dcmclient and press Enter.

To launch the Network Advisor Client from a remote host, complete the following steps.
Windows and Linux: Follow the below steps on launching the client from a web browser.

Note 1: The web start remote client is supported with JRE versions listed in 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

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

  https://NetworkAdvisorServerhost1.companyname.com/
  https://192.x.y.z/

  If the Network Advisor web server port number does not use the default (443 if is SSL Enabled; otherwise, the default is 80), you must enter the web server port number in addition to the IP address. For example, *IP_Address:Port_Number*. 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:
    - Click the **Web Start the Client** link.
      The Log In dialog box displays.

    - Click the **Download client bundle** (64-bit OS only) link.

To launch the Network Advisor Client from a web browser, complete the following steps.

5. Open a browser window and enter the Network Advisor IP address in the **Address** bar.
   For example:
   https://192.x.y.z/

   If the Network Advisor web server port number does not use the default (443 if is SSL Enabled; otherwise, the default is 80), you must enter the web server port number in addition to the IP address. For example, *IP_Address:Port_Number*. In the following examples, 8080 is the web server port number:
   https://192.x.y.z:8080/

   The web client login page displays with the server name and IP address in the upper left.

6. 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, please follow the below steps:

1. Launch "Java Control Panel" (refer to
http://java.com/en/download/help/win_controlpanel.xml to locate Java Control Panel
application on Windows)
2. In the Java Control Panel, click on the **Security** tab.
3. Select the **Enable Java content** check box in the browser. This will enable the Java plug-in in
the browser.
4. Click **Apply**. When the Windows User Account Control (UAC) dialog appears, allow
permissions to make the changes. Click **OK** in the Java Plug-in confirmation window.
5. Now launch Element Manager from Network Advisor Client.

Before Upgrading or Installing the Software

Before you install the application, make sure your system meets the minimum pre-installation
requirements. Refer to "Pre-installation requirements" in Installation and Migration Guide. If you are
migrating data, refer to "Data Migration" chapter.

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.

System Requirements for Network Advisor without AMP

Below table summarizes the memory, host, and disk space requirements for a remote client.

Memory, Host, and Disk space requirements for 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

Below table summarizes the minimum system requirements for server (plus 1 client) installation.

Minimum 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	10GB	20GB

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

Recommended system requirements for server (plus 1 client) installation

Resources	Small	Medium	Large
Installed Memory	16GB	16GB	16GB
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	20GB	80GB	100GB

NOTE
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 2GB for the client and 6GB 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 5 MB 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.

System Requirements for Network Advisor with Brocade Analytics Monitoring Platform

Here is the minimum system requirements for BNA to manage AMP devices.

Minimum System Requirements
- RAM Memory: 16 GB
- Processor: 6
- Disk Space: 40 GB

Note: Minimum system requirements is to validate the functionality with 1 or 2 AMP devices and 100 to 200 flows. Performance issues (slowness) and longevity issues shouldn't be reported with this system configuration.

Recommended System Requirements

Installation resources	20K Flows	40K Flows	60K Flows	80K Flows	100K Flows
Installed Memory	32 GB	32 GB	32 GB	64 GB	64 GB
Processor Core Count (physical + logical)	24 (12 physical + 12 logical)	24 (12 physical + 12 logical)	24 (12 physical + 12 logical)	48 (24 physical + 24 logical)	48 (24 physical + 24 logical)
Disk Space (including future migration)	4 TB	8 TB	12 TB	16 TB	20 TB
Server Heap	6 GB	6 GB	6 GB	6 GB	6 GB
Client Heap	2 GB	2 GB	2 GB	2 GB	2 GB

Recommended system configuration for remote java client with AMP

This is applicable for both – desktop client and browser based web client.

Resources	Small	Medium	Large
Installed Memory	4 GB	6 GB	6 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	10 GB	10 GB	10 GB

When BNA monitors 10 AMPs or 100000 flows, the system requirements for server (plus 1 desktop/web client) installation are:
- RAM Memory: 64 GB
- Processor: 48 core processor (24 physical and 24 virtual)
- Disk Space: 20 TB (Recommended: SSD)

When BNA monitors 10 AMPs or 100000 flows, the system requirements for the remote client (desktop or web client) are:
- RAM Memory: 6 GB
- Processor: 8 core processor (4 physical and 4 virtual)
- Disk Space: 1 GB

NOTE
> 1. It is recommended to use only the remote client for the Brocade Network Advisor server when managing Brocade Analytics Monitoring Platform with more than 20K flows
> 2. SSD storage is strongly recommended for better performance when managing Brocade Analytics Monitoring Platform. Future releases of Brocade Network Advisor when supporting Brocade Analytics Monitoring Platform will require the use of SSD and the storage space requirements may increase due to additional capabilities.

3. When managing Brocade Analytics Monitoring Platform, it is recommended to use a server with a minimum of two Processors/CPUs, 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 Brocade Analytics Monitoring Platform, the Brocade 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 (14.0.0, 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 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 to 14.2.x release.

Note 9: Cleanup the monitor entries in BNA 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
    - SAN Analytics Monitoring: Top Flows
    - 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.

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 BNA home location and restart the server for changes to take effect.

Brocade Network Advisor downgrade to previous versions is not supported.

Configuration Considerations

Supported scalability limits by Network Advisor edition

	Enterprise Edition			Professional Plus Edition + IP Base 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
IP Switches*	50	200	1550 (Supported) 1200 (recommended) (with performance monitoring on up to 20000 ports)	50	50
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

*The IP switch count includes MPLS and VDX switches.

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

Limitations and Restrictions

Qlogic branded Brocade adapters are not supported for discovery.

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

1. **Backup and restore recommendations**

   a) With AMP discovered in Network Advisor, 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 BNA installation directory and the backup process takes about 1.5 hours for 100GB of data.

   b) By default, the Network Advisor server backup is scheduled for every day - a backup every 24hrs. With AMP discovered in the Network Advisor, since the data size will be huge,
      i. If user needs better BNA 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 BNA will be impacted due to the backup process. Based on the need, the backup can be planned.
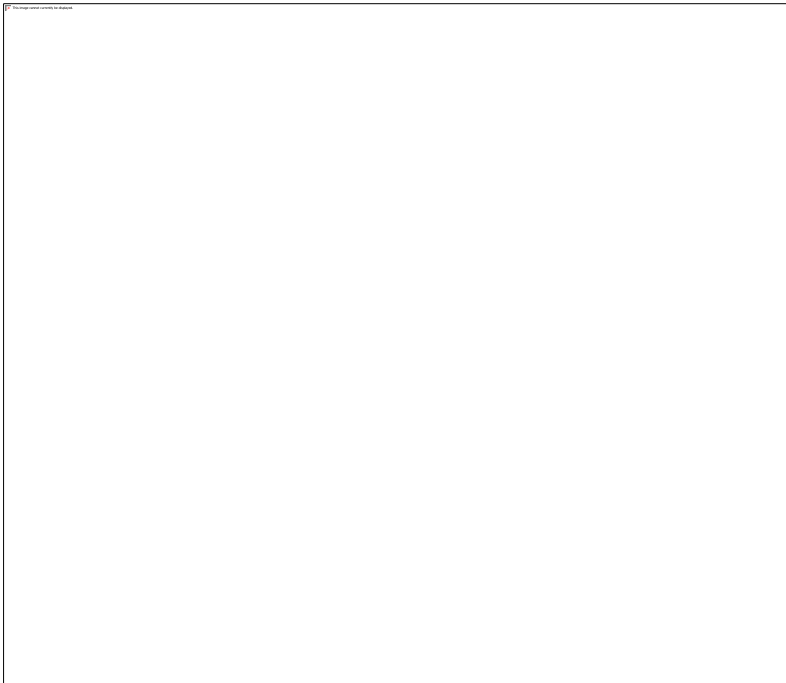
c) While migrating Network Advisor from pre-14.2.1 version to 14.2.1 or later, it may take longer time for the Source monitor DB services to stop. As a result an error is being shown in "Resource validation and data migration" screen: "Migration Failed. Network Advisor will roll back to the previous version".
When the issue happens, please do the following:
- i. Rollback to the source version
- ii. Open Server Management Console (SMC) and stop all the services.
- iii. Then install the destination version and do the migration

2. **Support save recommendations**
   a) With AMP discovered in Network Advisor, 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.
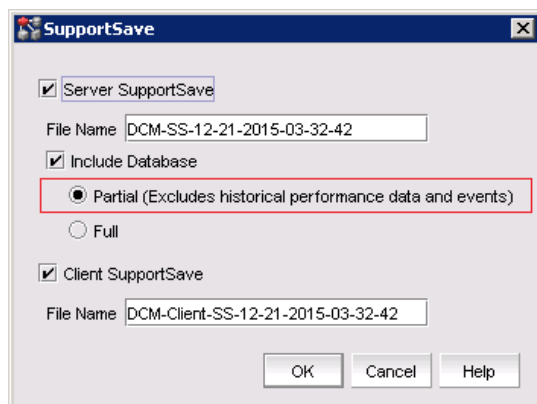
3. **Disk space recommendation in case of Migration**
   a) It is recommended to have free disk space of 3 times the size of "BNA installation folder/data". Note that it would take approximately 2 hours to complete the migration for 100G of data folder size.
   Example:
   Size of the "BNA installation 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.

4. **Performance considerations for Dashboard**
   a) When there are more than 30k flows monitored in BNA
   - 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.

5. **An AMP device should be discovered by only one BNA 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 Trial or Licensed version SAN + IP Professional Plus Licensed version SAN + IP Enterprise Licensed version
SAN Professional Plus Licensed Version	SAN Enterprise Licensed version SAN + IP Professional Plus Licensed version SAN + IP Enterprise Licensed version
SAN Enterprise Trial	SAN Enterprise Licensed version SAN + IP Enterprise Trial or Licensed version
SAN Enterprise Licensed version	SAN + IP Enterprise Licensed version

IP Upgrade Paths

Current software release	To software release
IP Professional	IP Base Trial or Licensed version SAN + IP Professional Plus Licensed version SAN + IP Enterprise Licensed version
IP Base Trial	IP Base Licensed version SAN + IP Professional Plus Licensed version SAN + IP Enterprise Licensed version
IP Base Licensed version (lower count)	IP Base Licensed version (higher count) SAN + IP Enterprise Licensed version

SAN+IP Upgrade Paths

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

NOTE:

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 + IP	Professional Plus SAN + IP
	Professional Plus SAN
Enterprise SAN	Professional Plus SAN + IP
	Professional Plus SAN

Package downgrade paths

Current software release	To software release
Enterprise SAN + IP	Enterprise SAN Enterprise IP Professional Plus SAN
Professional Plus SAN + IP	Enterprise SAN Enterprise IP Professional Plus SAN
Professional SAN + IP	Enterprise SAN Enterprise IP Professional Plus SAN

MPLS Downgrade Paths

Current software release	To software release
Enterprise SAN + IP with MPLS	Enterprise SAN + IP with fewer MPLS Enterprise SAN + IP without MPLS Enterprise IP with MPLS Enterprise IP without MPLS Professional Plus SAN + IP without MPLS Professional Plus SAN + IP with fewer MPLS
Enterprise IP with MPLS	Enterprise SAN + IP with fewer MPLS Enterprise SAN + IP without MPLS Enterprise IP with fewer MPLS Enterprise IP without MPLS Professional Plus SAN + IP without MPLS Professional Plus SAN + IP with fewer MPLS
Professional Plus SAN + IP with MPLS	Enterprise SAN + IP with fewer MPLS Enterprise SAN + IP without MPLS Enterprise IP with MPLS Enterprise IP without MPLS Professional Plus SAN + IP without MPLS Professional Plus SAN + IP with fewer MPLS

IP Product count downgrade paths

Current software release	To software release
Enterprise SAN with SMI Agent + IP	Enterprise SAN + IP with fewer products Professional Plus SAN + IP with fewer products Enterprise IP with fewer products
Enterprise IP	Enterprise IP with fewer products
Professional Plus SAN with SMI Agent + IP	Professional Plus SAN + IP with fewer products Enterprise IP with fewer products

User Guides

List of Documents

You can download the software and documentation from the MyBrocade website.

- Brocade Network Advisor Installation and Migration Guide
- Brocade Network Advisor SAN User Manual
- Brocade Network Advisor SAN User Manual (AMP)
- Brocade Network Advisor SAN + IP User Manual
- Brocade Network Advisor SAN + IP User Manual (AMP)
- Brocade Network Advisor IP User Manual
- Brocade Network Advisor Software Licensing Guide
- Brocade Network Advisor Port Commissioning Quick Start Guide
- Brocade Network Advisor REST API Guide
- Brocade Network Advisor SMI Agent Developer's Guide
- Virtual Connect Enterprise Manager Server Guide
- Brocade Analytics Monitoring Platform User Guide

Refer to www.brocade.com or http://my.brocade.com for latest versions of the documents.

Reporting Errors in the Guides
Send an email to documentation@brocade.com to report errors in the user guides.

Known Documentation Errors
- Network Advisor user manuals do not contain the updated OSS-TPS information.
  For OSS-TPS information refer to OSCD page http://www.brocade.com/en/support/support-tools/oscd.html

- In the Network Advisor SAN_AMP_IP User Manual 14.2.1 (Part Number: 53-1004934-02), SAN_AMP User Manual (Part Number: 53-1004935-02):
  - Firmware requirements section should read:

    "After migration from 14.0.x/14.1.x, you must enable the Monitor service for monitoring the Brocade Analytics Monitoring Platform".

  - Upgrade and Migration considerations section should show the following table:

Release	Version
Network Advisor 14.0.x	14.0.1, 14.0.2,14.0.3
Network Advisor 14.1.x	14.1.0, 14.1.1

Network Advisor 14.2.x	14.2.0

- o Following NOTEs should read:

    "Direct migration from pre-14.0.x releases to 14.2.x is not supported. Refer to Supported migration paths in the Installation Guide for migration paths from DCFM, INM and pre-14.0.x releases."

    "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 version 14.2.x for SAN+IP network management with the procurement of the SAN functionality"

    "Network migration is not supported from 14.0.x releases to the 14.2.x release."

- o Following NOTE should be removed from SAN_AMP_Manual and in SAN_IP_AMP_Manual: "If pre 14.1 version having AMP firmware 1.4 / 1.5, upgrade the AMP to 2.0 after migrated to 14.1 and before enabling the AMP services. Historic data for AMP flows from pre-14.1 will not be migrated to 14.1.x after migration."

- In the Network Advisor Installation and Migration Guide, 14.2.x (Part Number: 53-1004882-02), add the following details.
  1. In the section "Linux swap space requirements", change "Greater than 4 GB and less than 8 GB" to "Greater than 6 GB and less than 8 GB".
- In the Network Advisor SAN Installation and Migration Guide, 14.2.x (Part Number: GC27-6622-03), add the following details.
  - In the section "Linux swap space requirements", change "Greater than 4 GB and less than 8 GB" to "Greater than 6 GB and less than 8 GB".
- In the Network Advisor IP User Manual 14.2.1 (Part Number: 53-1004881-02)
  - o Following contents should be removed under
    - ➢ Zoning Chapter:
      - Zoning Best Practices
      - From Zone database size section,
        - o The supported maximum zone database size is 1 MB for fabric with minimum one pizza box and 2MB for director-only fabrics.
        - o If the fabric contains only Backbone Chassis platforms, the supported maximum zone database size is 2 MB.

    - ➢ Fabric Insight Portal Chapter:
      - Under viewing port properties section, replace screenshot with IP Port Properties dialog box, currently it shows FC port properties dialog box.

Contacting Brocade Support

Contact your Network Advisor provider for software support. To expedite your call, have the following information immediately available:

- Technical Support contract number, if applicable
- Network Advisor edition
- Network Advisor version
- Detailed description of the problem, including the supportsave data, screen shots of the problem if applicable
- Description of any troubleshooting steps already performed and the results

To contact Brocade, go to http://www.brocade.com/services-support/index.page for the latest e-mail and telephone contact information.

Defects

Open defects in Network Advisor 14.2.1

This section lists the open defects with Critical, High and Medium Technical Severity as of May 12 2017 in Network Advisor 14.2.1

Defect ID:	DEFECT000590799		
Technical Severity:	High	Probability:	Medium
Product:	Brocade Network Advisor	Technology Group:	Device Monitoring
Reported In Release:	Network Advisor14.0.1	Technology:	Flow Vision (SAN)
Symptom:	VE Port is shown as unknown in the port picker dialog		
Condition:	Right click the ge-port in topology and launch "Add Flow" dialog. The port picker dialog displays VE-port as unknown.		

Defect ID:	DEFECT000595077		
Technical Severity:	High	Probability:	Low
Product:	Brocade Network Advisor	Technology Group:	Fault Management
Reported In Release:	Network Advisor14.0.1	Technology:	Events
Symptom:	In the Network Advisor Master Log the "Link up on port unknown " message is shown for Brocade X6-8 Director.		
Condition:	Brocade X6-8 Director is being managed by the Network Advisor; IO is running. Issue is observed after enabling VF and creating new FID on Brocade X6-8 Director.		

Defect ID:	DEFECT000621147		
Technical Severity:	High	Probability:	Medium
Product:	Brocade Network Advisor	Technology Group:	Management
Reported In Release:	Network Advisor14.2.0	Technology:	Configuration Fundamentals
Symptom:	Zoning dialog will take more than 5 min to get launched		
Condition:	When user launches zoning dialog in Network Advisor which has both SAN and IP enabled		

Defect ID:	DEFECT000626055		
Technical Severity: High		**Probability:** Low	
Product: Brocade Network Advisor		**Technology Group:** Device Monitoring	
Reported In Release: Network Advisor14.2.0		**Technology:** MAPS - Monitoring and Alerting Policy Suite	
Symptom: F-Port will only get fenced instead of port decommission			
Condition: When the MAPS threshold is exceeded for the MAPS rule which is configured for the port decommission and fenced action and the password is not configured for CIMOM server			

Defect ID:	DEFECT000626807		
Technical Severity: High		**Probability:** Medium	
Product: Brocade Network Advisor		**Technology Group:** Monitoring	
Reported In Release: Network Advisor14.2.0		**Technology:** Hardware Monitoring	
Symptom: On clicking "Stop" button to abort multiple D-port test, the 'Stopped' status is not updated for few ports.			
Condition: When user performs the diagnostic port test on multiple ports (E and F-Ports) and aborts the test by clicking on "Stop" button.			

Defect ID:	DEFECT000627655		
Technical Severity: High		**Probability:** Low	
Product: Brocade Network Advisor		**Technology Group:** Device Monitoring	
Reported In Release: Network Advisor14.2.0		**Technology:** MAPS - Monitoring and Alerting Policy Suite	
Symptom: FICON host is not notified when a port statistics threshold is exceeded on a F-Port, but no subsequent notification is sent for the fenced port by Network Advisor			
Condition: When FMS enabled and MAPS is running with the FENCE action enabled and port is fenced by Network Advisor			

Defect ID:	DEFECT000628583		
Technical Severity: High		**Probability:** Medium	
Product: Brocade Network Advisor		**Technology Group:** Management	
Reported In Release: Network Advisor14.2.0		**Technology:** Configuration Fundamentals	
Symptom: Although Zone names cannot begin with a numeric character or a special character. the Network Advisor documentation incorrectly reads this: Please include the below sentence : (Zone names, Zone configuration names, and Alias name can begin with an alpha numeric character and can have one or more special characters " _ " , "-", "$", "^".)			
Condition: Issue exists in the SAN AMP and SAN+IP AMP user guides.			

Defect ID:	DEFECT000628794		
Technical Severity: High		**Probability:** Low	
Product: Brocade Network Advisor		**Technology Group:** Management	
Reported In Release: Network Advisor14.0.2		**Technology:** Configuration Fundamentals	
Symptom: After upgrading the Network Advisor v14.0.2 the user defined FTP password has been reset to the default one.			
Condition: Observed after the Network Advisor upgrade to v14.0.2.			
Recovery: Manually set the FTP password after completing the Network Advisor upgrade.			

Defect ID:	DEFECT000629334		
Technical Severity: Medium		**Probability:** Medium	
Product: Brocade Network Advisor		**Technology Group:** Monitoring	
Reported In Release: Network Advisor12.4.3		**Technology:** Hardware Monitoring	
Symptom: CLI command portstatsshow reports a non-zero value for er_rx_c3_timeout attribute.			
Condition: The issue is seen when querying the CIM class Brocade_SwitchFCPortStats.			

Defect ID:	DEFECT000630200		
Technical Severity: High		**Probability:** Low	
Product: Brocade Network Advisor		**Technology Group:** Device Management	
Reported In Release: Network Advisor14.2.1		**Technology:** Firmware Management	
Symptom: Network Advisor does not display any warning message when downgrading the switches with the user-defined MAPS rules.			
Condition: Observed when firmware downgrade to pre-v8.1.0 FOS version is performed on the switches with the user-defined MAPS rules.			

Defect ID:	DEFECT000630634		
Technical Severity: High		**Probability:** Medium	
Product: Brocade Network Advisor		**Technology Group:** Monitoring	
Reported In Release: Network Advisor14.2.1		**Technology:** Hardware Monitoring	
Symptom: Don't have option to change bar chart to line chart and line chart to bar chart for system defined templates.			
Condition: By default disabled for all the user operations. That's the reason user not able to change chart type			
Workaround: Use has option to change from system defined template to user defined template.			

Defect ID:	DEFECT000632198		
Technical Severity: High		**Probability:** High	
Product: Brocade Network Advisor		**Technology Group:** Client	
Reported In Release: Network Advisor14.2.1		**Technology:** Active Sessions	
Symptom: The Collection IO Exception widget shows average count instead of total count			
Condition: This issue will be seen for the Dual vTap flows			

Defect ID:	DEFECT000632432		
Technical Severity: High		**Probability:** High	
Product: Brocade Network Advisor		**Technology Group:** Device Monitoring	
Reported In Release: Network Advisor14.2.1		**Technology:** Fabric Tracking (SAN)	
Symptom: Intermittently Network Advisor does not update ISL links in Topology.			
Condition: Observed when the Track Fabric Changes option was turned off.			
Workaround: Close and re-launch the Network Advisor client.			

Defect ID:	DEFECT000633128		
Technical Severity: High		**Probability:** Low	
Product: Brocade Network Advisor		**Technology Group:** Management	
Reported In Release: Network Advisor14.0.1		**Technology:** Configuration Fundamentals	
Symptom: STP is disabled when trying to deploy VLAN to the ports.			
Condition: STP is disabled when user tries to deploy the port VLANs			

Defect ID:	DEFECT000633726		
Technical Severity:	Medium	**Probability:**	Low
Product:	Brocade Network Advisor	**Technology Group:**	Device Monitoring
Reported In Release:	Network Advisor14.2.0	**Technology:**	MAPS - Monitoring and Alerting Policy Suite
Symptom:	In MAPS dialog, user is not able to give negative value for SFT_TEMP		
Condition:	In BNA 14.2 for all the MAPS policies(custom policies) the user will not be able to set the negative values for SFP_TEMP measure. This issue will be seen consistently irrespective of the FOS version.		

Defect ID:	DEFECT000633912		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Management
Reported In Release:	Network Advisor14.2.0	**Technology:**	Configuration Fundamentals
Symptom:	User is not able to view default MAPS policies		
Condition:	After upgrading to Network Advisor 14.2, user will not be able to see the default MAPS policies.		

Defect ID:	DEFECT000634564		
Technical Severity:	Medium	**Probability:**	High
Product:	Brocade Network Advisor	**Technology Group:**	Device Management
Reported In Release:	Network Advisor14.2.1	**Technology:**	Device configuration (SAN)
Symptom:	BR-6547 device in AG mode is being shown as a switch in the Network Advisor.		
Condition:	Issue is observed when viewing device properties in the Network Advisor.		

Defect ID:	DEFECT000634955		
Technical Severity:	High	**Probability:**	High
Product:	Brocade Network Advisor	**Technology Group:**	Management
Reported In Release:	Network Advisor14.2.1	**Technology:**	Configuration Fundamentals
Symptom:	The message "This action cannot be performed on the selected Tunnel, because the default logical switch has not been discovered or monitored" is displayed when the user tries to edit the FCIP Tunnel parameters even with the default switch is discovered in BNA.		
Condition:	Tunnels are created in non-default logical switches and no GE ports are acquired for the default logical switch as device details collection is in progress		

Defect ID:	DEFECT000635519		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Device Management
Reported In Release:	Network Advisor14.2.1	**Technology:**	Device configuration (General)
Symptom:	Intermittently, one out of 10 times, one of the switch which is FICON capable but HIF disabled and becomes unusable while creating logical switches		
Condition:	When user try to create multiple FICON Logical Switches from Network Advisor		

Defect ID:	DEFECT000635890		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Management
Reported In Release:	Network Advisor14.2.1	**Technology:**	Configuration Fundamentals
Symptom:	Firmware Management dialog does not list the imported firmware version in the Download tab.		
Condition:	After importing FOS v8.1.1 into Network Advisor Firmware Repository the version is not being listed in Firmware to Download column's combo box in Download tab.		
Workaround:	Close and reopen the Firmware Management dialog.		

Defect ID:	DEFECT000636122		
Technical Severity: High		**Probability:** Medium	
Product: Brocade Network Advisor		**Technology Group:** Management	
Reported In Release: Network Advisor14.2.1		**Technology:** Configuration Fundamentals	
Symptom: The configuration of IPSec-Policy fails			
Condition: Configuration name which is trying to create is already available for the peer switch of the tunnel			
Workaround: Use another ipsec-policy name for the switch which is not available in the peer switch			

Defect ID:	DEFECT000636967		
Technical Severity: Medium		**Probability:** Medium	
Product: Brocade Network Advisor		**Technology Group:** Device Management	
Reported In Release: Network Advisor14.2.0		**Technology:** Discovery	
Symptom: Few of the properties like port count, SNMP contact will be empty in device proprieties dialog			
Condition: This will be seen in all the Network OS devices			

Defect ID:	DEFECT000637432		
Technical Severity: High		**Probability:** High	
Product: Brocade Network Advisor		**Technology Group:** Device Management	
Reported In Release: Network Advisor14.2.1		**Technology:** Topology Views	
Symptom: Network Advisor does not update ports of the VCS cluster's principal node.			
Condition: When a backed up configuration is being restored on the VCS cluster that has up to 15 nodes.			

Defect ID:	DEFECT000637760		
Technical Severity: High		**Probability:** High	
Product: Brocade Network Advisor		**Technology Group:** Device Management	
Reported In Release: Network Advisor14.2.1		**Technology:** Device configuration (IP)	
Symptom: "Access points" tab is not shown in the controller properties sheet.			
Condition: When the firmware is being upgraded on the controller.			

Defect ID:	DEFECT000637762		
Technical Severity: High		**Probability:** High	
Product: Brocade Network Advisor		**Technology Group:** Monitoring	
Reported In Release: Network Advisor14.2.1		**Technology:** Hardware Monitoring	
Symptom: AP Report shows some APs are bound to vSZ-H controller when they are actually bound to SZ100 controller.			
Condition: When user generates the AP report via Network Advisor.			

Defect ID:	DEFECT000637892		
Technical Severity: Medium		**Probability:** Low	
Product: Brocade Network Advisor		**Technology Group:** Device Monitoring	
Reported In Release: Network Advisor14.0.1		**Technology:** Reports	
Symptom: The links between ICX7250 and ICX7450 devices are not displayed in the layer 2 topology map in the Network Advisor.			
Condition: The issue observed on ICX7250 and ICX7450 switches with FI v8.0.60.			
Workaround: Enable LLDP and disable FDP and CDP on both the switches.			

Defect ID:	DEFECT000638588		
Technical Severity:	High	**Probability:**	Medium
Product: Brocade Network Advisor		**Technology Group:** Device Monitoring	
Reported In Release: Network Advisor14.2.1		**Technology:** Performance	
Symptom: Virtual Fabric Deployment fails with reason "No response from the switch"			
Condition: When user changes the default Logical Switch FID from 128 to any other number, creates multiple Logical Switches with assigned ports and then applies logical fabric settings to all associated logical switches			

Defect ID:	DEFECT000640549		
Technical Severity:	High	**Probability:**	Medium
Product: Brocade Network Advisor		**Technology Group:** Device Management	
Reported In Release: Network Advisor14.2.1		**Technology:** Configuration File Management	
Symptom: The Logical Switch Change Confirmation and Status dialog is not being launched when click OK on the Logical Switches dialog box.			
Condition: Issue observed after performing multiple operations with the Logical Switches (create, delete, edit).			

Defect ID:	DEFECT000640775		
Technical Severity:	High	**Probability:**	Medium
Product: Brocade Network Advisor		**Technology Group:** Device Management	
Reported In Release: Network Advisor14.2.1		**Technology:** Firmware Management	
Symptom: Firmware download on ICX 7150 switch via Network Advisor fails with 'End of File' error.			
Condition: When SCP option is being selected in Server > Options dialog for the product communication.			
Recovery: Use CLI or FTP to download the image			

Defect ID:	DEFECT000641581		
Technical Severity:	High	**Probability:**	Medium
Product: Brocade Network Advisor		**Technology Group:** Management	
Reported In Release: Network Advisor14.2.1		**Technology:** Configuration Fundamentals	
Symptom: Firmware download, initiated from the Network Advisor on multiple switches, did not complete for all the selected switches.			
Condition: After the firmware download failed on one of the switches the process did not continue for the rest of the selected switches.			

Defects Closed with Code Change in Network Advisor 14.2.1

This section lists the defects with Critical, High and Medium Technical Severity closed with a code change as of May 12, 2017 in Network Advisor 14.2.1.

Defect ID:	DEFECT000594125		
Technical Severity:	High	**Probability:**	Medium
Product: Brocade Network Advisor		**Technology Group:** Fault Management	
Reported In Release: Network Advisor14.0.1		**Technology:** Troubleshooting	
Symptom: User is unable to perform Diagnostic Port Test on ICL and QSFP ports. Observe that electrical & optical loop-back test is skipped with reason as "No SFP or Chip support".			
Condition: Launch Diagnostic Port dialog and select 16G ICL/32 ICL/32 QSFP ports and start the test.			

Defect ID:	DEFECT000597027	
Technical Severity: High	Probability: Low	
Product: Brocade Network Advisor	Technology Group: Device Monitoring	
Reported In Release: Network Advisor14.0.1	Technology: Flow Vision (SAN)	
Symptom: Unable to see the sub flows for a selected flow definition		
Condition: Create a flow which has source / destination as * and specify the LUN ID. Select the flows from the left hand panel in flow vision dialog to right hand panel.		

Defect ID:	DEFECT000598070	
Technical Severity: High	Probability: Medium	
Product: Brocade Network Advisor	Technology Group: Device Management	
Reported In Release: Network Advisor14.0.1	Technology: Topology Views	
Symptom: Additional port info displays shows status of E-Ports for F-Ports		
Condition: This happens intermittently when we do blade level decommission or recommission operation		

Defect ID:	DEFECT000602409	
Technical Severity: High	Probability: Low	
Product: Brocade Network Advisor	Technology Group: Fault Management	
Reported In Release: Network Advisor14.0.2	Technology: Events	
Symptom: Master log event description is blank for one of the Management Server Events.		
Condition: In Network Advisor, the Master log shows a blank Description for one of the Management Server Events for v8.0.1a fabrics with running traffic.		

Defect ID:	DEFECT000619324	
Technical Severity: Medium	Probability: Low	
Product: Brocade Network Advisor	Technology Group: Monitoring	
Reported In Release: Network Advisor14.0.1	Technology: Hardware Monitoring	
Symptom: Real time graph do not plot the values for the discovered switches		
Condition: Real time Graph does not plot after un-managing the Host that was used as initiator/target during flow creation.		
Recovery: Rediscover the fabric and try again.		

Defect ID:	DEFECT000622869	
Technical Severity: High	Probability: Low	
Product: Brocade Network Advisor	Technology Group: Management	
Reported In Release: Network Advisor14.2.0	Technology: Configuration Fundamentals	
Symptom: Network Advisor FCIP Tunnel dialog will popup error stating that Default Switch not Managed		
Condition: When a pair of SW7840 is locked in a IPEX tunnel and resides in the logical fabric and has GiGE ports in the respective SW7840 Default Partitions.		

Defect ID:	DEFECT000625762	
Technical Severity: Medium	Probability: Medium	
Product: Brocade Network Advisor	Technology Group: Device Management	
Reported In Release: Network Advisor12.0.1	Technology: Firmware Management	
Symptom: Firmware download to NetIron XMR-MLX switch from a Network Advisor fails.		
Condition: Issue is observed in Network Advisor running on Linux platform.		

Defect ID:	DEFECT000627097		
Technical Severity: High		**Probability:** Low	
Product: Brocade Network Advisor		**Technology Group:** Device Monitoring	
Reported In Release: Network Advisor14.2.0		**Technology:** MAPS - Monitoring and Alerting Policy Suite	
Symptom: User will get maximum 500 rules reached message even though the maximum limit of rules is not reached			
Condition: When user try to create 500 rules each for two different user defined policies			

Defect ID:	DEFECT000627115		
Technical Severity: High		**Probability:** Low	
Product: Brocade Network Advisor		**Technology Group:** Management	
Reported In Release: Network Advisor14.2.0		**Technology:** Configuration Fundamentals	
Symptom: The trap which is sent after the MAPS quite time expiry will not have the correct violation count.			
Condition: This issue will be seen for all the MAPS rules configured with SNMP trap action and quite time.			

Defect ID:	DEFECT000627270		
Technical Severity: High		**Probability:** High	
Product: Brocade Network Advisor		**Technology Group:** Fault Management	
Reported In Release: Network Advisor14.2.0		**Technology:** Events	
Symptom: For Brocade X6-4 director switch the Master Log shows an event with the blank description.			
Condition: When user configures MAPS event for Brocade X6-4 chassis and the SNMP event is being triggered, the Network Advisor Master log shows the event with the blank description.			

Defect ID:	DEFECT000628028		
Technical Severity: High		**Probability:** Low	
Product: Brocade Network Advisor		**Technology Group:** Device Management	
Reported In Release: Network Advisor14.2.0		**Technology:** Device configuration (SAN)	
Symptom: For pizza box devices the addressing mode will be displayed as disabled			
Condition: When user tries to create FICON LS for the pizza box devices			

Defect ID:	DEFECT000628481		
Technical Severity: High		**Probability:** Low	
Product: Brocade Network Advisor		**Technology Group:** Device Monitoring	
Reported In Release: Network Advisor14.2.0		**Technology:** Reports	
Symptom: CLI "Collection Aggregated Time Series Report" report generation fails with "Database Connection Failed!" error, even though the Mater log shows and entry for successful authentication.			
Condition: If Network Advisor server bound to specific IP Address, the report generation would fail.			
Workaround: The workaround is to bind BNA server to "All" (Host name). The server Bind address can be configured through Options dialog or by re launching configuration wizard.			

Defect ID:	DEFECT000629079		
Technical Severity: High		**Probability:** Low	
Product: Brocade Network Advisor		**Technology Group:** Client	
Reported In Release: Network Advisor14.2.0		**Technology:** Installation & Migration	
Symptom: Unable to proceed with the Network Advisor installation with a selected preferred IP Address. The "port 22 is occupied" error message is shown in port configuration page.			
Condition: Issue observed in a dual NIC server with both NICs configured with IP addresses, when scp/ftp server is running with Ethernet address 1 as a preferred IP address. In this case, even though the ports associated with other Ethernet IP address are free, the error message is shown.			

Defect ID:	DEFECT000630506	
Technical Severity: High	Probability: Low	
Product: Brocade Network Advisor	Technology Group: Device Management	
Reported In Release: Network Advisor14.2.1	Technology: Device configuration (General)	
Symptom: User is not able to see the violations details in MAPS dialog.		
Condition: When any rule for Port Category gets violated.		

Defect ID:	DEFECT000631944	
Technical Severity: High	Probability: High	
Product: Brocade Network Advisor	Technology Group: Monitoring	
Reported In Release: Network Advisor14.2.1	Technology: Hardware Monitoring	
Symptom: The D-port test fails and GENERIC, BAD_EOF, BAD_OS, RX_C3_TIMEOUT, TX_C3_TIMEOUT errors are shown in the report.		
Condition: When user runs the D_Port test on 32 Gb QSFP ports.		

Defect ID:	DEFECT000634686	
Technical Severity: High	Probability: Low	
Product: Brocade Network Advisor	Technology Group: Partner Integration	
Reported In Release: Network Advisor14.0.1	Technology: RESTful API	
Symptom: The Internal Server Error is returned as a response for REST API (500 error).		
Condition: When user queries the enddeviceconnections REST API URI: /rest/resourcegroups/All/fcfabrics/<fabric key>/enddeviceconnections		

Defect ID:	DEFECT000635870	
Technical Severity: Medium	Probability: Low	
Product: Brocade Network Advisor	Technology Group: Device Management	
Reported In Release: Network Advisor14.2.0	Technology: Device configuration (SAN)	
Symptom: The MAPS dialog will be empty		
Condition: This issue is seen for all the switches having the Fabric OS version as 7.3.x		

Defect ID:	DEFECT000635998	
Technical Severity: High	Probability: High	
Product: Brocade Network Advisor	Technology Group: Monitoring	
Reported In Release: Network Advisor14.2.0	Technology: Hardware Monitoring	
Symptom: The Server Backup initiated from Network Advisor failed with error message "Previous backup failed".		
Condition: When user takes Server Backup for the third time (after two successful attempts) in Network Advisor when AMP is enabled.		
Workaround: Delete the existing backups manually and trigger a new backup.		

Defect ID:	DEFECT000636810	
Technical Severity: Medium	Probability: Medium	
Product: Brocade Network Advisor	Technology Group: Device Monitoring	
Reported In Release: Network Advisor14.0.2	Technology: Policy Monitor	
Symptom: The SFP dialog is empty		
Condition: If user launches SFP data for any switch which has "Power ON Years" value greater than one		

Defect ID:	DEFECT000638312	
Technical Severity: High	Probability: High	
Product: Brocade Network Advisor	Technology Group: Device Monitoring	
Reported In Release: Network Advisor14.2.0	Technology: Performance	
Symptom: Network Advisor performance degrades over time, becoming unresponsive and possible crashing.		

Condition:	When the switch is AMP enabled and user monitors from Network Advisor.

Defect ID:	DEFECT000638652		
Technical Severity:	Medium	Probability:	Medium
Product:	Brocade Network Advisor	Technology Group:	Fault Management
Reported In Release:	Network Advisor14.2.0	Technology:	Events
Symptom:	Network Advisor fails to send Summary emails at the specified summary intervals, although E-mail event notifications are enabled.		
Condition:	When E-mail event notifications are being configured via Users dialog.		

Defect ID:	DEFECT000639221		
Technical Severity:	Medium	Probability:	High
Product:	Brocade Network Advisor	Technology Group:	Device Monitoring
Reported In Release:	Network Advisor14.2.0	Technology:	Performance
Symptom:	Threshold is not triggered for the historical data collection.		
Condition:	Issue observed for the Ping stats collector (IP) threshold.		

Defects Closed without Code Change in Network Advisor 14.2.1

This section lists the defects with Critical, High and Medium Technical Severity closed without a code change as of May 12, 2017 in Network Advisor 14.2.1.

Defect ID:	DEFECT000559622	Technical Severity:	High
Reason Code:	Not Reproducible	Probability:	Low
Product:	Brocade Network Advisor	Technology Group:	Management
Reported In Release:	Network Advisor12.4.1	Technology:	Configuration Fundamentals
Symptom:	Although the firmware download was successful, the error message "Active and Standby CPs failed to gain HA synchronization within 10 minutes" was shown in Network Advisor.		
Condition:	Intermittently observed only on director class switches.		

Defect ID:	DEFECT000628897	Technical Severity:	High
Reason Code:	Not Reproducible	Probability:	Low
Product:	Brocade Network Advisor	Technology Group:	Management
Reported In Release:	Network Advisor14.2.0	Technology:	Configuration Fundamentals
Symptom:	In the partition management status dialog - delete logical switch failed Reason: No response from switch(Found) will be shown as status		
Condition:	When user tries to delete LS in the partition management dialog from Network Advisor		
Workaround:	Workaround would be to delete individual Logical Partitions.		
Recovery:	No recovery was needed because the deletion operation was actually successful.		

Defect ID:	DEFECT000628985	Technical Severity:	High
Reason Code:	Not Reproducible	Probability:	Low
Product:	Brocade Network Advisor	Technology Group:	Device Management
Reported In Release:	Network Advisor14.2.0	Technology:	Device configuration (General)
Symptom:	In the partition management status dialog - create logical switch failed Reason: VF is not manageable even server sleeps for 20 seconds on core switch		
Condition:	When user tries to create eight LS and without moving the ports in the partition management dialog from 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 BNA 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 BNA

- 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 Brocade 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 Brocade 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 Brocade Analytics Monitoring Platform
- HTTP TRACK/TRACE methods are not blocked in BNA 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 for this issue: 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:\/"*.

- 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 BNA 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 Brocade 7840 may fail due to GE port sharing or if the associated VE port exists in another LS

Important IP Notes

Miscellaneous Important Notes that Apply to IP Installations

1. For large networks the Adaptive polling turned off by default for all IP devices (even for migrated servers).

2. SNMP write credentials will not be populated by default for NI/FI/NOS devices.

3. Each IP product has a System max value that can be configured for various parameters, such as "ip-filter-sys" for ACLs. Network Advisor deployments do not check whether the payload being sent to the device has a number greater than the system-max value. In such deployment scenarios, the deployment may report success even though the number was limited to the system-max value. To ensure successful deployments, make sure the payload being sent is no greater than System max value.

4. Syslog messages will not be received for the VDX 8770 that is configured with different IP addresses for CPs.

5. Pizza Box switches running Network OS 4.0 are displayed with 'Product Type' as 'Router' in Network Advisor, even when they do not have Layer 3 license.

6. When two ports of the same storage are connected to two VDX devices, only one of the attached ports is displayed in the Zoning dialog.

7. On VDX devices managed through in band IP address in Network Advisor, firmware download, product support save and configuration backup operations fail.

8. Fabric Watch violation can be viewed under following path Fabric Vision-->MAPS-->Violations.

9. Firmware upgrade in NetIron devices using simplified image doesn't update the boot image from NI 5.6 and above. Boot image need to deploy separately.

10. Discovery of a cluster running Network OS 6.0 and above requires addition of SNMP user settings from CLI as default user support is not available.

11. Configuration backup on MLX running 5.8.00a code using SCP fails with 'Bad client version string [Unknown cause]'. Work around is to use the TFTP, SCP then TFTP and TFTP then SCP. The issue is not seen in NI 6.0 and later.

12. In IP Address and Detailed Reports IP Management Ports will not be consistent with the CLI port naming conventions. This is caused by SNMP index and port name inconsistencies. In some cases, Management ports will not be displayed in the reports.

13. L2 topology does not show link between Ruckus Wireless Controllers and connected L2 switches as Ruckus Wireless Controllers don't support LLDP.

14. BNA would not rediscover the controller managing Access Points if there is a change detected in the MAC Address of one or more Access Points. The controller has to be deleted first, and then discovered to see the Access Points with the new MAC Address.

15. To use SSL Certificates for ServerIron products, contact your customer support representative

16. The Identifier column in the Ethernet Ports table of a detailed report shows incorrect identifier details for Control Bridge's second slot ports.

17. The Control Bridge ports of a Campus Fabric do not show role as 'SPX PORT' in device properties port tab if Campus Fabric has more than 2 Port Extenders.

Boot, Monitor, Firmware Image Updates

1. Network Advisor does not support boot and firmware upgrade and downgrade for ADX devices running 12.1 or above.

2. Firmware Download to NetIron CES devices fails via SCP with the error message "There is not enough space on MP flash". Below are the considerations before downloading the image to NI CES device.
   1) If device flash size is 32 MB, it will support either primary or secondary flash. If image is already present in primary flash and needs to download for secondary flash and vice-versa, then we should manually delete the primary and secondary flash respectively by using the command "delete primary or delete secondary" and download will be happen as expected.
   2) If it is 64 MB, it will support for both primary and secondary flash and the download will be happen successfully.
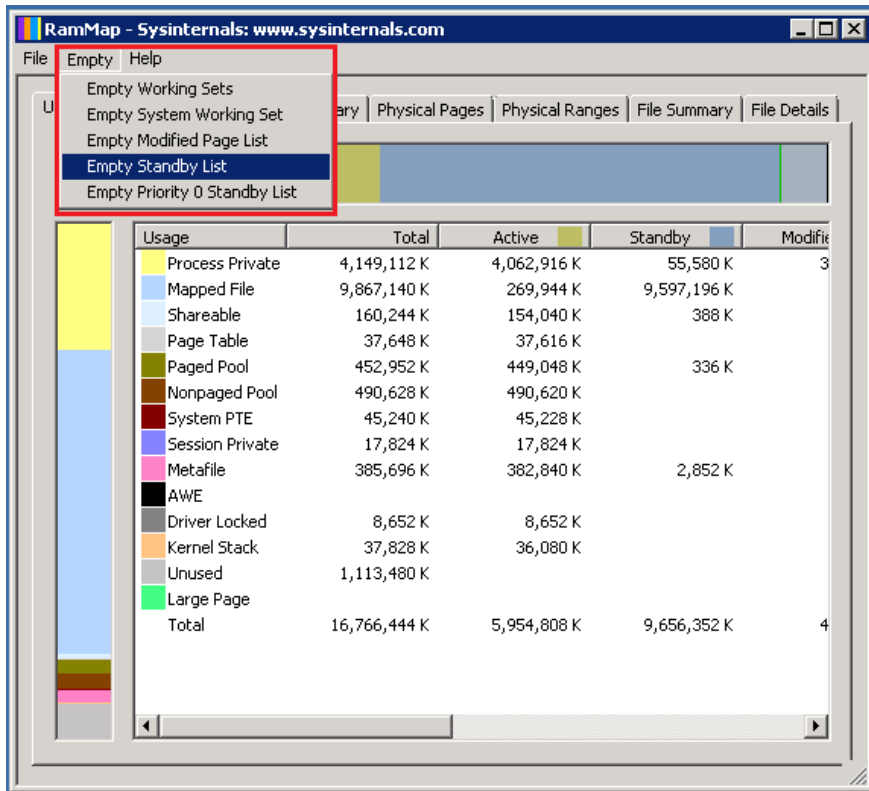
Important Notes common for SAN and IP

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: 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 BNA 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. Intermittently HTTP 500 error message is displayed when launching the Web Client. Server restart will fix the issue.

10. User needs to run the "sanperformancestatenable" script from BNA 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 <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*

11. REST API does not provide FCIP circuit measures for the GigE port.

12. BNA is now enforcing minimum disk space requirements during migration. When the disk space requirements are not met, BNA display a message prompting the user to use the script to delete performance data and retry migration.

13. 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.

14. When Network Advisor is managing more than 1500 IP products, user might experience some performance degradations such as delays while launching some dialogs.

15. 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

16. 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.

17. 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.

18. 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.

19. 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

20. 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.

21. 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".

22. 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.

23. During migration, BNA uninstallation process requires 1 GB of physical RAM. Sometimes Windows OS do not clear the released memory and keeping it in standby Memory. Use Microsoft tool like "RAM MAP" to clean up the unused RAM from standby list
    - Download RAMMap.zip file from URL - https://technet.microsoft.com/en-us/sysinternals/rammap.aspx
    - Extract the zip file and run the runmap.exe
    - Click empty menu > Empty Standby List

Usage	Total	Active	Standby	Modifie
Process Private	4,149,112 K	4,062,916 K	55,580 K	3
Mapped File	9,867,140 K	269,944 K	9,597,196 K	
Shareable	160,244 K	154,040 K	388 K	
Page Table	37,648 K	37,616 K		
Paged Pool	452,952 K	449,048 K	336 K	
Nonpaged Pool	490,628 K	490,620 K		
System PTE	45,240 K	45,228 K		
Session Private	17,824 K	17,824 K		
Metafile	385,696 K	382,840 K	2,852 K	
AWE				
Driver Locked	8,652 K	8,652 K		
Kernel Stack	37,828 K	36,080 K		
Unused	1,113,480 K			
Large Page				
Total	16,766,444 K	5,954,808 K	9,656,352 K	4

Domestic and International Modem based Call Home is no longer supported

Alternatively, customers using Domestic or International Call Home Modem feature can reconfigure their Call Home to utilize the Brocade Email option for continued Call Home notifications in the event of a system problem. Please refer to the Call Home section of the Brocade 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 Brocade 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 BNA (14.2.1) from OEM1 version to OEM2 version
    a. Partially uninstall the source BNA 14.2.1 OEM1 version
    b. Now install BNA 14.2.1 OEM2 version
    c. In the 'copy data and settings' page, browse to the BNA 14.2.1 OEM1 version and continue with the migration.

Migrating BNA (pre-14.2.1) OEM1 version to BNA 14.2.1 OEM2 version
    d. Install the source BNA pre-14.2.1 OEM1 version
    e. Now install BNA 14.2.1 OEM2 version
    f. In the 'copy data and settings' page, browse to the BNA pre-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, v7.6
HP VCEM version	v7.4.1, v7.6

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 valueP1P / (1000 * 1000)) / (Polling intervalP2P)
RX	FC	MP	.1.3.6.1.3.94.4.5.1.7	RX = (Delta valueP1P / (1000 * 1000)) / (Polling intervalP2P)
TX	G	SP	.1.3.6.1.2.1.31.1.1.1.10	TX = (Delta valueP1P / (1000 * 1000)) / (Polling intervalP2P)
RX	GE	SNMP	.1.3.6.1.2.1.31.1.1.1.6	RX = (Delta valueP1P / (1000 * 1000)) / (Polling intervalP2P)
TX	FCIP	SNMP	.1.3.6.1.2.1.31.1.1.1.10	TX = (Delta valueP1P / (1000 * 1000)) / (Polling intervalP2P)
RX	FCIP	SNMP	.1.3.6.1.2.1.31.1.1.1.6	RX = (Delta valueP1P / (1000 * 1000)) / (Polling intervalP2P)
Uncompressed Tx/Rx MB/sec	FCIP	SNMP	.1.3.6.1.4.1.1588.4.1.1.6	(Delta valueP1P / (1000 * 1000)) / (Polling intervalP2P)
TX	EE Monitors	HTTP	PortRX (variable from the return html file)	TX = (Delta valueP1P / (1000 * 1000)) / (Polling intervalP2P)
RX	EE Monitors	HTTP	PortTX (variable from the return html file)	RX = (Delta valueP1P / (1000 * 1000)) / (Polling intervalP2P)
TX	HBA, CNA	HCM API	NA	TX = (Delta valueP1P / (1000 * 1000)) / (Polling intervalP2P)
RX	HBA, CNA	HCM API	NA	RX = (Delta valueP1P / (1000 * 1000)) / (Polling intervalP2P)
TX	TE	SNMP	1.3.6.1.2.1.31.1.1.1.10	TX = (Delta valueP1P / (1000 * 1000)) / (Polling intervalP2P)
RX	TE	SNMP	.1.3.6.1.2.1.31.1.1.1.6	RX = (Delta valueP1P / (1000 * 1000)) / (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 value1 of TX or RX) / ((Bytes

				transmitted * port speed)*(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 value1 of TX or RX) /((125000000* port speed)*(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 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 valueP1P / (1000 * 1000)
Other Counters				Other counters = Delta valueP1P
Current Compression Ratio	FCIP	NA	NA	(ifHCInOctets + ifHCOutOctets) / fcipExtendedLinkCompressedBytes .

1. Delta valueP[1]P: is the difference of value retrieved between the two consecutive poling cycles.
2. Polling intervalP[2] P: 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 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 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:

<u>Od heap size:</u>

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

<u>Curent Heap Size:</u>

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
   c. 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
   c. 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:

2. Launch the Server Management Console from the Start menu.

3. Click Start to start the SLP service.

4. Open a command window.

5. Type cd c:\Management_Application\cimom \bin and press Enter to change to the directory where slpd.bat is located.

6. Type > slptool findsrvs service:service-agent and press Enter to verify the SLP service is running as a Service Agent.

7. Type > slptool findsrvs service:wbem and press Enter to verify the SLP service is advertising its WBEM services.

8. Choose one of the following options to verify the SLP service is advertising the WBEM SLP template over its configured client protocol adapters.

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

2. 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.