Network Advisor 14.4.2 Release Notes

Contents of this file:

HPE B-series Network Advisor Enterprise, Professional Plus, and Professional 14.4.2 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 NA software and Release Notes:

- *Go to* http://www.hpe.com.
- Select **Support** from the drop-down menu in the top right corner of the home page.
- Under Product Support, click **HPE Support Center.**
- Enter your B-series switch (i.e. SN6600B) into the search box, and you will be presented with a list of models associated with this switch. Click on the link for your model.
- Click **Drivers & Software.**
- Select "HPE SAN Network Advisor **Application Version: v14.4.2"**
- To read Release Notes, click on the **Release Notes** link

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.

April 23, 2018

Brocade Network Advisor 14.4.2

Release Notes v1.1

Contents

Document history

Version	Summary of changes	Publication date
1.0	Initial Release for Network Advisor 14.4.2	04/18/2018
1.1	Updated publication fields for defects	04/23/2018

Preface

Contacting Brocade Technical Support

As a Brocade customer, you can contact Brocade Technical Support 24x7 online or by telephone. Brocade OEM customers should contact their OEM/solution provider.

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

Brocade customers

For product support information and the latest information on contacting the Technical Assistance Center, go to . http://www2.brocade.com/en/support/contact-brocade-support.html.

If you have purchased Brocade product support directly from Brocade, use one of the following methods to contact the Brocade Technical Assistance Center 24x7.

Online	Telephone
Preferred method of contact for non-urgent issues: • My Cases through MyBrocade • Software downloads and licensing tools • Knowledge Base	Required for Sev 1-Critical and Sev 2-High issues: • North America: 1-800-752-8061 (Toll-free) • International: 1-408-333-6061 (Not toll-free) • Toll-free numbers are available in many countries and are listed on the http://www2.brocade.com/en/support/contact-brocade-support.html page.

Brocade OEM customers

If you have purchased Brocade product support from a Brocade OEM/solution provider, contact your OEM/solution provider for all of your product support needs.

- OEM/solution providers are trained and certified by Brocade to support Brocade® products.
- Brocade provides backline support for issues that cannot be resolved by the OEM/solution provider.
- Brocade Supplemental Support augments your existing OEM support contract, providing direct access to Brocade expertise. For more information, contact Brocade or your OEM.

- For questions regarding service levels and response times, contact your OEM/solution provider.

Related documentation

Visit the Broadcom website to locate related documentation for your product and additional Brocade resources.

White papers, data sheets, and the most recent versions of Brocade software and hardware manuals are available at https://www.broadcom.com/products/fibre-channel-networking/.

Product documentation for all supported releases is available to registered users at MyBrocade. Click the Support tab and select Document Library to access documentation on MyBrocade. You can locate documentation by product or by operating system.

Release notes are bundled with software downloads on MyBrocade. Links to software downloads are available on the MyBrocade landing page and in the Document Library.

Document feedback

Quality is our first concern at Brocade, and we have made every effort to ensure the accuracy and completeness of this document.

However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. You can send your feedback to documentation.pdl@broadcom.com.

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

Overview

Brocade Network Advisor 14.4.2 is a software maintenance release based on Brocade Network Advisor 14.4.1. All hardware platforms and features supported in Brocade Network Advisor 14.4.1 are also supported in Brocade Network Advisor 14.4.2.
The fixes included in this release are listed in the defect tables below in this document.

Build 39 is the GA build for Brocade Network Advisor 14.4.2.

Software Features

New software features – Network Advisor 14.4.2

The following software features are new in this release.

- REST Interface Changes (RDP and syslog/snmp trap forwarding)
- Defect fixes

New software features – Network Advisor 14.4.1

The following software features are new in this release.

- Fabric OS platform support
  - Fabric OS 8.2.0
  - Brocade G630 switch
  - FC32-64 blade for Brocade X6 Director
- FCOE support for FC32-64 blade
  - Show the FCoE attributes for Ethernet ports
  - Indicate the Ethernet/FC ports
  - Performance support for FCoE devices
- NVMe support for Brocade X6 Directors and G630
  - NVMe devices discovery
  - NVME Flow Vision
    - Add Flow Definition Dialog shows NSID radio button
    - Flow Vision dialog enhanced to include NSID column
    - NSID column in Top N Flows/Bottom N Flows dashboard widget
  - Performance Management Enhancements to support measures for NVMe
  - NVMe support for MAPS
- Zoning Enhancements
  - Alias support for Target Driven Peer Zones
  - Zone Configuration Dialog
  - Hide peer zone property member
  - Dummy TDZ support
  - Zoning support for FCoE devices
- MAPS Enhancements

    - Ethernet Port group and Optic monitoring for FCoE port
    - MAPS Email enhancements
    - MAPS support to Monitor Number of IP Extension Flows
    - MAPS – Category name changes from “FCIP Health” to “Extension Health”
    - MAPS – Category name changes from “GigE Port” to “Extension GE Port Health” Category
- Miscellaneous BNA Enhancements
    - Default value of Product communication for SAN switches changed to “HTTPS then HTTP”
    - Custom RASLOG Events are added in the call home event filter
    - Firmware File download using MFT GET
        - Manage File Transfer – GET REST API (To Retrieve File)
        - Manage File Transfer - GET REST API (To Download Firmware File)
    - Discovery - AG as a seed switch
    - Email Event Notification
    - Special Instruction and switch name in call home
    - Parallel FC/IPEX HCL Support on Brocade X6 Directors
    - New Operating System Support – Windows Server 2016
- REST API Enhancements
    - Port Speed update operation
    - RDP Metrics Support
    - REST API support Peer Zone creation
    - Peer Zone Modification
    - REST API Support for Configuring TDZ Status in FC Port
    - Rest API Support for Retrieving TDZ Status for FC Port
    - Rest API Support for Renaming Alias
- Analytics Monitoring Platform Features
    - AMP OS 2.2.0
    - Multipath IO (MPIO) Support
        - Show Multiple paths to a LUN identified by the Logical Unit WWN
        - Show Logical Unit WWN details in Network Flow and Investigation mode
        - Collection of flows by the Logical Unit WWN for an application centric view
    - IT/ITL resource limits and ITL limits per IT
    - RFEs
        - Supporting FID level collection deployment
        - Lifting the 80 flows per collection limit
        - Top oversubscribed IT flows widget
        - Aggregated Violations Details in FIP Dashboard

Modified software features

Changes to Network Advisor licenses / packages:

- Network Advisor 14.4 does not support a fresh installation of SAN+IP package. However, if a SAN+IP package is already installed on a pre-14.4, then that version of the Network Advisor can be successfully upgraded to 14.4.

- The Network Advisor 14.4 neither supports a fresh installation of IP only package, nor migration from pre-14.4 releases of IP only package.

Security Vulnerability Fixes

This section lists the Common Vulnerabilities and Exposures (CVEs) fixes that are added in Network Advisor v14.4.2.

- CVE-2018-2579: An unspecified vulnerability in Oracle Java SE related to the Java SE, Java SE Embedded, JRockit Libraries component could allow an unauthenticated attacker to obtain sensitive information resulting in a low confidentiality impact using unknown attack vectors

- CVE-2018-2588: An unspecified vulnerability in Oracle Java SE related to the Java SE, Java SE Embedded, JRockit LDAP component could allow an authenticated attacker to obtain sensitive information resulting in a low confidentiality impact using unknown attack vectors.
- CVE-2018-2663: An unspecified vulnerability in Oracle Java SE related to the Java SE, Java SE Embedded, JRockit Libraries component could allow an unauthenticated attacker to cause a denial of service resulting in a low availability impact using unknown attack vectors.

- CVE-2018-2677: An unspecified vulnerability in Oracle Java SE related to the Java SE, Java SE Embedded AWT component could allow an unauthenticated attacker to cause a denial of service resulting in a low availability impact using unknown attack vectors.

- CVE-2018-2678: An unspecified vulnerability in Oracle Java SE related to the Java SE, Java SE Embedded, JRockit JNDI component could allow an unauthenticated attacker to cause a denial of service resulting in a low availability impact using unknown attack vector

- CVE-2018-2602: An unspecified vulnerability in Oracle Java SE related to the Java SE, Java SE Embedded I18n component could allow an unauthenticated attacker to cause low confidentiality impact, low integrity impact, and low availability impact.

- CVE-2018-2599: An unspecified vulnerability in Oracle Java SE related to the Java SE, Java SE Embedded, JRockit JNDI component could allow an unauthenticated attacker to cause no confidentiality impact, low integrity impact, and low availability impact.

- CVE-2018-2603: An unspecified vulnerability in Oracle Java SE related to the Java SE, Java SE Embedded, JRockit Libraries component could allow an unauthenticated attacker to cause a denial of service resulting in a low availability impact using unknown attack vectors.

- CVE-2018-2629: An unspecified vulnerability in Oracle Java SE related to the Java SE, Java SE Embedded, JRockit JGSS component could allow an unauthenticated attacker to cause no confidentiality impact, high integrity impact, and no availability impact

- CVE-2018-2657: **:** An unspecified vulnerability in Oracle Java SE related to the Java SE, JRockit Serialization component could allow an unauthenticated attacker to cause a denial of service resulting in a low availability impact using unknown attack vectors.
  CVSS Base Score: 5.3.

- CVE-2018-2618: An unspecified vulnerability in Oracle Java SE related to the Java SE, Java SE Embedded, JRockit JCE component could allow an unauthenticated attacker to obtain sensitive information resulting in a high confidentiality impact using unknown attack vectors.

- CVE-2018-2641: An unspecified vulnerability in Oracle Java SE related to the Java SE, Java SE Embedded AWT component could allow an unauthenticated attacker to cause no confidentiality impact, high integrity impact, and no availability impact.

- CVE-2018-2582: An unspecified vulnerability in Oracle Java SE related to the Java SE, Java SE Embedded Hotspot component could allow an unauthenticated attacker to cause no confidentiality impact, high integrity impact, and no availability impact.

- CVE-2018-2634: An unspecified vulnerability in Oracle Java SE related to the Java SE, Java SE Embedded JGSS component could allow an unauthenticated attacker to obtain sensitive information resulting in a high confidentiality impact using unknown attack vectors.
  CVSS Base Score: 6.8.

- CVE-2018-2637: An unspecified vulnerability in Oracle Java SE related to the Java SE, Java SE Embedded, JRockit JMX component could allow an unauthenticated attacker to cause high confidentiality impact, high integrity impact, and no availability impact.

- CVE-2018-2633: An unspecified vulnerability in Oracle Java SE related to the Java SE, Java SE Embedded, JRockit JNDI component could allow an unauthenticated attacker to take control of the system.

- CVE-2018-2638: An unspecified vulnerability in Oracle Java SE related to the Java SE Deployment component could allow an unauthenticated attacker to take control of the system.

- CVE-2018-2639: An unspecified vulnerability in Oracle Java SE related to the Java SE Deployment component could allow an unauthenticated attacker to take control of the system.

- JRE upgrade to 1.8u162 [Java vulnerability issues listed in the Oracle security advisory: http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html#AppendixJAVA]

New hardware

The following section lists new hardware introduced with Network Advisor 14.4 release.

New devices

Product name	Device name
Brocade G630	Gen 6 (32 Gbps) Fibre Channel 128-port fixed port switch

New blades

Blade	Description	Compatible devices
Brocade FC32-64 Port Blade	64 port Gen 6 (32 Gbps) Fibre Channel or 10Gb/25Gb/40Gb FCoE blade	Brocade X6 Director

RFCs and standards

This software conforms to the Fibre Channel standards in a manner consistent with accepted engineering practices and procedures. In certain cases, Brocade might add proprietary supplemental functions to those specified in the standards. For a list of FC standards conformance, visit the following Brocade Web site: http://www.brocade.com/sanstandards.

Supported OS, Browsers, JRE

Supported Operating Systems

- Windows Server 2016 Datacenter, Standard
- 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 57 and later (Windows only)
- Chrome 62 and later (Windows, MAC OS)

Supported JRE versions

Network Advisor version	JRE version supported
14.4.2	JRE 1.8u162

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
- Fabric OS v8.1.1
- Fabric OS v8.2.0x

- 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 < 2048 value from 2048 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:
    c. 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
    d. Open the java.security file and change the jdk.certpath.disabledAlgorithms=MD2, RSA keySize < 2048 value from 2048 to 256.
    For example, jdk.certpath.disabledAlgorithms=MD2, RSA keySize < 256

Hardware support

Supported devices

NOTE

For IP Product information please refer to Brocade Network Advisor SAN+IP User Manual

Supported SAN Devices

The following firmware platforms are supported by this release of the Network Advisor:

- Fabric OS 6.0 or later
- Fabric OS 7.0 or later
- Fabric OS 8.0 or later
- Fabric OS 8.1 or later
- Fabric OS 8.2 or later

NOTE
Discovery of a secure Fabric OS fabric in strict mode is not supported.
NOTE
To ensure that a configuration is fully supported, always check the appropriate SAN, storage or blade server product support page to verify support of specific code levels on specific switch platforms prior to installing on your switch. Use only Fabric OS versions that are supported by the provider.
The hardware platforms in the following table are supported by this release of the Network Advisor.
NOTE
The recommended compatible version of AMP OS is v2.2.0 for BNA 14.4. AMP OS v2.1.0 is the minimum supported version for compatibility with BNA 14.4 and is intended only for temporary use until upgrading to AMP OS v2.2.0.

Device name	Terminology used in documentation
Brocade 300 Switch	24-port, 8-Gbps FC switch
Brocade 4012 Switch	Embedded 12-port, 4- Gbps FC switch
Brocade 4016 Switch	Embedded 16-port, 4-Gbps FC switch
Brocade 4018 Switch	Embedded 18-port, 4-Gbps FC switch
Brocade 4020 Switch	Embedded 20-port, 4-Gbps FC switch
Brocade 4024 Switch	Embedded 24-port, 4-Gbps FC switch
Brocade 5100 Switch	40-port, 8-Gbps FC switch
Brocade 5300 Switch	80-port, 8-Gbps FC switch
Brocade 5410 Embedded Switch	Embedded 12-port, 8-Gbps switch
Brocade 5424 Embedded Switch	Embedded 24-port, 8-Gbps switch
Brocade 5431 Embedded Switch	Embedded 16-port, 8-Gbps stackable switch
Brocade 5450 Embedded Switch	Embedded 16-port, 8-Gbps switch
Brocade 5460 Embedded Switch	Embedded 24-port, 8-Gbps switch
Brocade 5470 Embedded Switch	Embedded 24-port, 8-Gbps switch
Brocade 5480 Embedded Switch	Embedded 24-port, 8-Gbps switch
Brocade 6505 Switch	24-port, 16-Gbps edge switch
Brocade M6505 blade server SAN I/O module	24-port, 16-Gbps blade server SAN I/O module
Brocade 6510 Switch	48-port, 16-Gbps switch
Brocade 6520 Switch	96-port, 16-Gbps switch
Brocade 6542 blade server SAN I/O module	48-port, 16-Gbps blade server SAN I/O module
Brocade 6543 blade server SAN I/O module	24-port, 16-Gbps blade server SAN I/O module
Brocade 6545 blade server SAN I/O module	26-port, 16-Gbps blade server SAN I/O module
Brocade 6546 blade server SAN I/O module	24-port, 16-Gbps blade server SAN I/O module
Brocade 6547 blade server SAN I/O moduleh	48-port, 16-Gbps blade server SAN I/O module
Brocade 6548 blade server SAN I/O module	28-port, 16-Gbps blade server SAN I/O module
Brocade 7800 Switch	8-Gbps extension switch
Brocade 7840 Switch	16-Gbps 24-FC port, 18-GbE port switch
Brocade 8000 Switch	8-Gbps 8-FC port, 10-GbE 24-DCB port switch

Brocade 8470 FCoE Embedded Switch	FCoE embedded switch
Brocade VA-40FC Switch	8-Gbps 40-port switch
Brocade Encryption Switch	8-Gbps encryption switch
Brocade Gen 6 platform (32-Gbps) fixed-port switch (Brocade G610)	24-port, 32-Gbps switch
Brocade Gen 6 platform (32-Gbps) fixed-port switch (Brocade G620)	64-port, 32-Gbps switch
Brocade Gen 6 platform (32-Gbps) fixed-port switch (Brocade G630)	128-port, 32-Gbps switch
Brocade DCX Professional and Professional Plus (Trial and Licensed) versions can discover, but not manage this device. This device cannot be used as a Seed switch.	8-slot backbone chassis
Brocade DCX with FC8-16, FC8-32, and FC8-48 Blades Professional and Professional Plus (Trial and Licensed) versions can discover, but not manage this device. This device cannot be used as a Seed switch.	8-slot backbone chassis with 8-Gbps 16-FC port, 8-Gbps 32-FC port, and 8-Gbps 48-FC port blades
Brocade DCX with FC8-64 Blades Professional and Professional Plus (Trial and Licensed) versions can discover, but not manage this device. This device cannot be used as a Seed switch.	8-slot backbone chassis with 8-Gbps 64-FC port blades
Brocade DCX with FC10-6 Blades Professional and Professional Plus (Trial and Licensed) versions can discover, but not manage this device. This device cannot be used as a Seed switch.	8-slot backbone chassis with FC 10 - 6 ISL blade
Brocade DCX with FS8-18 Blades Professional and Professional Plus (Trial and Licensed) versions can discover, but not manage this device. This device cannot be used as a Seed switch.	8-slot backbone chassis with encryption blade
Brocade DCX with FX8-24 Blades Professional and Professional Plus (Trial and Licensed) versions can discover, but not manage this device. This device cannot be used as a Seed switch.	8-slot backbone chassis with 8-Gbps 12-FC port, 10-GbE ports, 2-10 GbE ports blade
Brocade DCX with FCoE10-24 Blades Professional and Professional Plus (Trial and Licensed) versions can discover, but not manage this device. This device cannot be used as a Seed switch.	8-slot backbone chassis with 10-Gbps 24-port FCoE blade
Brocade DCX-4S	4-slot backbone chassis
Brocade DCX-4S with FC8-16, FC8-32, and FC8-48 Blades	4-slot backbone chassis with 8-Gbps 16-FC port, 8-Gbps 32-FC port, and 8-Gbps 48-FC port blades
Brocade DCX-4S with FC8-64 Blades	4-slot backbone chassis with 8-Gbps 64-FC port blades
Brocade DCX-4S with FC10-6 Blades	4-slot backbone chassis with FC 10 - 6 ISL blade

Brocade DCX-4S with FS8-18 Blades	4-slot backbone chassis with encryption blade
Brocade DCX-4S with FX8-24 Blades	4-slot backbone chassis with 8-Gbps 12-FC port, 10-GbE ports, 2-10 GbE ports blade
Brocade DCX-4S with FCoE10-24 Blades	4-slot backbone chassis with 10-Gbps 24-port FCoE blade
Brocade DCX 8510-4	16-Gbps 4-slot backbone chassis
Brocade DCX 8510-4 with FS8-18 Encryption Blades	16-Gbps 4-slot backbone chassis with encryption blades
Brocade DCX 8510-4 with FC8-64 and FX8-24 Blades	16-Gbps 4-slot backbone chassis with 8-Gbps 64-port and 8-Gbps router extension blades
Brocade DCX 8510-4 with FC16-32 and FC16-48 Blades	16-Gbps 4-slot backbone chassis with 16-Gbps 32-port and 16-Gbps 48-port blades
Brocade DCX 8510-4 with FC8-32E and FC8-48E Blades	16-Gbps 4-slot backbone chassis with 8-Gbps 32-port and 8-Gbps 48-port blades
Brocade DCX 8510-4 with FC16-64 Blades	16-Gbps 4-slot backbone chassis with 16-Gbps 64-port blades
Brocade DCX 8510-8 Professional and Professional Plus (Trial and Licensed) versions can discover, but not manage this device. This device cannot be used as a Seed switch.	16-Gbps 8-slot backbone chassis
Brocade DCX 8510-8 with FS8-18 Encryption Blades Professional and Professional Plus (Trial and Licensed) versions can discover, but not manage this device. This device cannot be used as a Seed switch.	16-Gbps 8-slot backbone chassis with encryption blades
Brocade DCX 8510-8 with FC8-64 and FX8-24 Blades Professional and Professional Plus (Trial and Licensed) versions can discover, but not manage this device. This device cannot be used as a Seed switch.	16-Gbps 8-slot backbone chassis with 8-Gbps 64-port and 8-Gbps router extension blades
Brocade DCX 8510-8 with FC16-32 and FC16-48 Blades Professional and Professional Plus (Trial and Licensed) versions can discover, but not manage this device. This device cannot be used as a Seed switch.	16-Gbps 8-slot backbone chassis with 16-Gbps 32-port and 16-Gbps 48-port blades
Brocade DCX-8510-8 with FCoE10-24 Blades Professional and Professional Plus (Trial and Licensed) versions can discover, but not manage this device. This device cannot be used as a Seed switch.	16-Gbps 8-slot backbone chassis with 10-Gbps 24-port FCoE blade
Brocade DCX 8510-8 Professional and Professional Plus (Trial and Licensed) versions can discover, but not manage this device. This device cannot be used as a Seed switch.	16-Gbps 8-slot backbone chassis with 16-Gbps 64-port blades
Brocade X6-4 Director	32-Gbps, 4-slot backbone chassis

Brocade X6-8 Director Professional and Professional Plus (Trial and Licensed) versions can discover, but not manage this device. This device cannot be used as a Seed switch.	32-Gbps, 8-slot backbone chassis
FA4-18 Application Platform Blade	Application platform blade
FC8-16 Blade	FC 8-GB 16-port blade
FC8-32 Blade	FC 8-GB 32-port blade
FC8-32E Blade Only supported on the DCX 8510-4 and DCX 8510-8 chassis.	FC 8-GB 32-port blade
FC8-48 Blade	FC 8-GB 48-port blade
FC8-48E Blade Only supported on the DCX 8510-4 and DCX 8510-8 chassis.	FC 8-GB 48-port blade
FC8-64 Blade	FC 8-GB 64-port blade
FC10-6 Blade	FC 10 - 6 ISL blade
FC16-32 Blade	16-Gbps 32-port blade
FC16-48 Blade	16-Gbps 48-port blade
FC16-64 Blade	16-Gbps 64-port blade
FC32-64 Blade	32-Gbps 64-port blade
FCoE10-24 Blade Only supported on the DCX, DCX-4S, and DCX 8510-8 chassis.	10-Gbps FCoE Port router blade
FS8-18 Encryption Blade	Encryption blade
FX8-24 Blade	8-Gbps extension blade
FC32-48 Port Blade	32-Gbps 48-port blade
SX6 Extension Blade	32-Gbps, router extension blade

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]	

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 LPe32000 Gen 6 HBA	Driver Versions: ESXi: 10.0.727.44 Windows: 10.0.720.0 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) Firmware Version: SUSE SLES 12-SP3: v. 11.4.204.20
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	6.0, 6.5
VCenter	6.0, 6.5

Software upgrade and downgrade

Migration path

Migration to 14.4.1 is supported from the following previous releases as noted below:

Pre-14.3 release	Versions
Network Advisor 14.2.x	14.2.0, 14.2.1, 14.2.2
Network Advisor 14.3.x	14.3.0, 14.3.1
Network Advisor 14.4.x	14.4.1

Note 1: Network Advisor 14.2.x and 14.3.x, running on the Linux and Windows operating systems, can be upgraded to Network Advisor 14.4.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: Refer to *Supported migration paths* in the Installation and Migration Guide for migration paths from pre-14.2.x releases.

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

Note 5: 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 6: Fresh install for SAN+IP support has been removed. Migration from SAN to SAN+IP support also has been removed for 14.4.x

Note 7: IP only installation is not supported with 14.4.x

Note 8: Follow the below instructions to perform AMP migration from 14.2.x/14.3.x to 14.4.x:

- Start with the source version is running BNA 14.2.x/14.3.x
- And then upgrade AMP OS from 2.1.0 to AMP OS 2.2.0 (after successful BNA Migration)

Upgrade and downgrade considerations

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.

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 Professional Plus Licensed Version	SAN Enterprise Licensed version
SAN Enterprise Trial	SAN Enterprise Licensed version

SAN+IP Upgrade Paths

Note. BNA 14.4.x does not support a fresh installation of SAN+IP license. However, if a SAN+IP license is already installed on a pre-14.4.x BNA, then that version of BNA can be successfully upgraded to BNA 14.4.x.

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

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. If you combine more than one downgrade option, you must meet the requirements for all downgrade options.

Edition Downgrade Paths

Current software release	To software release
Enterprise SAN	Professional Plus SAN

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 must 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, 2 virtual)	4 (2 physical, 4 virtual)	4 (2 physical, 4 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, 2 virtual)	4 (2 physical, 4 virtual)	8 (4 physical, 8 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: 8
- Disk Space: 1 TB

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

Resources	5000 Flows	10000 Flows	20K Flows	40K Flows	60K Flows	80K Flows	>100K Flows
Installed Memory	16 GB	24 GB	32 GB	32 GB	32 GB	64 GB	64 GB
Processor Core Count (physical, logical)	8 (4 Physical, 8 Logical)	12 (6 Physical, 12 Logical)	24 (12 physical, 24 logical)	24 (12 physical, 24 logical)	24 (12 physical, 24 logical)	48 (24 physical, 48 logical)	48 (24 physical, 48 logical)
Disk Space (including future migration)	1 TB	2 TB	4 TB	8 TB	12 TB	16 TB	20 TB
Server Heap	4 GB	6 GB	6 GB	6 GB	6 GB	6 GB	6 GB
Client Heap	1 GB	2 GB	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, 2 virtual)	4 (2 physical, 4 virtual)	8 (4 physical, 8 virtual)
Disk Space	10 GB	10 GB	10 GB

When BNA monitors 10 AMPs or 200000 flows, the system requirements for server (plus 1 desktop/web client) installation are:

- RAM Memory: 64 GB
- Processor: 48 core processor (24 physical and 48 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 processors (4 physical and 8 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, or the server and Fabric OS switches 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.

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 14.4.x > Network Advisor 14.4.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.

Limitations and restrictions

Scalability

All scalability limits are subject to change. The limits noted in this section apply to all the platforms listed unless otherwise specified.

Supported scalability limits by Network Advisor edition:

	Enterprise Edition			Professional Plus Edition	Professional Edition
	Small	**Medium**	**Large**		
SAN Switch Ports	2000	5000	15000	2560	300
SAN Switches and Access Gateways	40	100	400	40	15
SAN Devices	5000	15000	40000	5000	1000
SAN Fabrics	25	50	100	36	2
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

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

Compatibility and interoperability

Discovery of Qlogic branded Brocade adapters is not supported.

Important notes

Known issue with internal SCP/SFTP service

Known issue with internal SCP/SFTP service <u>only if</u> migrated from <u>Network Advisor 14.4.0 to 14.4.1 or later</u>

If switch firmware download or switch supportsave operations fail when initiated from Brocade Network Advisor 14.4.1 or later that has SCP/SFTP configured as the preferred option, users may use one of the following workarounds:

Workaround:

1. Change the option in Network Advisor 14.4.x to use FTP as the preferred option

   Or

2. To continue using SCP/SFTP as the preferred option do the following:

   If <u>pre-14.4.0 (Network Advisor version prior to 14.4.0)</u> partially uninstalled location is available:

   a. Stop Network Advisor services.
   b. Replace *ssh-keypair.ser* in Network Advisor 14.4.1 or later with the file from pre-14.4.0 partially uninstalled location as follows:
      - Copy ssh-keypair.ser from
        C:\Program Files*Network Advisor* ***<pre-14.4.0>***conf.uninstall\security
        To
        C:\Program Files\Network Advisor **14.4.x**\conf\security
      - Restart Network Advisor services.

   c. After making the above mentioned changes, if switch firmware download or switch supportsave operations still fail on some switches, then do the following on each of those switches

      - Login to the switch as admin and delete the Network Advisor server IP address entry by executing one of the following commands
        - To delete just one Network Advisor server entry at a time do the following:
          sw0:FID128:admin> sshutil delknownhost
          IP Address/Hostname to be deleted: <Network Advisor IP Address>
          Please Confirm with Yes(Y,y), No(N,n) [N]: y
        - To delete all known SSH hosts from the switch execute the following command

```
sw0:FID128:admin> sshutil delknownhost -all
    Please Confirm with Yes(Y,y), No(N,n) [N]: y
```

If pre-14.4.0 partially uninstalled location is no longer available, then perform the following steps:

- Login as admin to the switch where firmware download or supportsave has failed and delete the Network Advisor server SSH host name/IP address entry by executing one of the following commands
  - To delete just one Network Advisor server entry at a time do the following:

    ```
    sw0:FID128:admin> sshutil delknownhost
    IP Address/Hostname to be deleted: <Network Advisor IP Address>
        Please Confirm with Yes(Y,y), No(N,n) [N]: y
    ```

  - To delete all known SSH hosts from the switch execute the following command

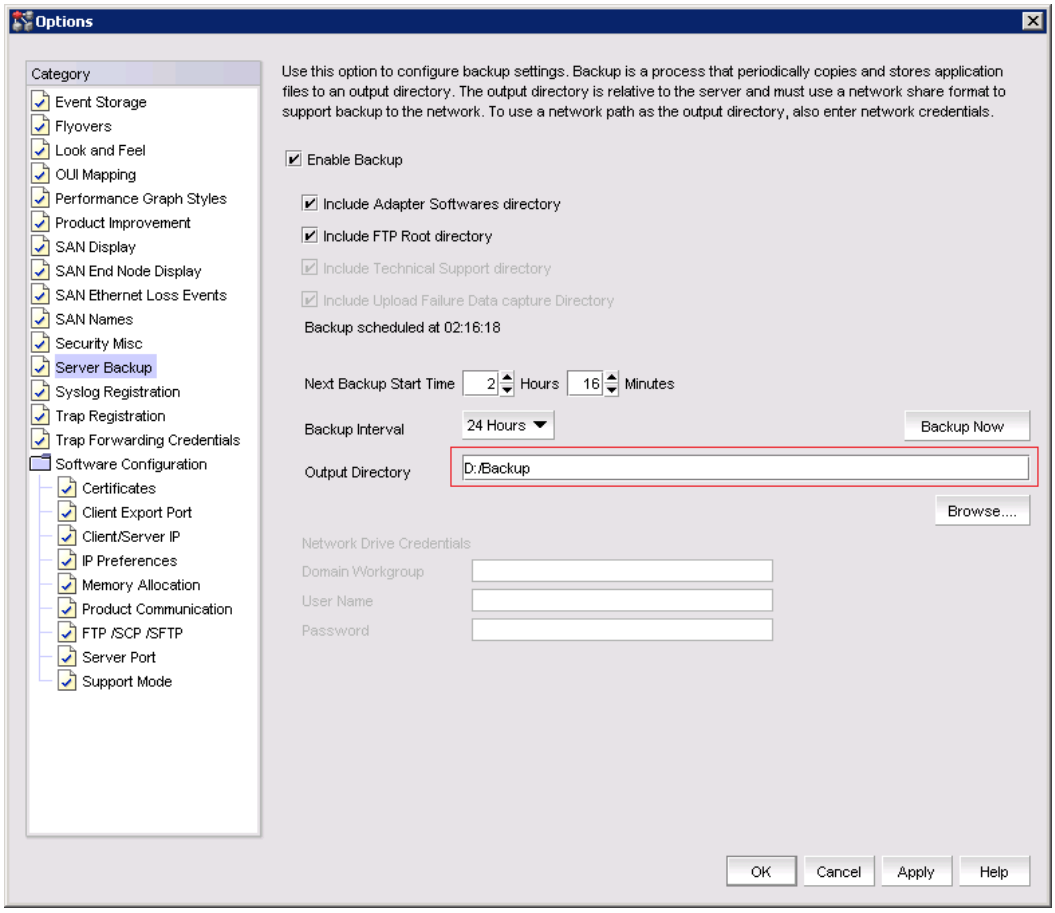
    ```
    sw0:FID128:admin> sshutil delknownhost -all
            Please Confirm with Yes(Y,y), No(N,n) [N]: y
    ```

Important Notes for managing Brocade Analytics Monitoring Platform

- **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.



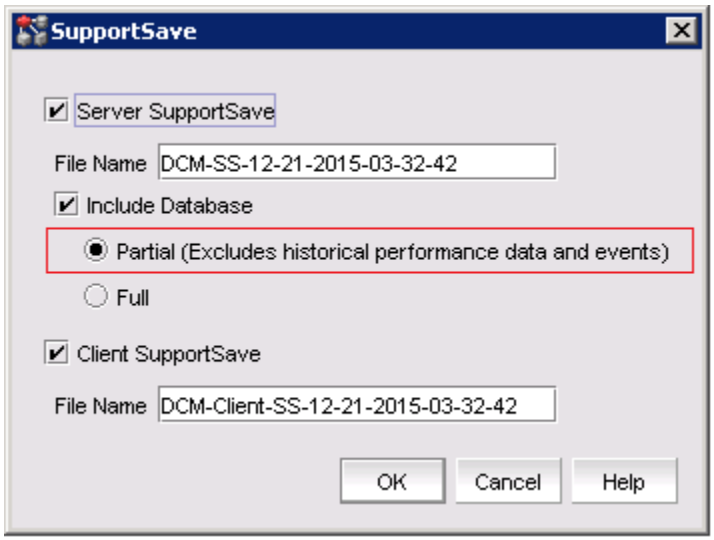
c) While migrating Network Advisor from pre-14.3.x version to 14.3.x or later, it may take longer time for the Source monitor DB services to stop. As a result an error is being shown in "Resource validation and data migration" screen: "Migration Failed. Network Advisor will roll back to the previous 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

- **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.



- **Disk space recommendation in case of Migration**
  - 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.

- **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.

- An AMP device should be discovered by only one BNA server.
- It is highly recommended to use unique FID for all AMP logical switches discovered in BNA
- Port Demand rate and ROS measures calculation cannot be done for NPIV ports and Hosts connected to AG
- Pending IOs widget shows data only for physical ports.
- **Data plotting in Port Investigate view when Navigating from Dashboard/Inventory detailed view**
  - Plotting first data point for ROS measure takes up to 40 secs.
  - Time stamp for ROS, Pending IOS may not match with other port measures (Ex: TX%, RX%)
    - Real time plotting happens based on the device time stamp.

    - Port level measure plotting may take up to 1 min in port investigation view.
- MAPS Events purging limit is changed to 50000 by default in Network Advisor 14.3.x (Earlier this limit was set with 10 Millions). User can customize this purging limit by changing the "Maximum Events" in Event Storage page from Option dialog.
- When user drill down a violation bar, the violation dialog would be empty when those MAPS events got purged.
- Report generation will be done in serial order so when a report generation is in progress, another report will be generated only after the completion of the first report
- Report generation might take some time based on the number of widgets available in the template.
- Threshold sub-widget header in TOP N report widgets will not be shown in generated output.
- After importing a collection, the banner will be retained till 1-2 mins until the deployment gets completed. Editing the collection within this time may lead to show the errors in banner "Group name already exists"
- If headless installation is done, AMP manageability will not be enabled by default. This need to be enabled explicitly by running "enableamp.bat" script from below location:
    - <Network Advisor Home>\monitor\bin
- After deleting the threshold widget, User will not be able to view the generated report output. So recommending not to delete the Threshold sub widget
- With a symmetric Fabric (Same Flow configuration in two or more fabrics)
    - In Threshold widget incorrect detail is displayed for "Occurrence" column
    - On applying name for port/flow filter of single fabric, report is generated for all the symmetric fabrics
- User will be able to launch web client with IPv6 address only from Chrome browser. Web client launch fails with Edge and Internet Explorer with IPv6 address.
- A delay of 2-3 mins may be observed while investigating MPIO path utilization for historical data. During this delay, network flows page shows hyphen (-) in place of path utilization percentage.
- BB Credit Zero measure in port historical investigate is plotted with the unit of errors. User need to select the Unit/Sec option from thick client Options -> Performance Graph Styles -> Unit Display
- While investigating ROS measure for multiple symmetric flows, same value will be plotted for all the flows. User need to select individual flow to view specific flow's ROS value.
- Real-time stats are not supported for path utilization. When user selects Real-time for the measure "path utilization", switching back to Historical is disabled. Work around is to switch to some other measure and navigate to historical
- Up on configuring the IT/ITL resource limits to that of the currently used count, user will need to reset the sys_mon_analytics_flow. In this case, refreshing the switch details page won't update with the changed limits. Work around is to go to some other page and get back to inventory.
- Due to enhanced security in Network Advisor 14.4.x the migration from earlier releases to 14.4.x will fail if the existing Network Advisor server certificate does not meet the enhanced security requirements.

  Available Workarounds:
  1. Replace the previous version's certificate with new Self Signed certificate, use Server→Options→Software Configuration→Certificates→Keystore Certificate, and choose Replace in the dropdown. Then restart Network Advisor services, make sure that Client is logged in, then migrate to 14.4x
  2. Replace the Certificate with a new Signed Certificate conforming to the following standard
     a. RSA Key size not less than 2048
     b. Signature algorithm sha256withRSAEncryption

3. Remove the disabled less secure algorithms restricted in 14.4.x in <Network Advisor Home>\jre64\lib\security\java.security file under disabled algorithms, which is SHA1 and RSA Key size < 2048

Important SAN Notes

- While pushing larger zone configurations, make sure to reserve enough space in zone db to accommodate HDR size of all the LS and actual committed configuration within the zone DB 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.

- Starting FOS 8.1.0x of 16 LS support provided 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
- SAN Inventory widget in default dashboard shows 'Error loading the data' on creating and deleting custom dashboards inconsistently when managing more than 9000 ports. User has to re-launch the client to see the data again.
- Do not enable "Use SSL 2.0 compatible ClientHello format" setting in Java Control Panel on the Network Advisor Client machine as it will interfere with the remote client launch.
- For AMP users with scaled number of AMP flows, it is recommended that you disable daily database backups for better Network Advisor performance with the AMP case.
  If local server has JRE version 1.8u112, the links in Configure SMIA Agent dialog in Server Management Console, will not launch.
  Workaround: Uninstall the JRE version 1.8u112 or install JRE version 1.8u111.
- While generating reports from Microsoft Windows command prompt and saving the report in non-default location, the report output directory path should not end with the backslash ("\"), or the backslash character should be prefixed with forward slash ("/"). For example: *–o "c:\/"*.
- 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.
- When hosts, vCenters, SMIA clients or SSL/TLS email servers do not have certificates with SHA2 algorithm and RSA keySize > 2048, the discovery and management of the hosts and vCenters, connections from SMIA clients, and email notifications (when Network Advisor is configured with SSL/TLS) will fail due to disabling of all weak hashing algorithms in Network Advisor 14.3.1 to make it more secure.

  If users wish to continue using certificates with weaker algorithms, they need to remove SHA1

and RSA keySize < 2048 from the disabled algorithms list in the java.security file present on the Network Advisor server as follows:

1. Navigate to <Network Advisor Home>\jre64\lib\security directory to open the java.security file and remove **SHA1** and **RSA keySize < 2048** from the disabled algorithm list:
   jdk.tls.disabledAlgorithms=MD5, DES, 3DES, DESede, RC2, DHE, DH, ECDHE, ECDH, SSLv3, RC4, MD5withRSA, **SHA1**, DSA, DH keySize < 768, \ EC keySize < 224, **RSA keySize < 2048**
2. Restart all the Network Advisor services through the Service Management Console

- Parallel firmware upgrade of fixed-port switches may cause traffic disruption. Serial firmware download is suggested in this case. Refer to the *SAN Device Configuration -> Firmware Management -> Firmware upgrade or downgrade considerations* chapter in the SAN User manual for more information.

- Call Home behavior was changed in Network Advisor 14.4.0/14.4.1 to trigger Call Home on all MAPS-1003 events to provide an option to users to get alerted about such events. If Call Home Filters are configured prior to migrating from a previous Network Advisor version, there will be no change in behavior. However if Call Home is being configured for the first time or is currently using the default configuration, then MAPS-1003 events will trigger Call Home. If this behavior is not desired, Call Home filters need to be configured to exclude MAPS-1003 events.

- Zone database entries in a peer zone may get deleted when user attempts to edit an alias of a principal member in a peer zone if there are ten or more principal members present in the peer zone.
  Observed when there are ten or more principal members present in a peer zone, and if those principal members contain one or more aliases, then an attempt to add or delete a member in any of those aliases will not succeed. Under this condition the Apply or OK button press will delete a random alias member instead of applying new changes; also, Edit Alias dialog will not close upon pressing the OK button. When this happens, if users save (OK/Apply button press on "Zoning" dialog) or activate the edited Zone Configuration (Activate button press on "Zoning" dialog), then it will delete already existing members of the alias. Which zone members get deleted is unpredictable and the number of members deleted corresponds to the number of times the OK or Apply button is pressed in the Edit Alias dialog.
  Recovery: While in the Edit Alias dialog, if user notices that OK and Apply buttons are not working (i.e. changes are not applied and OK button does not close the dialog), then abort the zone edit operation completely by pressing Cancel button on "Edit Alias" dialog and then press Cancel button on "Zoning" dialog.
  Workaround: To edit an alias, first remove it from the peer zone, edit it as needed, add it back to the peer zone, and then activate the zone configuration.
  Issue is tracked by DEFECT000660343 (see defect details below in this document).

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 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>

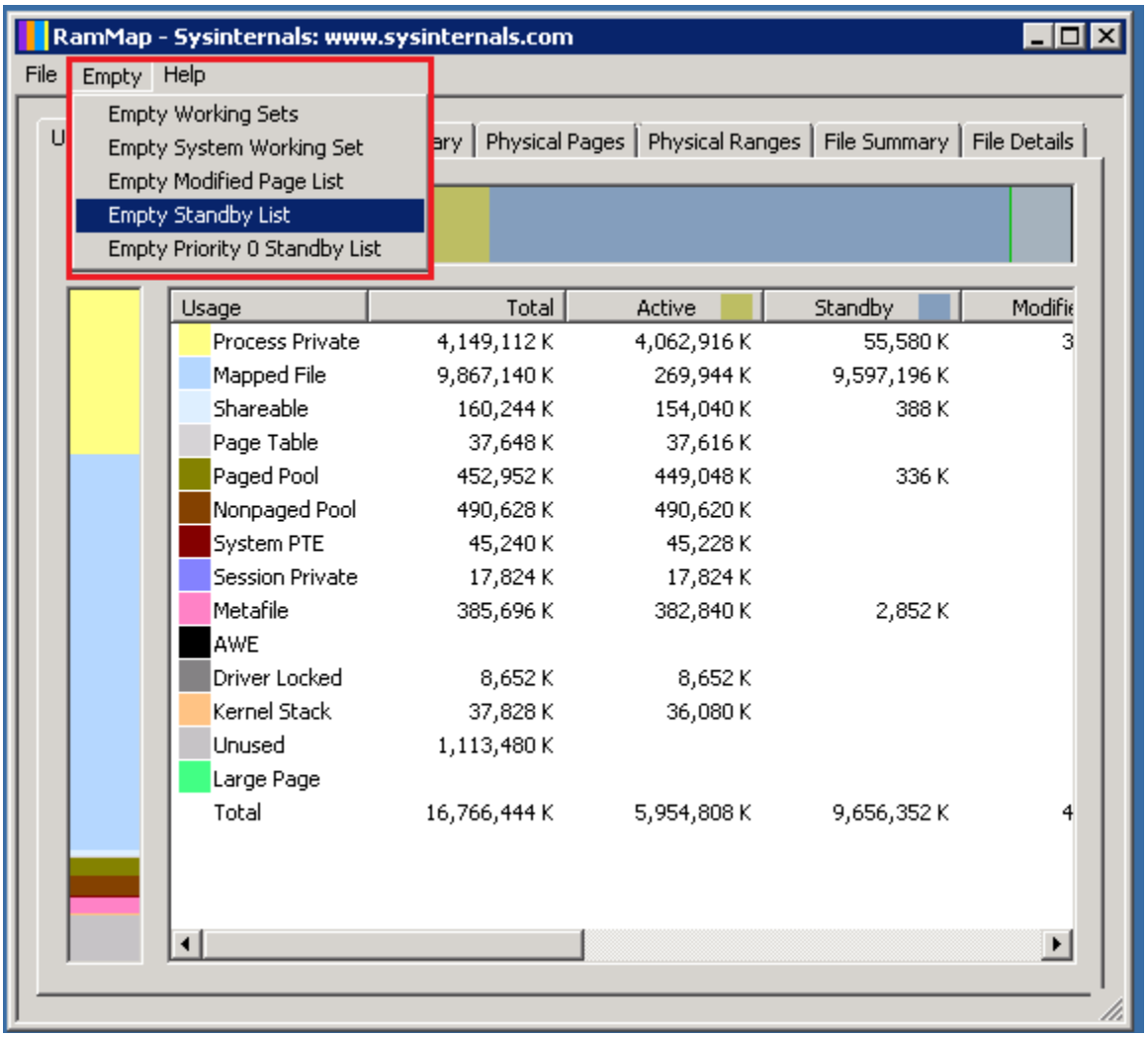
- **Firmware version 2.1.1b**

  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
24. The "From Email Address" attribute is not supported for NOS devices. Similarly, the "From Email Address" attribute is not supported for FOS devices with pre-8.2.0 firmware versions.
    However, in above cases the "From Email Address" is enabled and accepts input which is not being saved.
    "Test Email" attribute is not supported for NOS and should be grayed out. However, when mixture of FOS and NOS devices are managed in Network Advisor, the "Test Email" will be enabled as it is supported for FOS.
    The above behavior has been captured in DEFECT000660376 below in this document.
25. Any other standalone instance of PostgreSQL should not be present on the system where the Network Advisor application is installed. If such other instance of PostgreSQL exists on the same server, then it will be removed along with the Network Advisor during the Network Advisor uninstallation.



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 Network Advisor from OEM1 version to OEM2 version

a. Partially uninstall the source Network Advisor OEM1 version
b. Now install BNA 14.3.x OEM2 version
c. In the 'copy data and settings' page, browse to the BNA Pre-14.3.x OEM1 version and continue with the migration.

Migrating BNA (pre-14.3.x) OEM1 version to BNA 14.3.x OEM2 version

d. Install the source BNA Network Advisor OEM1 version
e. Now install BNA 14.3.x OEM2 version
f. In the 'copy data and settings' page, browse to the BNA pre-14.3.x 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	y	d	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 value[1]: is the difference of value retrieved between the two consecutive poling cycles.

2. Polling interval[2]: 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:

Od heap size:

small

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

medium

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

Large

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

Curent Heap Size:

small

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

medium

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

Large

platform.32.cimom.conf.set.MAX_HEAP_SIZE = 1024m
platform.64.cimom.conf.set.MAX_HEAP_SIZE = 3072m

Logging for CIMOM

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

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

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

Service Location Protocol (SLP) support

The Management application SMI Agent uses Service Location Protocol (SLP) to allow applications to discover the existence, location, and configuration of WBEM services in enterprise networks.

You do not need a WBEM client to use SLP discovery to find a WBEM Server; that is, SLP discovery might already know about the location and capabilities of the WBEM Server to which it wants to

send its requests. In such environments, you do not need to start the SLP component of the Management application SMI Agent.

However, in a dynamically changing enterprise network environment, many WBEM clients might choose to use SLP discovery to find the location and capabilities of other WBEM Servers. In such environments, start the SLP component of the Management application SMI Agent to allow advertisement of its existence, location, and capabilities.

SLP installation is optional and you can configure it during Management application configuration. Once installed, SLP starts whenever the Management application SMI Agent starts.

Management SMI Agent SLP application support

Management SMI Agent SLP application support includes the following components:

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

By default, the Management application SMI Agent is configured to advertise itself as a Service Agent (SA). The advertised SLP template shows its location (IP address) and the WBEM Services it supports. The default advertised WBEM services show the Management application SMI Agent:

- accepts WBEM requests over HTTP without SSL on TCP port 5988
- accepts WBEM requests over HTTPS using SSL on TCP port 5989

slptool commands

Use the following slptool commands to verify whether the SLP is operating properly.

- slptool findsrvs service:service-agent

  Use this command to verify that the Management application SMI Agent SLP service is properly running as a Service Agent (SA).

  Example output: service:service-agent://127.0.0.1,65535

- slptool findsrvs service:wbem

Use this command to verify that the Management application SMI Agent SLP service is properly advertising its WBEM services.

Example outputs:

service:wbem:https://10.0.1.3:5989,65535

service:wbem:http://10.0.1.3:5988,65535

This output shows the functionalities of Management application SMI Agent:

1. accepts WBEM requests over HTTP using SSL on TCP port 5989
2. accepts WBEM requests over HTTP without SSL on TCP port 5988
3. slptool findattrs service:wbem:http://IP_Address:Port
    a. Use this command to verify that Management application SMI Agent SLP service is properly advertising its WBEM SLP template over the HTTP protocol.
    b. Example input: slptool findattrs service:wbem:http://10.0.1.2:5988
    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

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 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

Reporting Errors in the Guides

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

Known Documentation Errors

- The copyright statement in Network Advisor user manuals should read the following:

  Copyright © 2018 Brocade Communications Systems LLC. All Rights Reserved. Brocade and the stylized B logo are among the trademarks of Brocade Communications Systems LLC. Broadcom, the pulse logo, and Connecting everything are among the trademarks of Broadcom. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

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

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

- In the Network Advisor Installation and Migration Guide following details are missing:
  - 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, 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 SAN AMP and SAN IP AMP User Manual:
  - Statement "Management Application server and Client System clocks are synchronized even if they are in different time zone" should be corrected as "Management application server and client system clocks should be synchronized even for different time zones since user would see the problem in historical data when customized time configured in client system"
  - For Upgrade and Migration, please refer to the below notes:
    - Follow the below instructions to perform migration from 14.2.x/14.3.x to 14.4.x:
      • Start with the source version is running BNA 14.2.x/14.3.x with AMP-service enabled; AMP running firmware v2.1.0.
      • First migrate the source BNA 14.2.x/14.3.x version to 14.4.x.
      • And then upgrade AMP OS from 2.1.0 to AMP OS 2.2.0 (after successful BNA Migration)
- Following content should be removed from the Network Advisor SAN User Manual and SAN AMP User Manual:
  - All references to CLI Configuration Management
  - MRP Topology
  - Configuring event actions for Snort messages
  - SSH/Telnet row (which is applicable to Ironware and Network OS) in Table 15 Product communication protocols
- Network Advisor SAN+IP User Manual and SAN+IP AMP User Manual have to be updated with the following information:
  - The "From Email Address" attribute is not supported for Network OS devices. Similarly, the "From Email Address" attribute is not supported for Fabric OS devices with pre-8.2.0

firmware versions. In above cases the "From Email Address" is enabled and accepts input which is not being saved.

- "Test Email" attribute is not supported for Network OS and should be grayed out.
- When mixture of Fabric OS and Network OS devices are managed in Network Advisor, the "Test Email" will be enabled as it is supported for FOS.

Defects

TSBs—Critical issues to consider prior to installing this release

Technical Support Bulletins (TSBs) provide detailed information about high priority defects or issues present in a release. The following sections specify all current TSBs that have been identified as being a risk to or resolved with this specific release. Please review carefully and refer to the complete TSB for relevant issues prior to migrating to this version of code. On http://my.brocade.com (sign-in required) this product documentation can be found by selecting **Support > Document Library** then under **Explore by Content Type** select **View All** > **Technical Service Bulletin** (note that TSBs are generated for all Brocade platforms and products, so not all TSBs apply to this release).

TSB issues resolved in Network Advisor 14.4

TSB	Summary
TSB 2017-267-A	Upgrading to Brocade Network Advisor 14.3.1 fails migration and rolls back to the source version.
TSB 2017-269-A	The WebTools or Brocade Network Advisor (BNA) remote client launch will be blocked by Java Security when running against a version of FOS or BNA that contains an expired Java code signing certificate.

Closed with code changes in Brocade Network Advisor 14.4.2

This section lists software defects with Critical, High, and Medium Technical Severity closed with a code change as of 4/9/18 in Brocade Network Advisor 14.4.2.

Defect ID:	DEFECT000627655		
Technical Severity:	High	**Probability:**	Medium
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:	DEFECT000651413

Technical Severity:	Medium	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Device Management
Reported In Release:	Network Advisor12.2.0	**Technology:**	Device configuration (SAN)
Symptom:	In Edit peer zone dialog the peer alias is being incorrectly displayed in the Principal member column.		
Condition:	When creating two peer zones with the same alias and adding this alias as a principal member in one zone and a peer member in another zone.		
Workaround:	Create one peer zone at a time and save it.		

Defect ID:	DEFECT000656795		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Client
Reported In Release:	Network Advisor14.4.0	**Technology:**	Online Help
Symptom:	Search functionality is not working in Network Advisor online help.		
Condition:	Observed in online help.		
Workaround:	Use pdf versions of Network Advisor user manuals.		

Defect ID:	DEFECT000657754		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Management
Reported In Release:	Network Advisor14.2.1	**Technology:**	Configuration Fundamentals
Symptom:	LSAN Zone configuration is not being applied to the fabric despite the successful status shown in Network Advisor.		
Condition:	Occurs when trying to activate an LSAN zone from Network Advisor on switches running pre-8.1.0 FOS version, if the LSAN zone name starts with non-alphabetic character.		

Defect ID:	DEFECT000657997		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Device Management
Reported In Release:	Network Advisor14.4.1	**Technology:**	Device configuration (SAN)
Symptom:	Failed to set the chassis name and the error displayed stating that reached the maximum length of characters which is 15.		
Condition:	Observed when attempting to set the chassis name which is longer than 15 characters but less than 32.		

Defect ID:	DEFECT000658400		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Client
Reported In Release:	Network Advisor14.4.0	**Technology:**	Options Dialog
Symptom:	Network Advisor shows ?Unknown? vendor for the Synergy card.		
Condition:	When Synergy chassis is discovered in the Network Advisor.		

Defect ID:	DEFECT000658457		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Device Management
Reported In Release:	Network Advisor14.4.0	**Technology:**	Firmware Management
Symptom:	Network Advisor showed the firmware download failure, when it had actually finished successfully on the switches.		
Condition:	Observed after upgrading the switch firmware version to v8.2.0 and above.		

Defect ID:	DEFECT000658513		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Device Management
Reported In Release:	Network Advisor14.4.0	**Technology:**	Device configuration (SAN)
Symptom:	Help is not launching in SNMP Setup--> Event Reception page and Legend is not launching in topology page		
Condition:	When user is trying to access online help.		

Defect ID:	DEFECT000658886		
Technical Severity:	High	**Probability:**	High
Product:	Brocade Network Advisor	**Technology Group:**	Device Monitoring
Reported In Release:	Network Advisor14.4.1	**Technology:**	MAPS - Monitoring and Alerting Policy Suite
Symptom:	Unable to create MAPS policy with measures for the groups: ALL_25Km_16GLWL_SFP, ALL_32GSWL_SFP, ALL_32GLWL_SFP, ALL_32GSWL_QSFP		
Condition:	When creating a policy with rules for the groups ALL_25Km_16GLWL_SFP, ALL_32GSWL_SFP, ALL_32GLWL_SFP, ALL_32GSWL_QSFP Network Advisor shows successful completion of operation, however, the rules are not being pushed to the switch.		
Workaround:	User can create the rules for respective groups using CLI.		

Defect ID:	DEFECT000659189		
Technical Severity:	Medium	**Probability:**	High
Product:	Brocade Network Advisor	**Technology Group:**	Device Monitoring
Reported In Release:	Network Advisor14.4.0	**Technology:**	Reports
Symptom:	Fabric Summary Report incorrectly reports number of devices in the fabric.		
Condition:	When same device is being connected to different switches in the fabric.		

Defect ID:	DEFECT000659256		
Technical Severity:	High	**Probability:**	High
Product:	Brocade Network Advisor	**Technology Group:**	Device Management
Reported In Release:	Network Advisor14.4.1	**Technology:**	Device configuration (SAN)
Symptom:	In CEE port properties tab, "LAG" has been renamed to "Port Channel" in Network Advisor user manuals.		
Condition:	In CEE port properties tab "LAG" has been renamed to "Port Channel" to be on par with Fabric OS terminology.		

Defect ID:	DEFECT000659442		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Management
Reported In Release:	Network Advisor14.3.1	**Technology:**	Configuration Fundamentals
Symptom:	Network Advisor user manuals contain outdated information and list database tables that no longer exist.		
Condition:	Issue exists in SAN and SAN+IP user manuals.		

Defect ID:	DEFECT000659584		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Device Monitoring
Reported In Release:	Network Advisor14.3.0	**Technology:**	Performance
Symptom:	Network Advisor does not show all historical performance graphs for some AG ports		
Condition:	Occurs when AG uses SNMPv1		

Defect ID:	DEFECT000659635		
Technical Severity:	High	**Probability:**	High
Product:	Brocade Network Advisor	**Technology Group:**	Device Management
Reported In Release:	Network Advisor14.4.1	**Technology:**	Device configuration (SAN)
Symptom:	REST API shows a blank response for TDZ status.		
Condition:	Issue observed when requesting TDZ status using REST URL while the switch is in unreachable state.		

Defect ID:	DEFECT000659769		
Technical Severity:	High	**Probability:**	High
Product:	Brocade Network Advisor	**Technology Group:**	Device Monitoring
Reported In Release:	Network Advisor14.4.1	**Technology:**	MAPS - Monitoring and Alerting Policy Suite
Symptom:	Distribution of MAPS policy fails with "Rule name not present " error.		
Condition:	When creating a policy by cloning default policy for X6 chassis in MAPS dialogue for 8.2.0 firmware switch and then distributing the cloned default policy to v7.4.2a switch.		

Defect ID:	DEFECT000659770		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Management
Reported In Release:	Network Advisor14.2.0	**Technology:**	Configuration Fundamentals
Symptom:	Saving a supportsave from the View Repository dialogue (i.e. when using File Stream to transfer the data) results in the saved file size 8 KB.		
Condition:	Observed when saving the large supportsave which is greater than 1 GB.		

Defect ID:	DEFECT000659798		
Technical Severity:	High	**Probability:**	High
Product:	Brocade Network Advisor	**Technology Group:**	Device Management
Reported In Release:	Network Advisor14.4.1	**Technology:**	Device configuration (SAN)
Symptom:	Logical Switch Change Configuration dialog shows ?Partially Failed? output with "Bind ports failed. Reason: The indicated port is not disabled? status details.		
Condition:	Observed while creating a fabric with zero based addressing mode and moving ports from LHP to RHP.		

Defect ID:	DEFECT000659828		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Management
Reported In Release:	Network Advisor14.4.1	**Technology:**	Configuration Fundamentals
Symptom:	Network Advisor does not allow moving unbound ports into a FICON Logical Switch and shows a popup dialog with the recommendation to bind ports.		
Condition:	Observed while creating a new FICON Logical Switch and intentionally leaving the selected ports unbound.		
Workaround:	Use the CLI to move unbound FC ports into the newly created FICON Logical Switch.		

Defect ID:	DEFECT000659835		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Device Monitoring
Reported In Release:	Network Advisor14.4.0	**Technology:**	Dashboards
Symptom:	Port Optics (SFP) dialog is blank for all switches.		
Condition:	Observed in non-English locale.		

Defect ID:	DEFECT000659898		
Technical Severity:	High	**Probability:**	High
Product:	Brocade Network Advisor	**Technology Group:**	Device Management
Reported In Release:	Network Advisor14.4.0	**Technology:**	Discovery
Symptom:	Network Advisor stopped communicating to the switches after performing the firmware download.		
Condition:	Observed after upgrading switches? firmware from pre-8.1.2 version to 8.1.2 or later.		

Defect ID:	DEFECT000659904		
Technical Severity:	Medium	**Probability:**	High
Product:	Brocade Network Advisor	**Technology Group:**	Partner Integration
Reported In Release:	Network Advisor14.4.2	**Technology:**	SMI Agent
Symptom:	Creating a Zone alias results in extrinsic operation class cast exception.		
Condition:	Observed when adding Zone alias from any CIMOM client.		

Defect ID:	DEFECT000659987		
Technical Severity:	High	**Probability:**	High
Product:	Brocade Network Advisor	**Technology Group:**	Monitoring
Reported In Release:	Network Advisor14.4.2	**Technology:**	Hardware Monitoring
Symptom:	MAPS Policy distribution from Network Advisor resulted in duplicate rules and termination of MAPS daemon on the switch.		
Condition:	When attempted bulk distribution of MAPS Policies from Network Advisor to Fabric OS switches running v8.1.x firmware versions.		

Defect ID:	DEFECT000659994		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Fault Management
Reported In Release:	Network Advisor14.4.1	**Technology:**	Call Home
Symptom:	Due to Call Home behavior change in in Network Advisor 14.4.0/14.4.1, Call Home alerts are being triggered on all MAPS-1003 events to provide an option to users to get alerted about such events.		
Condition:	Observed if Call Home is being configured for the first time or is currently using the default configuration, then MAPS-1003 events will trigger Call Home.		
Workaround:	Call Home filters need to be configured to exclude MAPS-1003 events.		

Defect ID:	DEFECT000660002		
Technical Severity:	High	**Probability:**	High
Product:	Brocade Network Advisor	**Technology Group:**	Device Monitoring
Reported In Release:	Network Advisor14.4.2	**Technology:**	Performance
Symptom:	Performance Monitor Historical graph will not be plotted for some of the ports.		
Condition:	Occurs in large networks with multiple 8510 and X6 directors, when large number of requests is being sent to the switch.		

Defect ID:	DEFECT000660025		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Monitoring
Reported In Release:	Network Advisor14.4.1	**Technology:**	Hardware Monitoring

Symptom:	MAPS Policy edit dialog in Network Advisor does not display the "Switch Status Marginal" and "Switch Status Critical" actions for the Resource group's "CPU" and "Memory" categories.
Condition:	Observed while configuring MAPS via Monitor >> Fabric Vision >> MAPS >> Configure dialog for v7.4.x switches.

Defect ID:	DEFECT000660195		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Management
Reported In Release:	Network Advisor14.4.0	**Technology:**	Configuration Fundamentals
Symptom:	?Rule Name not found? error is shown in MAPS dialog.		
Condition:	Observed while importing an edited MAPS policy via Network Advisor if rules count exceeds 500.		

Defect ID:	DEFECT000660205		
Technical Severity:	High	**Probability:**	High
Product:	Brocade Network Advisor	**Technology Group:**	Device Management
Reported In Release:	Network Advisor14.4.2	**Technology:**	Device configuration (SAN)
Symptom:	REST API user guide does not show correct data for events API and description of time data interpretation.		
Condition:	REST API user guide has to be updated with correct data for events API and description of time data interpretation.		

Defect ID:	DEFECT000660304		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Management
Reported In Release:	Network Advisor14.4.1	**Technology:**	Configuration Fundamentals
Symptom:	Failed to schedule AMP reports in Fabric Insight Portal.		
Condition:	Observed after providing scheduling details and clicking ?OK?. An ?Exception while persisting deployment configuration? is being thrown in the Network Advisor server log.		

Defect ID:	DEFECT000660318		
Technical Severity:	High	**Probability:**	High
Product:	Brocade Network Advisor	**Technology Group:**	Management
Reported In Release:	Network Advisor14.4.2	**Technology:**	Configuration Fundamentals

Symptom:	An alias moved between Peer and Principal member lists after it has been edited in Network Advisor.
Condition:	Observed while editing zone alias with the configuration similar to the following: 1. Create two Alias: “a1” and “a2” 2. Create peer zone “pz1” with “a1” as a Principal member and “a2” as a Peer member 3. Edit Alias “a1” to add a new member 4. As a result alias “a1” will move to Peer member list

Defect ID:	DEFECT000659760		
Technical Severity:	High	**Probability:**	High
Product:	Brocade Network Advisor	**Technology Group:**	Management
Reported In Release:	Network Advisor14.4.0	**Technology:**	Configuration Fundamentals
Symptom:			
Condition:	Occurs when editing a zone alias members by adding new WWPN and trying to activate zone configuration.		

Defect ID:	DEFECT000659420		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Management
Reported In Release:	Network Advisor14.4.0	**Technology:**	Configuration Fundamentals
Symptom:	Network Advisor displays incorrect information in COMPASS -> Manage Product Groups "Available Targets" dialog.		
Condition:	Observed when configuring COMPASS.		

Defect ID:	DEFECT000657274		
Technical Severity:	High	**Probability:**	High
Product:	Brocade Network Advisor	**Technology Group:**	Device Management
Reported In Release:	Network Advisor14.3.0	**Technology:**	Device configuration (SAN)
Symptom:	While triggering the switch supportsave from Network Advisor, server is getting an error response from the switch.		
Condition:	When v8.1.0c switch is configured for strong security by running seccryptocfg with "default_strong" template, and SFTP protocol is being used in Network Advisor.		

Closed without code changes in Brocade Network Advisor 14.4.2

This section lists software defects with Critical, High, and Medium Technical Severity closed without a code change as of 4/9/18 in Brocade Network Advisor 14.4.2.

Defect ID:	DEFECT000620924	**Technical Severity:**	Medium
Reason Code:	Not Reproducible	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Device Management
Reported In Release:	Network Advisor12.4.2	**Technology:**	Discovery
Symptom:	The client performance is slow. The SAN tab takes 7 to 9 minutes to load.		
Condition:	When a large number of VMs are present in the vCenter monitored by Network Advisor.		

Defect ID:	DEFECT000629294	**Technical Severity:**	Medium
Reason Code:	Will Not Fix	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Device Management
Reported In Release:	Network Advisor14.2.0	**Technology:**	Configuration Wizard (IP)
Symptom:	Network Advisor allows specifying an incorrect address range while creating a Logical Switch in FICON fabric, and this incorrect address range is being shown in the popup dialog.		
Condition:	Observed while creating a Logical Switch in FICON fabric and moving address-bound ports into the new switch.		
Workaround:	User has to specify address range within the supported range of address assignments of the particular switch model.		

Defect ID:	DEFECT000644622	**Technical Severity:**	Medium
Reason Code:	Not Reproducible	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Management
Reported In Release:	Network Advisor14.2.0	**Technology:**	Configuration Fundamentals
Symptom:	Slow response observed when toggling between SAN tab and Dashboard tab in Network Advisor desktop client.		
Condition:	Observed in a specific environment. Not reproducible in other lab test beds, even with higher data load.		

Defect ID:	DEFECT000647059	**Technical Severity:**	High
Reason Code:	Will Not Fix	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Management
Reported In Release:	Network Advisor14.4.0	**Technology:**	Configuration Fundamentals
Symptom:	When moving FC ports into a FICON Logical Switch, the X6 chassis shows "FFDC queue pdm: queue full" error .		
Condition:	Observed for X6 chassis when moving large number of FC ports (~100) into a FICON Logical Switch, with selected the Addressing check box and re-enable.		
Workaround:	Limit the number of FC ports to 50 per operation.		

Defect ID:	DEFECT000652001	**Technical Severity:**	High

Reason Code:	Will Not Fix	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Device Monitoring
Reported In Release:	Network Advisor14.4.0	**Technology:**	Flow Vision (SAN)
Symptom:	Occasionally to close the LUN picker dialog it is necessary to click OK/Cancel button few times.		
Condition:	Observed on X6 directors when creating a flow monitor.		

Defect ID:	DEFECT000652241	**Technical Severity:**	High
Reason Code:	Will Not Fix	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Device Management
Reported In Release:	Network Advisor14.4.0	**Technology:**	Device configuration (SAN)
Symptom:	Occasionally unplanned restart of the Network Advisor service observed.		
Condition:	When D-port test for multiple ports was initiated via Network Advisor.		
Workaround:	Run D-port for a single port selection.		

Defect ID:	DEFECT000657248	**Technical Severity:**	High
Reason Code:	Will Not Fix	**Probability:**	High
Product:	Brocade Network Advisor	**Technology Group:**	Device Management
Reported In Release:	Network Advisor14.4.0	**Technology:**	Device configuration (SAN)
Symptom:	Rarely an outdated status message is shown in Firmware Download status window for Brocade-6510 switch.		
Condition:	Observed in Network Advisor during firmware download to Brocade-6510 switch.		

Defect ID:	DEFECT000659280	**Technical Severity:**	High
Reason Code:	Will Not Fix	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Management
Reported In Release:	Network Advisor14.4.1	**Technology:**	Configuration Fundamentals
Symptom:	Network Advisor does not update Port Status and Additional Port Info details for ports 44-47 status of G620 switch.		
Condition:	When enabling encryption on G620 switch via Merge FICON Wizard.		

Defect ID:	DEFECT000659612	**Technical Severity:**	High
Reason Code:	Will Not Fix	**Probability:**	High
Product:	Brocade Network Advisor	**Technology Group:**	Management
Reported In Release:	Network Advisor14.4.1	**Technology:**	Configuration Fundamentals
Symptom:	Network Advisor allows some configuration changes on the ports that are reserved for encryption support.		

Condition:	Observed on G620 switches after port encryption is being enabled on any of the ports 44-47 (which are reserved for encryption support).

Defect ID:	DEFECT000659797	**Technical Severity:**	High
Reason Code:	Will Not Fix	**Probability:**	High
Product:	Brocade Network Advisor	**Technology Group:**	Device Management
Reported In Release:	Network Advisor14.4.1	**Technology:**	Device configuration (SAN)
Symptom:	Port optics dialog does not show values for secondary ports in QSFP.		
Condition:	Observed for QSFP ports with 40G Bi-Di LKA optics,		

Defect ID:	DEFECT000659857	**Technical Severity:**	Medium
Reason Code:	Will Not Fix	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Device Management
Reported In Release:	Network Advisor14.4.1	**Technology:**	Topology Views
Symptom:	User had to wait an extreme lengthy time for F-Ports to transition to disabled state.		
Condition:	Observed while configuring large number of ports as SIM_Ports.		
Workaround:	Use smaller batches of ports for configuration.		

Defect ID:	DEFECT000660108	**Technical Severity:**	High
Reason Code:	Will Not Fix	**Probability:**	High
Product:	Brocade Network Advisor	**Technology Group:**	Device Management
Reported In Release:	Network Advisor14.4.2	**Technology:**	Device configuration (SAN)
Symptom:	Logical Switch creation operation via Network Advisor has never completed and status remained ?In Progress?. Network Advisor log showed 401 unauthorized error.		
Condition:	Observed when following sequence of operations is performed within short period of time: a Logical Switch has been created, then deleted, and then created again using the same FID.		
Workaround:	When recreating the Logical Switch after deleting it do the following: a) Wait for up to 60 min if need to re-use the same FID b) Use different FID if recreating the Logical Switch within 60 min		
Recovery:	Restart the Network Advisor client.		

Defect ID:	DEFECT000660125	**Technical Severity:**	Medium
Reason Code:	Will Not Fix	**Probability:**	High
Product:	Brocade Network Advisor	**Technology Group:**	Device Monitoring
Reported In Release:	Network Advisor14.4.2	**Technology:**	Flow Vision (SAN)
Symptom:	Occasionally falling to resize the Flow Vision dialog using the vertical separator line.		
Condition:	Observed in the Flow Vision dialog.		

Workaround:	Use "minimize" or "maximize" arrows of a SplitPane divider to fully expand the panes and view the content.

Defect ID:	DEFECT000642995		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Device Monitoring
Reported In Release:	Network Advisor14.3.0	**Technology:**	Dashboards
Symptom:	In Analytics Summary view, Port widgets shows duplicate data.		
Condition:	For discovered FCR fabric with enable vTap on both the edge fabric - below widgets display duplicate entries: one with FC address and another with the alias name. - Top Initiator Port Flow Latency/Performance - Top Target Port Flow Latency/Performance - Top Target Port Pending IOs		

Defect ID:	DEFECT000646780		
Technical Severity:	High	**Probability:**	High
Product:	Brocade Network Advisor	**Technology Group:**	Device Management
Reported In Release:	Network Advisor14.4.0	**Technology:**	Discovery
Symptom:	Discovery of the fabrics that contain Gen5 or Gen6 directors may take more than 10 minutes. Also, after the successful discovery of the fabric, the SNMP status intermittently may show SNMP communication failure or success.		
Condition:	This occurs if the Gen5 or Gen6 chassis have Brocade SX6 Extension Blade inserted.		

Defect ID:	DEFECT000650885		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Device Monitoring
Reported In Release:	Network Advisor14.4.0	**Technology:**	Flow Vision (SAN)
Symptom:	IO insight measures are not getting collected for G620.		
Condition:	When FOS v8.1.1 is running on G620.		

Defect ID:	DEFECT000652001		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Device Monitoring
Reported In Release:	Network Advisor14.4.0	**Technology:**	Flow Vision (SAN)
Symptom:	Occasionally to close the LUN picker dialog it is necessary to click OK/Cancel button few times.		
Condition:	Observed on X6 directors when creating a flow monitor.		

Defect ID:	DEFECT000654131		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Device Monitoring

Reported In Release:	Network Advisor12.4.3	**Technology:**	MAPS - Monitoring and Alerting Policy Suite
Symptom:	'No Data Points' error shown for FC ports historical reports and no data graphed on Real-time reports		
Condition:	Observed occasionally on some of the switches while collecting performance data.		

Defect ID:	DEFECT000654450		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Client
Reported In Release:	Network Advisor14.4.0	**Technology:**	Installation & Migration
Symptom:	Occasionally the "Server restart required" message is shown when trying to install or migrate Network Advisor, and the error will persist even after restarting the server.		
Condition:	When installing Network Advisor after the previous instance was uninstalled, or migrating to the new version of Network Advisor.		
Workaround:	Delete the service using "sc delete dcmmon-database" command. Then start the installation.		

Open defects

This section lists open software defects with Critical, High, and Medium Technical Severity as of 4/9/18 in Brocade Network Advisor 14.4.2.

Defect ID:	DEFECT000658549		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Device Management
Reported In Release:	Network Advisor14.4.1	**Technology:**	Device configuration (SAN)
Symptom:	AMP resource graph is not being displayed in Network Advisor.		
Condition:	When configuring IT or ITL reservation limit less than used count, which needs a flow reset on AMP device, and then saving the configuration. Observed that the AMP resource graph is not refreshed even after next polling cycle.		
Workaround:	1. Click the inventory tab or click back button in the AMP switch details page. 2. Now click on same AMP to view the switch details page. 3. Updated AMP resource graph is getting displayed.		

Defect ID:	DEFECT000659885		
Technical Severity:	High	**Probability:**	High
Product:	Brocade Network Advisor	**Technology Group:**	Management
Reported In Release:	Network Advisor14.4.1	**Technology:**	Configuration Fundamentals

Symptom:	Intermittently a successfully imported device is showing up as "Unknown" in LSAN zoning dialog.
Condition:	Observed in a routed environment.

Defect ID:	DEFECT000660172		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Device Management
Reported In Release:	Network Advisor14.2.2	**Technology:**	Device configuration (SAN)
Symptom:	Network Advisor migration failure observed.		
Condition:	When database password contained the special character "=" (equal sign).		
Workaround:	Use any of the special characters from the below list: ! @ # $ * ( ) Do not use "=" as it is considered as an assignment operator in Windows command prompt.		

Defect ID:	DEFECT000660328		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Device Management
Reported In Release:	Network Advisor14.4.2	**Technology:**	Device configuration (General)
Symptom:	"Move Node WWN" checkbox is enabled in the drop down menu for a selected Domain, Port Index (D,P).		
Condition:	Observed in Zoning dialog when creating a zone alias with Domain, Port Index (D, P) members.		

Defect ID:	DEFECT000660329		
Technical Severity:	High	**Probability:**	High
Product:	Brocade Network Advisor	**Technology Group:**	Device Management
Reported In Release:	Network Advisor14.4.2	**Technology:**	Device configuration (SAN)
Symptom:	Help is not launching in Real Time/Historical graph window under Flow Vision. Help is not launching in SAN inventory widget in the Dashboard.		
Condition:	Observed in Flow Vision and Dashboard windows.		
Workaround:	Refer to the PDF format of Network Advisor user manuals.		

Defect ID:	DEFECT000660332		
Technical Severity:	High	**Probability:**	Medium

Product:	Brocade Network Advisor	**Technology Group:**	Device Monitoring
Reported In Release:	Network Advisor14.4.1	**Technology:**	Dashboards
Symptom:	SAN Status dashboard widget is not available for custom dashboards.		
Condition:	Observed when a custom dashboard is created in Network Advisor.		

Defect ID:	DEFECT000660343		
Technical Severity:	High	**Probability:**	High
Product:	Brocade Network Advisor	**Technology Group:**	Device Management
Reported In Release:	Network Advisor14.4.2	**Technology:**	Device configuration (SAN)
Also Existed in Release:	Network Advisor 14.2.1, 14.3.x, 14.4.1		
Symptom:	Zone database entries in a peer zone may get deleted when user attempts to edit an alias of a principal member in a peer zone if there are ten or more principal members present in the peer zone.		
Condition:	When there are ten or more principal members present in a peer zone, and if those principal members contain one or more aliases, then an attempt to add or delete a member in any of those aliases will not succeed. Under this condition the Apply or OK button press will delete a random alias member instead of applying new changes; also, Edit Alias dialog will not close upon pressing the OK button. When this happens, if users save (OK/Apply button press on “Zoning” dialog) or activate the edited Zone Configuration (Activate button press on “Zoning” dialog), then it will delete already existing members of the alias. Which zone members get deleted is unpredictable and the number of members deleted corresponds to the number of times the OK or Apply button is pressed in the Edit Alias dialog.		
Workaround:	To edit an alias in a peer zone having ten or more principal members, first remove the alias from the peer zone, edit it as needed, add it back to the peer zone, and then save or activate the zone configuration.		
Recovery:	While in the Edit Alias dialog, if user notices that OK and Apply buttons are not working (i.e. changes are not applied and OK button does not close the dialog), then abort the zone edit operation completely by pressing Cancel button on “Edit Alias” dialog and then press Cancel button on “Zoning” dialog.		

Defect ID:	DEFECT000660344		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Device Management
Reported In Release:	Network Advisor14.4.2	**Technology:**	Device configuration (SAN)
Symptom:	Offline Zone merge failure observed in Network Advisor.		
Condition:	Observed when alias or zone name starts with a number or contains a special character.		

Defect ID:	DEFECT000660371		
Technical Severity:	Medium	**Probability:**	Medium

Product:	Brocade Network Advisor	**Technology Group:**	Monitoring
Reported In Release:	Network Advisor14.2.0	**Technology:**	Hardware Monitoring
Symptom:	Call home e-mail does not display the correct Product Type. It shows "999" instead of "148".		
Condition:	Observed for two BR-7840 switches when call home is configured.		

Defect ID:	DEFECT000660373		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Device Management
Reported In Release:	Network Advisor14.4.2	**Technology:**	Device configuration (SAN)
Symptom:	Peer member icon is being displayed in a standard zone when an alias is part of the standard zone and principal member of the peer zone.		
Condition:	Observed in a configuration similar to this: 1) Create an alias "a1" 2) Add alias "a1" to a peer zone as a principal member 3) Add alias "a1" to a standard zone		

Defect ID:	DEFECT000660374		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Device Management
Reported In Release:	Network Advisor14.4.2	**Technology:**	Device configuration (SAN)
Symptom:	Unable to add an offline member to an alias in Edit Alias dialog.		
Condition:	1.Create an alias from zone/LSAN dialog and right click on the alias 2. Hover the mouse cursor on tree option and click on the edit button 3. Click on Detached WWN text field 4. Observe that unable to type anything in detached WWN text field.		

Defect ID:	DEFECT000660376		
Technical Severity:	Medium	**Probability:**	High
Product:	Brocade Network Advisor	**Technology Group:**	Device Monitoring
Reported In Release:	Network Advisor14.4.2	**Technology:**	MAPS - Monitoring and Alerting Policy Suite
Symptom:	The "From Email Address" attribute is not supported for NOS devices. Similarly, the "From Email Address" attribute is not supported for FOS devices with pre-8.2.0 firmware versions. However, in above cases the "From Email Address" is enabled and accepts input which is not being saved. "Test Email" attribute is not supported for NOS and should be grayed out. However, when mixture of FOS and NOS devices are managed in Network Advisor, the "Test Email" will be enabled as it is supported for FOS.		
Condition:	Observed in "MAPS Email Setup" dialog with both NOS and FOS platforms managed.		

Defect ID:	DEFECT000657914		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade Network Advisor	**Technology Group:**	Management
Reported In Release:	Network Advisor14.4.0	**Technology:**	Configuration Fundamentals
Symptom:	IPEX Tunnel changes are not being applied in FCIP Tunnels dialog, and the only enabled button is the dialog remains the [Cancel] button.		
Condition:	Observed while editing an FCIP tunnel on 7840 switch.		

Defect ID:	**DEFECT000660410**		
Technical Severity:	High	**Probability:**	High
Product:	Brocade Network Advisor	**Technology Group:**	Device Management
Reported In Release:	Network Advisor14.4.2	**Technology:**	Device configuration (SAN)
Also Existed in Release:	Network Advisor 14.4.1		
Symptom:	A harmless pop up message is being displayed during Network Advisor installation: "Operating system is not recommended This application is not testing on this operating system. You can click OK to install anyway. For optimal performance, refer system requirements in user manual. Do you want to continue the installation?"		
Condition:	Observed on RHEL 6.9, RHEL 7.3, and OEL 7.3 OS platforms.		
Recovery:	Click OK and proceed with the installation.		

Defect ID:	DEFECT000660283		
Technical Severity:	Medium	**Probability:**	High
Product:	Brocade Network Advisor	**Technology Group:**	Management
Reported In Release:	Network Advisor14.4.1	**Technology:**	Configuration Fundamentals
Symptom:	Support save operation, triggered from Network Advisor fails with error “Operation Failed. Reason : 256 : Remote Host: Could not connect to remote host”		
Condition:	Issue observed in Network Advisor 14.4.x, when switch is configured to use one of the following cyphers: weak cyphers (CBC) only, i.e. 3des-cbc, aes128-cbc, aes192-cbc, aes256-cbc or both - weak (CBC) and strong (CTR) cyphers, i.e. aes128-cbc, 3des-cbc, aes192-cbc,aes256-cbc, aes128-ctr,aes192-ctr,aes256-ctr		
Workaround:	Configure the switches to use CTR cyphers only. For this run the following command on the switch: seccryptocfg --replace -type SSH -cipher aes128-ctr,aes192-ctr,aes256-ctr		