BROCADE
A Broadcom Company

Brocade Network Advisor 14.4.5

Release Notes v1.0

Copyright © 2020 Broadcom. All Rights Reserved. Broadcom, the pulse logo, Brocade, and the stylized B logo are among the trademarks of Broadcom in the United States, the EU, and/or other countries. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

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

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, to view the licensing terms applicable to the open source software, and to obtain a copy of the programming source code, please download the open source disclosure documents in the Broadcom Customer Support Portal (CSP). If you do not have a CSP account or are unable to log in, please contact your support provider for this information.

Use of all versions of Brocade Network Advisor (the “Software”) is subject to current the terms and conditions of the Brocade Network Advisor End User License Agreement (the “EULA”), as amended by Brocade from time to time. It is the user’s responsibility to understand and comply with the terms of the EULA. By downloading, installing, using, posting, distributing or otherwise making available the Software, you agree to be bound on an ongoing basis by the EULA as updated by Brocade from time to time.

Table of Contents

Chapter 1: Preface

1.1 Contacting Technical Support for Your Brocade® Product

For product support information and the latest information on contacting the Technical Assistance Center, go to https://www.broadcom.com/support/fibre-channel-networking/. If you have purchased Brocade® product support directly from Broadcom, use one of the following methods to contact the Technical Assistance Center 24x7.

Online	Telephone
For nonurgent issues, the preferred method is to log in to myBroadcom at https://www.broadcom.com/mybroadcom. (You must initially register to gain access to the Customer Support Portal.) Once there, select **Customer Support Portal** > **Support Portal**. You will now be able to navigate to the following sites: **Knowledge Search**: Clicking the top-right magnifying glass brings up a search bar. **Case Management**: The legacy MyBrocade case management tool (MyCases) has been replaced with the Fibre Channel Networking case management tool. **DocSafe:** You can download software and documentation. **Other Resources**: Licensing Portal (top), SAN Health (top and bottom), Communities (top), Education (top).	Required for Severity Level 1 (Critical) issues: Please call Fibre Channel Networking Global Support at one of the numbers listed at https://www.broadcom.com/support/fibre-channel-networking/.

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

- OEM/solution providers are trained and certified by Broadcom to support Brocade products.
- Broadcom 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 on this option, contact Broadcom or your OEM.

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

Chapter 2: Overview

Brocade Network Advisor 14.4.5 is a software maintenance release based on Brocade Network Advisor 14.4.4. All hardware platforms and features supported in Brocade Network Advisor 14.4.4 are also supported in Brocade Network Advisor 14.4.5.

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

Chapter 3: Software Features

3.1 New Software Features—Network Advisor 14.4.5

The following software features are new in this release:

- Network Advisor license key validation changes (see details in section 3.1.1)
- Fabric OS EULA enforcement during Fabric OS firmware download
- New OUI support: 38-BA-B0
- New operating system support: Windows Server 2019
- Defect fixes

3.1.1 Network Advisor Licensing changes

3.1.1.1 Network Advisor Installation

Starting with release 14.4.5, when installing Brocade Network Advisor, a transaction key instead of a license key is required.

During installation, when the configuration wizard prompts you to provide a serial number and a license key or transaction key, you must provide a valid serial number and transaction key.

The installed 14.4.5 product has functionality equivalent to the Enterprise licensed version and with no expiration date.

If you are migrating to Network Advisor 14.4.5 from an earlier version, after migration the installed Network Advisor is equivalent to the Enterprise version, even if you migrated from a Professional Plus edition.

Brocade Network Advisor 14.4.5 supports a maximum of 15,000 switch ports and 100 fabrics. Further discovery beyond this limit is restricted. After installation, you can click Help > License to display the current managed port and fabric counts

3.1.1.2 Migration From Earlier Releases

Brocade Network Advisor 14.4.5 supports only the Enterprise edition. Professional, Professional Plus, and Trial editions are not supported.

You can migrate to Network Advisor 14.4.5 from the Enterprise and Professional Plus editions. If you migrate from the Professional Plus edition, the new product has functionality equivalent to the Enterprise edition.

Migration is not supported for the Professional or Trial editions. Additionally, migration is not supported for the SMI Agent-only package.

Brocade Network Advisor 14.4.5 does not support a fresh installation of the SAN+IP package. However, if a pre-14.4.5 SAN+IP Enterprise or Professional Plus package is already installed, then that version of Network Advisor can be successfully upgraded to a SAN+IP 14.4.5 Enterprise package.

The following table summarizes the supported migration packages.

Current Software Package	Migration to 14.4.5 Supported?	Target Software Package
Enterprise Licensed	Yes	Enterprise
Enterprise Trial	No	N/A

Professional Plus	Yes	Enterprise
Professional	No	N/A
SAN + IP Enterprise Licensed	Yes	SAN + IP Enterprise
SAN + IP Enterprise Trial	No	N/A
SAN + IP Professional Plus	Yes	SAN + IP Enterprise
SAN + IP Professional	No	N/A
SMI Agent	No	N/A

3.2 New Software Features—Network Advisor 14.4.4

The following software features are new in this release:

- JRE update to v1.8u202
- Utility to split a large size file, like supportsave, into smaller chunks for easy transmission over the network
- Fabric OS® platform support
  - –Fabric OS 8.2.2
- Defect fixes

3.3 New Software Features—Network Advisor 14.4.3

The following software features are new in this release:

- Fabric OS® platform support
  - –Fabric OS 8.2.1
- RFEs:
  - –Support for Fabric OS 8.2.1 MAPS enhancements
  - –Brocade G610 Switch power supply and fan-in and fan-out thresholds
  - –Switch port violation reports (for both AMP and non-AMP)
  - –Multipath utilization for an LU WWID report (for AMP)
- Defect fixes

3.4 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

3.5 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 the Brocade X6 Director
- FCOE support for the FC32-64 blade
  - –Show the FCoE attributes for Ethernet ports
  - –Indicate the Ethernet/FC ports
  - –Support performance for FCoE devices
- NVMe support for Brocade X6 Directors and Brocade G630 Switches
  - –NVMe devices discovery
  - –NVMe Flow Vision
    - The **Add Flow Definition** dialog shows the **NSID** radio button.
    - The **Flow Vision** dialog is enhanced to include the **NSID** column.
    - The **NSID** column in the **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 ports
  - –Email enhancements
  - –Support to monitor the number of IP extension flows
  - –Category name changes from “FCIP Health” to “Extension Health”
  - –Category name changes from “GigE Port” to “Extension GE Port Health” category
- Miscellaneous Brocade Network Advisor 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 a file)
    - Manage File Transfer – GET REST API (to download a 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 aliases

- 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

3.6 Modified Software Features

Changes to Network Advisor licenses/packages:

- Network Advisor 14.4.1 and 14.4.2 do not support a fresh installation of the SAN+IP package. However, if a SAN+IP package is already installed on a pre-14.4.1/14.4.2 version, that version of the Network Advisor can be successfully upgraded to 14.4.
- Support for the fresh SAN+IP installation as well as for migration from SAN to SAN+IP is available in Network Advisor 14.4.3 and later.
- Network Advisor 14.4 supports neither a fresh installation of the IP only package nor a migration from pre-14.4 releases of the IP only package.

3.6.1 Security Vulnerability Fixes

This section lists the Common Vulnerabilities and Exposures (CVEs) fixes that are added in Network Advisor 14.4.3.

- CVE-2016-0793: Incomplete blacklist vulnerability in the servlet filter restriction mechanism in WildFly (formerly JBoss Application Server) before 10.0.0.Final on Windows allows remote attackers to read the sensitive files in the (1) WEB-INF or (2) META-INF directory via a request that contains (a) lowercase or (b) "meaningless" characters.
- CVE-2015-9251: jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.
- CVE – 2018-5996: Insufficient exception handling in the method NCompress::NRar3::CDecoder::Code of 7-Zip before 18.00 and p7zip can lead to multiple memory corruptions within the PPMd code, allows remote attackers to cause a denial of service (segmentation fault) or execute arbitrary code via a crafted RAR archive.
- CVE-2017-17969: Heap-based buffer overflow in the NCompress::NShrink::CDecoder::CodeReal method in 7-Zip before 18.00 and p7zip allows remote attackers to cause a denial of service (out-of-bounds write) or potentially execute arbitrary code via a crafted ZIP archive.
- CVE-2018-2815: Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Serialization). Supported versions that are affected are Java SE: 6u181, 7u171, 8u162 and 10; Java SE Embedded: 8u161; JRockit: R28.3.17. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying

data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).

- CVE-2018-2795: Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 6u181, 7u171, 8u162 and 10; Java SE Embedded: 8u161; JRockit: R28.3.17. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
- CVE-2018-2797: Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JMX). Supported versions that are affected are Java SE: 6u181, 7u171, 8u162 and 10; Java SE Embedded: 8u161; JRockit: R28.3.17. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
- CVE-2018-2799: Vulnerability in the Java SE, JRockit component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 6u181, 7u171, 8u162, 10 and JRockit: R28.3.17. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Java SE, JRockit executes to compromise Java SE, JRockit. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, JRockit, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 7.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).
- CVE-2018-2796: Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Concurrency). Supported versions that are affected are Java SE: 7u171, 8u162 and 10; Java SE Embedded: 8u161; JRockit: R28.3.17. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
- CVE-2018-2798: Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: AWT). Supported versions that are affected are Java SE: 6u181, 7u171, 8u162 and 10; Java SE Embedded: 8u161; JRockit: R28.3.17. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).

- CVE-2018-2783: Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 6u181, 7u161 and 8u152; Java SE Embedded: 8u152; JRockit: R28.3.17. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded, JRockit accessible data as well as unauthorized access to critical data or complete access to all Java SE, Java SE Embedded, JRockit accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).
- CVE-2018-2794: Vulnerability in the Java SE, JRockit component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 6u181, 7u171, 8u162, 10 and JRockit: R28.3.17. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Java SE, JRockit executes to compromise Java SE, JRockit. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, JRockit, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 7.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).
- CVE-2018-2942: Vulnerability in the Java SE, JRockit component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 6u181, 7u171, 8u162, 10 and JRockit: R28.3.17. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Java SE, JRockit executes to compromise Java SE, JRockit. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, JRockit, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 7.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).
- CVE-2018-2972: Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JNDI). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151; JRockit: R28.3.16. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: This vulnerability applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:L).
- CVE-2018-2952: Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Concurrency). Supported versions that are affected are Java SE: 6u191, 7u181, 8u172 and 10.0.1; Java SE Embedded: 8u171; JRockit: R28.3.18. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).

- CVE-2014-0050: MultipartStream.java in Apache Commons FileUpload before 1.3.1, as used in Apache Tomcat, JBoss Web, and other products, allows remote attackers to cause a denial of service (infinite loop and CPU consumption) via a crafted Content-Type header that bypasses a loop's intended exit conditions.
- Defect BNA-654882: HTTP Security Header Not Detected. "Content-Security-Policy HTTP Header" and "Public-Key-Pins HTTP Header" were missing on ports 443 and 8443.
- CVE-2015-7804: Off-by-one error in the phar_parse_zipfile function in ext/phar/zip.c in PHP before 5.5.30 and 5.6.x before 5.6.14 allows remote attackers to cause a denial of service (uninitialized pointer dereference and application crash) by including the / filename in a .zip PHAR archive.
- CVE-2016-2334: Heap-based buffer overflow in the NArchive::NHfs::CHandler::ExtractZlibFile method in 7zip before 16.00 and p7zip allows remote attackers to execute arbitrary code via a crafted HFS+ image.
- CVE-2016-2335: The CInArchive::ReadFileItem method in Archive/Udf/UdfIn.cpp in 7zip 9.20 and 15.05 beta and p7zip allows remote attackers to cause a denial of service (out-of-bounds read) or execute arbitrary code via the PartitionRef field in the Long Allocation Descriptor in a UDF file.

Chapter 4: New Hardware

The following sections list new hardware introduced with the Network Advisor 14.4 release.

4.1 New Devices

Product Name	Device Name
Brocade G630 Switch	Gen 6 (32Gb/s) Fibre Channel 128-port fixed-port switch

4.2 New Blades

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

Chapter 5: Supported Operating Systems, Browsers, and JRE Versions

5.1 Supported Operating Systems

- Windows Server 2008 R2 SP1 Datacenter, Standard and Enterprise
- Windows Server 2012 R2 Standard, Datacenter
- Windows Server 2016 Datacenter, Standard
- Windows Server 2019 Datacenter, Standard
- Windows 8.1 Enterprise (Client only)
- Windows 10 Enterprise
- MAC OS 10.12 (Sierra) (Fabric Insight Portal only)
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7
- SUSE Linux Enterprise Server 11.3
- SUSE Linux Enterprise Server 12.0
- Oracle Linux 7.6
- Oracle Linux 7.7

5.2 Supported Browsers

Recommended browser versions:

- Chrome 78 and later (Windows, MAC OS)
- Edge 44 (Windows 10 only)
- Firefox 70 and later (Windows only)
- Internet Explorer 11 and later (Windows 10 only)

5.3 Supported JRE Versions

Network Advisor Version	JRE Version Supported
14.4.5	JRE 1.8u202

NOTE:

1. The Web Tools launch from Network Advisor is also supported for the above combination.
2. Applicable only to Web Tools 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 Web Tools will be blocked and the "`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 installed, an attempt to launch the Web Tools will be blocked and the "`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.

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 the JRE Support table. Beyond the JRE expiration date you will see the message "`Your Java version is out of date`" when you 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 proceeding 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?`"

4. JRE 1.8.0 update 66 and later support begin with the following Fabric OS versions:
   –Fabric OS 7.4.0
   –Fabric OS 8.0.0
   –Fabric OS 8.0.1
   –Fabric OS 8.1.0x
   –Fabric OS 8.1.1
   –Fabric OS 8.2.0x
   –Fabric OS 8.2.1x
   –Fabric OS 8.2.2x

- Apply the following workaround on a computer when launching Web Tools using a browser or the Network Advisor Remote client for all Fabric OS versions earlier than those listed above:

  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:

  a. Navigate to the Network Advisor installation directory.

  On Windows, navigate to `<Network Advisor install directory>\jre64\lib\security`. On

  Linux, navigate to `<Network Advisor install directory>/jre/lib/security`.

  b. Open the `java.security` file and change the `jdk.certpath.disabledAlgorithms=MD2, RSA keySize < 2048` value from 2048 to 256.

  For example: `jdk.certpath.disabledAlgorithms=MD2, RSA keySize < 256`.

NOTE No additional JRE is required on the system with the Network Advisor server to access the Server Management Console (SMC) or the local client. The remote client requires Oracle JRE. For the current supported JRE version for the management application, see the table at the beginning of this section.

Chapter 6: Hardware Support

NOTE For IP product information, refer to the *Brocade Network Advisor SAN+IP User Manual*

6.1 Supported SAN Devices

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

- 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:

1. Discovery of a secure Fabric OS fabric in strict mode is not supported.
2. To ensure that a configuration is fully supported, always check the appropriate SAN storage or blade server product support page to verify support for specific code levels on specific switch platforms before installation 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 2.2.0 for Brocade Network Advisor 14.4. AMP OS 2.1.0 is the minimum *supported* version for compatibility with Brocade Network Advisor 14.4 and is intended only for temporary use until upgrading to AMP OS 2.2.0.

Device Name	Terminology Used in Documentation
Brocade 300 Switch	24-port, 8Gb/s FC switch
Brocade 5424 Embedded Switch	Embedded 24-port, 8Gb/s switch
Brocade 5431 Embedded Switch	Embedded 16-port, 8Gb/s stackable switch
Brocade 5450 Embedded Switch	Embedded 16-port, 8Gb/s switch
Brocade 5460 Embedded Switch	Embedded 24-port, 8Gb/s switch
Brocade 5470 Embedded Switch	Embedded 24-port, 8Gb/s switch
Brocade 5480 Embedded Switch	Embedded 24-port, 8Gb/s switch
Brocade 6505 Switch	24-port, 16Gb/s edge switch
Brocade M6505 blade server SAN I/O module	24-port, 16Gb/s blade server SAN I/O module
Brocade 6510 Switch	48-port, 16Gb/s switch
Brocade 6520 Switch	96-port, 16Gb/s switch

Device Name	Terminology Used in Documentation
Brocade 6542 blade server SAN I/O module	48-port, 16Gb/s blade server SAN I/O module
Brocade 6543 blade server SAN I/O module	24-port, 16Gb/s blade server SAN I/O module
Brocade 6545 blade server SAN I/O module	26-port, 16Gb/s blade server SAN I/O module
Brocade 6546 blade server SAN I/O module	24-port, 16Gb/s blade server SAN I/O module
Brocade 6547 blade server SAN I/O module	48-port, 16Gb/s blade server SAN I/O module
Brocade 6548 blade server SAN I/O module	28-port, 16Gb/s blade server SAN I/O module
Brocade 7800 Switch	8Gb/s extension switch
Brocade 7840 Switch	16Gb/s 24-FC port, 18GbE port switch
Brocade DCX 8510-4	16Gb/s 4-slot backbone chassis

Device Name	Terminology Used in Documentation
Brocade DCX 8510-4 with FC16-32, FC16-48 and FC16-64 blades	16Gb/s 4-slot backbone chassis with 16Gb/s 32-port and 16Gb/s 48-port and 16Gb/s 64-port blades
Brocade DCX 8510-8	16Gb/s 8-slot backbone chassis
Brocade DCX 8510-8 with FC16-32, FC16-48 and FC16-64 blades	16Gb/s 8-slot backbone chassis with 16Gb/s 32-port and 16Gb/s 48-port blades and 16Gb/s 64-port blades
Brocade X6-4 Director	32Gb/s 4-slot backbone chassis
Brocade X6-8 Director	32Gb/s 8-slot backbone chassis
Brocade Gen 6 platform (32Gb/s) fixed-port switch (Brocade G610)	24-port, 32Gb/s switch
Brocade Gen 6 platform (32Gb/s) fixed-port switch (Brocade G620)	64-port, 32Gb/s switch
Brocade Gen 6 platform (32Gb/s) fixed-port switch (Brocade G630)	128-port, 32Gb/s switch
FC32-64 blade	32Gb/s 64-port blade
FC32-48 port blade	32Gb/s 48-port blade
SX6 extension blade	32Gb/s router extension blade

6.2 Supported Adapters

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

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

For Brocade adapters, HCM 3.2.4 is integrated with Brocade Network Advisor.

Adapter Types		Driver/Firmware Versions
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

Adapter Types		Driver/Firmware Versions
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 x 8 to 32Gb Fibre Channel Adapter – SFP+ QLE2764 Quad-port PCIe 3.0 x 8 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

6.3 Supported vCenter Versions

Virtual Machine Management: vCenter and ESXi Supported Versions.

ESXi	6.0, 6.5
VCenter	6.0, 6.5

Chapter 7: Software Upgrade and Downgrade

7.1 Migration Path

Migration to 14.4.5 is supported from the following previous releases:

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, 14.4.2, 14.4.3, 14.4.4

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.
2. All Network Advisor editions are supported only on 64-bit servers. To migrate Enterprise and Professional Plus editions to a 64-bit server, refer to the "Pre-migration requirements when migrating from one server to another" section of the installation and migration guide.
3. Refer to supported migration paths in the installation and migration guide for migration paths from pre-14.2.x releases.
4. Refer to supported migration paths in the installation and migration guide for SMI-agent-only migration paths.
5. Make sure that the minimum free space is 1.5 times the available size of the Network Advisor data folder (`<Install_Home>\data`) for performing migration for the servers with a large amount of Performance, Events, and Flow Vision data in the database.
6. The fresh install for SAN+IP support has been removed in 14.4.1 and 14.4.2 releases. Hence migration from SAN to SAN+IP support has also been removed in 14.4.1 and 14.4.2.

   Network Advisor 14.4.3 and later supports the fresh installation of SAN+IP as well as the migration from SAN to SAN+IP.
7. IP-only installation is not supported with 14.4.x.
8. Follow the instructions below to perform AMP migration from 14.2.x/14.3.x to 14.4.x:

   a. Start with the source version running Brocade Network Advisor 14.2.x/14.3.x.

   b. Upgrade from AMP OS 2.1.0 to AMP OS 2.2.0 (after successful Brocade Network Advisor migration).

7.2 Upgrade and Downgrade Considerations

If the OEM name for any of the switch models has changed from one release to another, you will need to change the properties file after migration. To see these new names, change the existing model name to that of the new name in the `oem-switch-model-mapping.properties` file located in the `conf` folder of the Brocade Network Advisor home location, and restart the server for the changes to take effect.

A Brocade Network Advisor downgrade to previous versions is not supported.

7.3 Before Upgrading or Installing the Software

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

7.4 System Specifications—Requirements and Recommendations

7.4.1 Memory, Host, and Disk Space Requirements

Memory requirements are applicable only when there are no other applications running on the Network Advisor server. Paging space should be equal to or should exceed the physical memory size.

NOTE: When Network Advisor is installed on the VM, the system resources must be dedicated to the VM.

7.4.2 System Specifications for Network Advisor without the Analytics Monitoring Platform

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

Table 1: Memory, Host, and Disk Space Requirements for a Remote Client

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

The following table summarizes the minimum and recommended system requirements for server (plus 1 client) installation. Recommended specifications will provide better Network Advisor performance.

Table 2: System Requirements for Server (Plus 1 Client) Installation per Edition

Resources	Enterprise Edition
Installed Memory	6 GB (recommended 12 GB)
Processor Core Count (including physical and logical cores)	2 (recommended 4)
Disk Space	20 GB (recommended 30 GB)

Table 3: System Requirements for Server (Plus 1 Client) Installation per Network Size

Resources	Small	Medium	Large
Installed Memory	16 GB	16 GB (recommended 32 GB)	16 GB (recommended 32 GB)
Processor Core Count (including physical and logical cores)	2 (1 physical, 2 virtual) (recommended 4: 2 physical, 4 virtual)	4 (2 physical, 4 virtual) (recommended 8: 4 physical, 8 virtual)	8 (4 physical, 8 virtual) (recommended 12: 6 physical, 12 virtual)

Resources	Small	Medium	Large
Disk Space	20 GB (recommended 30 GB)	80 GB (recommended 100 GB)	100 GB (recommended 150 GB)

NOTE:

1. If you use sFlow, it is recommended that you add an additional 100 GB of disk space.
2. It is recommended that you add an additional 40 GB of disk space for the default temporary directory.
3. 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.

7.4.3 System Specifications for Network Advisor with the Analytics Monitoring Platform

Recommended System Specifications

Resources	5K Flows	10K Flows	20K Flows	40K Flows	60K Flows	80K Flows	> 100K Flows
Installed Memory	16 GB (recommended 32 GB)	24 GB (recommended 32 GB)	32 GB	32 GB	32 GB (recommended 48 GB)	64 GB	64 GB (recommended 96 GB)
Processor Core Count (physical, logical)	8 (4 physical, 8 logical) (recommended 12: 6 physical, 12 virtual)	12 (6 physical, 12 logical) (recommended 16: 8 physical, 16 virtual)	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) (SSD recommended)	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 Specifications for Remote Java Client with AMP

This is applicable for both the desktop client and the 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

NOTE:

1. It is recommended to use only the remote client for the Brocade Network Advisor server when managing the Brocade Analytics Monitoring Platform with more than 20K flows.
2. When managing the Brocade Analytics Monitoring Platform, Brocade Network Advisor supports a maximum of 8K switch ports in a fabric.

7.4.4 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 that you use the following memory settings for your operating system.

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

7.4.5 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:

- In Enterprise edition, 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:
  – Increase the server memory size. You can configure the server memory size from the **Options** dialog in the **Memory Allocations** pane. For instructions, refer to the Network Advisor user manual or online help.
  – Increase the PostgreSQL database shared buffers memory allocation to 1024 MB by editing the `Install_Home\data\databases\postgresql.conf` file.

7.5 Installing Network Advisor

Installation instructions are provided for the following operating systems:

- Microsoft Windows
- Linux

NOTE:

1. It is not recommended to run any other application on the Network Advisor server.

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

7.5.1 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.

7.5.2 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.

7.5.3 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:

1. Select **Start > Programs > Network Advisor 14.4.x > Network Advisor 14.4.x**.
2. Click the **Desktop** icon.
3. Launch the command prompt, navigate to `<Install Home>/bin`, type **dcmclient**, and press **Enter**.

On Linux:

1. Click the **Desktop** icon.
2. Launch a 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 steps below to launch the client from a Web browser.

NOTE:

1. The web-start remote client is supported with the JRE versions listed in the “Supported JRE Versions” section of this document. The supported JRE version must be installed on the remote client system before establishing a server connection.
2. The remote client can be launched in the following ways:

1. Open a browser window and enter the Network Advisor server host name 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 SSL is 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.

2. Click **Desktop Client**.

   The Network Address web-start page displays.

3. Choose one of the following options:
   – Click the **Web Start the Client** link.

     The **Log In** dialog displays.

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

4. To launch the Network Advisor client from a Web browser, complete the following steps:
   a. 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 SSL is 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.

   b. Click **Desktop Client** to launch the Java client from any page of the Web client.

   The **Log In** dialog displays.

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

5. To turn on Java content in the browser, follow the steps below:
   a. Launch the Java Control Panel (refer to http://java.com/en/download/help/win_controlpanel.xml to locate the Java Control Panel application on Windows).
   b. In the Java Control Panel, click the **Security** tab.
   c. Select the **Enable Java Content** check box in the browser. This will enable the Java plug-in within the browser.
   d. 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.
   e. Launch Element Manager from Network Advisor client.

Chapter 8: Limitations and Restriction

8.1 Scalability

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

Table 4: Supported Scalability Limits by Network Advisor Edition

	Enterprise Edition		
	Small	**Medium**	**Large**
SAN Switch Ports	2000	5000	15,000
SAN Switches and Access Gateways	40	100	400
SAN Devices	5000	15,000	40,000
SAN Fabrics	25	50	100
Managed Hosts	20	100	400
vCenters	1	5	10
VMs (includes powered-down VMs)	1000	5000	10,000
ESX Hosts	200	1000	2000

NOTE:

1. Virtual Fabrics are counted as fabrics when calculating the managed count limits.
2. The supported network latency between the Network Advisor server and the client or server and devices is 100 ms.

8.2 Compatibility and Interoperability

Discovery of QLogic-branded Brocade adapters is not supported.

Chapter 9: Important Notes

9.1 Important Notes for Changing the IP Address of the Network Advisor Server

Use the following procedure to change the IP address of the Network Advisor server:

1. Change the Network Advisor server IP address using server system utilities.
2. Launch the Network Advisor Configuration wizard, select the new IP address, and apply changes.
3. Reboot the server.

If the above steps are not performed in the specified sequence, or if any system level changes, such as MAC address, UUID, hostname, or S/N changes, are performed on the Network Advisor server, then the Network Advisor server may fail to start after a server reboot.

If this occurs, then you can resolve this problem by using the following procedure:

1. Check the file “<Network Advisor _install_home>\jboss\standalone\configuration\standalone-dcm.xml” to see if ***redirect-socket="https"*** is present in the following line:
   <http-listener name="default" socket-binding="http" ***redirect-socket="https"*** max-post-size="9999999999"/>
2. If ***redirect-socket="https"*** is missing, then add it and save the file.
3. Launch the Network Advisor Configuration wizard and select the new/correct IP address, and then apply the changes.
4. Restart the Network Advisor server.

To avoid the possibility of missing parameter in the "standalone-dcm.xml" configuration file after system reboot, as a preventive measure you can disable the HTTP redirect option. After disabling that option, to launch Network Advisor remote/web client you will have to use “https://< Network Advisor server IP address>” instead of typing just the Network Advisor server IP address.

If you wish to disable HTTP redirect option then you can use the following procedure:

1. Launch the Network Advisor Configuration wizard.
2. Uncheck “Redirect HTTP Requests to HTTPS”.
3. Finish the wizard and apply the changes.

This will restart the services, and will also remove the HTTP redirect-related configuration line from the “standalone-dcm.xml” file.

9.2 Known Issue with Internal SCP/SFTP Service

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

If the 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 two workarounds.

Workarounds:

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 the pre-14.4.0 (Network Advisor version before 14.4.0) 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 the pre-14.4.0 partially uninstalled location as follows:

      i. 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`

      ii. Restart Network Advisor services.

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

      Log in to the switch as admin and delete the Network Advisor server IP address entry by issuing 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/Host name 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, issue the following command:

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

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

   Log in as admin to the switch where the firmware download or supportsave has failed and delete the Network Advisor server SSH host name/IP address entry by issuing 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/Host name 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, issue the following command:

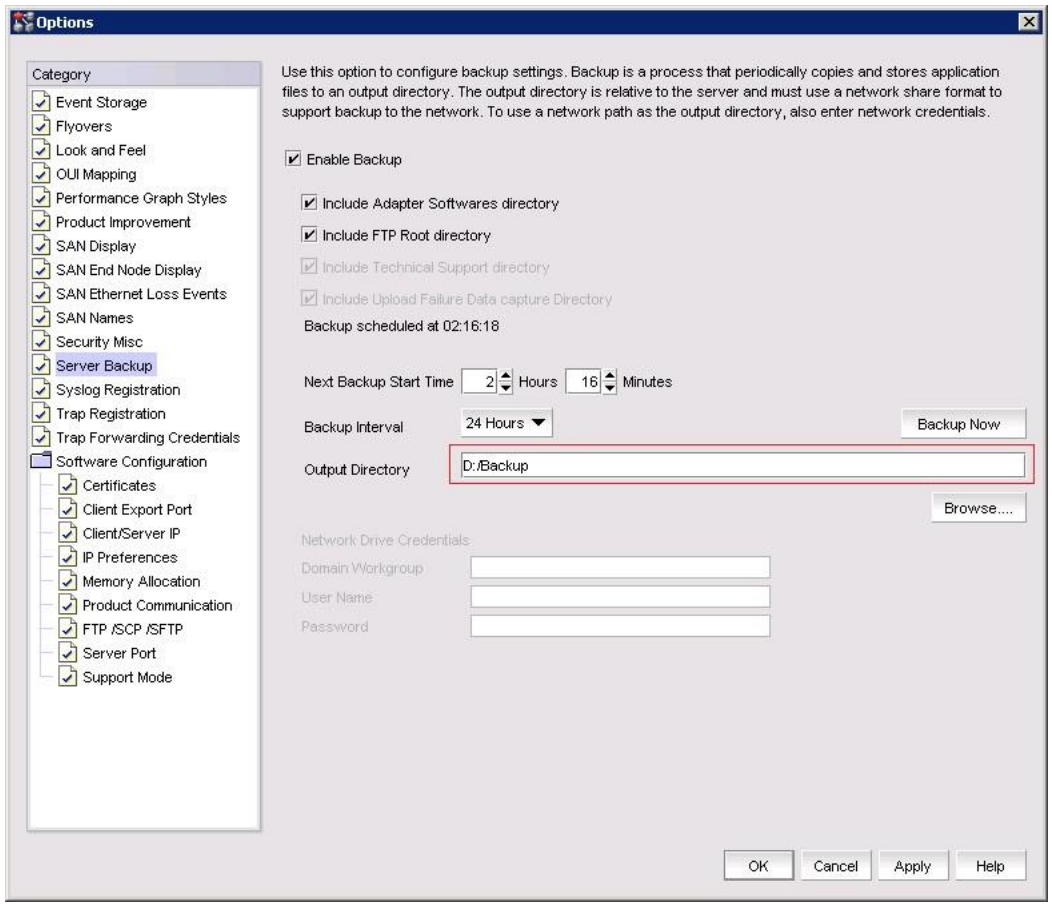
     ```
     sw0:FID128:admin> sshutil delknownhost -all Please
     Confirm with Yes(Y,y), No(N,n) [N]: y
     ```

9.3 Important Notes for Managing the Brocade Analytics Monitoring Platform

Backup and Restore Recommendations:

1. With AMP discovered in Network Advisor, for backup it is recommended that you use with an external device since backing up to CD is not the recommended method. The usable capacity of a CD is:
   – Approximately 700 MB, which must be replaced when full. It is recommended that you configure the backup system to target a hard drive or a network drive.
   – Note that the amount of space required for each backup is 1/10th of the size of the Brocade Network Advisor installation directory, and the backup process takes about 1.5 hours for 100 GB of data.
2. By default, the Network Advisor server backup is scheduled for every day: a backup every 24 hours. With AMP discovered in the Network Advisor, since the data size will be huge:
   – If the user needs better Brocade Network Advisor performance, it is recommended to disable the default scheduled backup by disabling the **Enable Backup** option (also shown in the figure below) and triggering a manual backup on a weekly basis or based on the need by enabling the **Enable Backup** check box and selecting the **Backup Now** button.

– If the user needs a daily data backup, the performance of the Brocade Network Advisor will be impacted due to the backup process. Based on the need, the backup can be planned.



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

   When the issue happens, do the following:

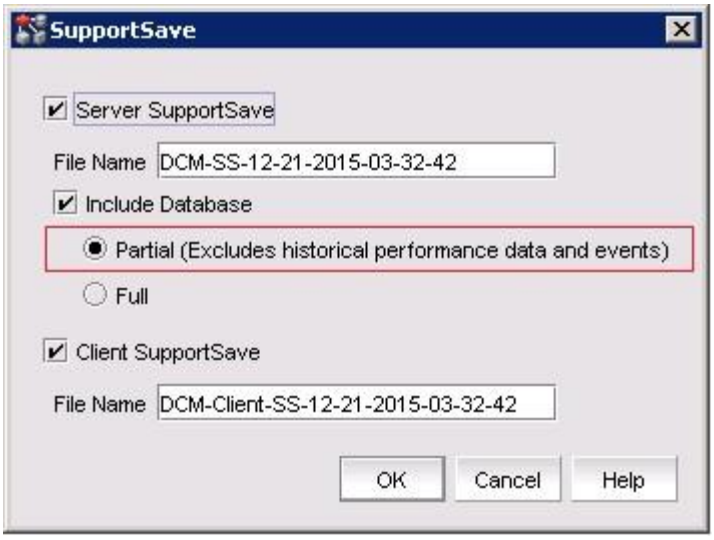
   a. Roll back to the source version.

   b. Open the **Server Management Console** (SMC) and stop all services.

   c. Install the destination version and do the migration.

Support Save Recommendations

With AMP discovered in Network Advisor, for capturing the server and client support save data, it is recommended to select the **Partial** option, which excludes 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 the Brocade Network Advisor installation folder/data. Note that it takes approximately 2 hours to complete the migration for a 100G data folder size.

Example:

Size of the Brocade Network Advisor installation folder/data is 500 GB.

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

Time for completing migration would be approximately 10 hours.

Performance Considerations for Dashboard

- When there are more than 30k flows monitored in Brocade Network Advisor:
  - It is recommended to select a 30-minute or 1-hour time scope for better performance of the drill-down graphs/dialogs.
  - The drill-down graph/dialog launch will take around 5 minutes when the user selects a 6 hours/12 hours/1 day time scope.
- An AMP device should be discovered by only one Brocade Network Advisor server.
- It is highly recommended to use a unique FID for all AMP logical switches discovered in Brocade Network Advisor.
- The port demand rate and ROS measures calculation cannot be done for NPIV ports and hosts connected to the AG.
- The Pending IOs widget shows data only for physical ports.
- Data plotting in Port Investigate view when navigating from the Dashboard/Inventory detailed view:
  - Plotting the first data point for ROS measure takes up to 40 seconds.
  - The time stamp for ROS, Pending IOS may not match other port measures (for example, TX%, RX%). Real-time plotting happens based on the device time stamp.
  - Port-level measure plotting may take up to 1 minute in Port Investigate view.
- The MAPS events purging limit is changed to 50,000 by default in Network Advisor 14.3.x (Earlier this limit was set to 10 millions). The user can customize this purging limit by changing **Maximum Events** in the **Event Storage** page from the **Option** dialog.
- When the user drills down a violation bar, the violation dialog is empty when those MAPS events are 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.
- The 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 for 1 to 2 minutes until the deployment is completed. Editing the collection within this time may lead to showing errors in banner "`Group name already exists`."
- If headless installation is done, AMP manageability will not be enabled by default. This must be enabled explicitly by running the `enableamp.bat` script from the following location:

  `<Network Advisor Home>\monitor\bin`
- After deleting the Threshold widget, the user cannot view the generated report output. So it is recommended not to delete the Threshold sub-widget.
- With a symmetric fabric (the same flow configuration in two or more fabrics):
  - In the Threshold widget, an incorrect detail is displayed for the **Occurrence** column.
  - On applying the name for the port/flow filter of a single fabric, a report is generated for all symmetric fabrics.
- The user can launch the Web client with an IPv6 address only from the Chrome browser. The Web client launch fails with Edge and Internet Explorer with IPv6 addresses.
- A delay of 2 to 3 minutes may be observed while investigating MPIO path utilization for historical data. During this delay, the network flows page shows a hyphen (-) in place of the path utilization percentage.
- The BB Credit Zero measure in port historical investigate is plotted with the unit of errors. The user must select the **Unit/ Sec** option from the thick client **Options > Performance Graph Styles > Unit Display**.
- While investigating the ROS measure for multiple symmetric flows, the same value will be plotted for all flows. The user must select an individual flow to view a specific flow's ROS value.
- Real-time stats are not supported for path utilization. When a user selects real-time for the measure "path utilization," switching back to historical is disabled. The workaround is to switch to some other measure and navigate to historical.
- Upon configuring the IT/ITL resource limits to those of the currently used count, the user must reset the sys_mon_analytics_flow. In this case, refreshing the switch details page does not update with the changed limits. The workaround is to go to some other page and get back to the 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:

  - Replace the previous version's certificate with a new self-signed certificate, use **Server > Options > Software Configuration > Certificates > Keystore Certificate**, and choose **Replace** in the drop-down. Then restart Network Advisor services, make sure that the client is logged in, and migrate to 14.4x.
  - Replace the certificate with a new signed certificate that conforms to the following standard:
    - RSA key size not less than 2048
    - Signature algorithm sha256withRSAEncryption
  - Remove the disabled less secure algorithms restricted in 14.4.x in the `<Network Advisor Home>\jre64\lib\security\java.security` file under disabled algorithms, which are SHA1 and RSA Key size < 2048.

- When Network Advisor is managing AMPOS 2.2.0 and multipath is present in the SAN, the Fabric Insight Portal stops reporting data after the first few samples for all flows (see DEFECT000660488 in this document).
- Restoring backup from AMP enabled server fails due to incomplete backup from some database tables (BNA-800647).

  To avoid this, disable scheduled backup and take a manual backup as follows:

  - To disable the scheduled backup:
    - Server --> Options--> Server Backup
    - Uncheck "Enabled Backup"
  - To take a manual backup:
    - Open terminal in Network Advisor server (with root / administrator privilege)
    - Navigate to "<Network_Advisor>\monitor\bin" folder
    - Execute the command "service dcmmonsvc stop"
    - This will stop the Network Advisor monitor services
    - Launch BNA client, go to Server -> Options -> Server Backup

- Confirm the output directory which will be target directory for the backup. Make sure the directory has read/write permissions.
- Take backup by clicking on "Backup now" button
- Ensure the backup is collected in the output directory

– To bring back the AMP service:
- Navigate to "<Network_Advisor>\monitor\bin" folder.
- Execute the command "service dcmmonsvc start "

9.4 Important SAN Notes

- While pushing larger zone configurations, make sure to reserve enough space in the zone database to accommodate the HDR size of all the LS and the actual committed configuration within the zone database maximum size. It is recommended to add zones gradually. Pushing a zone database with a size greater than the maximum zone database size will set the available zone database size to a negative value, which in turn causes a deadlock where any zone operation will not work.
- Starting with FOS 8.1.0x, 16 LS support is provided on each Brocade 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 the preferred protocol. The workaround is to use the FTP/SFTP option in Brocade Network Advisor.
- SNMPv3 using the AES256 algorithm may not work with certain passwords since there could be a mismatch for encryption/decryption of passwords. For example: "pass1", "xyz12mo" fails, whereas "xyz12" works. This is because the AES256 algorithm is not a standard implementation.
- Trying to move 200+ ports to a logical switch with the **Reset to Default** option selected results in an operation timeout.
- During installation, if the Network Advisor database initialization fails on the Windows operating system, the user must verify access to the drive on which the installation is performed. If only the user "Administrator" has access to the drive, required permissions should also be provided to "Authenticated Users" and then the installation should be continued.
- The FCIP links will not be shown in the topology for tunnels with degraded circuits.
- IP ping, IP route, and trace route are not supported on the Brocade 7840/SX6.
- Network Advisor uses SNMPv3 by default to discover SAN products. If required, the user can select the **Manual** option in the **Discovery** dialog and choose SNMPv1 for discovery, as in the case of AG discovery, which requires the 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 following Java properties:

  On Windows:

  `C:\Users\<logged-in user name>\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 following 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`

- The real-time graph will not display proper data for FCIP tunnels when the polling interval is 10 seconds. The user must keep a 20 second polling interval in the graph to see the correct data for the Brocade 7840/SX6.
- Emulex: HTTPS discovery for an ESXi host will work only with certificate import.

  Workaround:

  Perform the following two steps to work around this issue.

  a. Add the following line in the `<User Home>/.java/deployment/deployment.properties` file:

     `deployment.expiration.check.enabled=false`

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

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

  b. Launch the Java Control Panel using the following command, and click the **Ok** button:

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

- If Network Advisor is installed on the Linux operating system, the Fabric OS Element Manager and HCM cannot be launched when the client is launched using the `dcmclient` script available in the Network Advisor installation folder. The **Launch in Context** (LIC) dialogs from the SMIA configuration tool (launched from the **Server Management Console**) also cannot be launched (for example, **Discovery** dialog, **Options** dialog). To use the above features on Linux machines, launch the Network Advisor client from a browser (after installing the supported JRE 7 version), pointing to the Network Advisor server installed on that machine.

  Workaround:

  Perform the following steps to work around this issue.

  – Add following line in the `<User Home>/.java/deployment/deployment.properties` file:

    `deployment.expiration.check.enabled=false`

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

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

  – Launch the Java Control Panel using following command, and click **OK**.

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

- Secure Syslog is not supported from Network Advisor.
- SAN Configuration Purge Backup is enabled automatically when “Enable Scheduled Backup” is set and remains enabled after disabling the scheduled backup.
- The user is not recommended to perform write operations such as delete or enable/disable on FCIP tunnels that have circuits with different IDs.
- When the CIMOM server is bound to the host name, the SLP service fails to get registered.

  Workaround:

  To overcome this issue, the user can bind the CIMOM server to the IP address instead of the host name.

- A firmware upgrade will happen serially for Brocade 7840s with HA-configured tunnels between them. For parallel download on Brocade 7840s, use the CLI.
- FCIP circuit trace route verification fails when attempted from Network Advisor.
- Launching Web Tools is not supported for the Brocade Analytics Monitoring Platform.
- The SAN Inventory widget in the default dashboard shows “`Error loading the data`” on creating and deleting custom dashboards inconsistently when managing more than 9000 ports. The user must relaunch the client to see the data again.

- Do not enable the **Use SSL 2.0 compatible ClientHello format** setting in the Java Control Panel on the Network Advisor Client machine since it will interfere with the remote client launch.
- For AMP users with a scaled number of AMP flows, it is recommended that you disable daily database backups for better Network Advisor performance with the AMP case.
- If the local server has JRE version 1.8u112, the links in the **Configure SMIA Agent** dialog in the **Server Management Console** will not launch.

  Workaround:

  Uninstall JRE version 1.8u112 or install the latest supported JRE version.

- While generating a report from the Microsoft Windows command prompt and saving the report in a non-default location, the report output directory path should not end with a backslash ("\"), or the backslash character should be prefixed with a forward slash ("/"). For example: `-o "c:\/"`.
- As per the Fabric OS design, all three AAA servers (RADIUS, ADLDAP, TACACS+) must be configured together. All three AAA server settings should be present in the configuration file (from COMPASS) when you want to add any one server additionally (RADIUS, ADLDAP, TACACS+). This can be achieved in COMPASS using the **Import from Switch** and **Edit** options.

  For example, let's say that all three AAA servers are configured on the switch. From COMPASS, if you try to push only the ADLDAP configuration during the sync operation, already configured RADIUS and TACACS+ configurations on the switch will be removed. The template configuration present in the configuration file will be downloaded to the 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 zones.
- When hosts, vCenters, SMIA clients or SSL/TLS email servers do not have certificates with the SHA2 algorithm and the RSA key size > 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 key size < 2048 from the disabled algorithms list in the `java.security` file present on the Network Advisor server as follows:

  – Navigate to the `<Network Advisor Home>\jre64\lib\security` directory to open the `java.security` file and remove SHA1 and RSA key size < 2048 from the disabled algorithm list:
  `jdk.tls.disabledAlgorithms=SSLv3, RC4, MD5withRSA, MD5, DES, 3DES, RC2, DESede, DHE, DH, ECDH, SHA1, DSA, DH keySize < 1024, \ EC keySize < 224, DES40_CBC, RC4_40, RSA keySize < 2048, 3DES_EDE_CBC,TLSv1,TLSv1.1`
  – Restart all Network Advisor services through the Service Management Console.

- Parallel firmware upgrade of fixed-port switches may cause traffic disruption. A serial firmware download is suggested in this case. For more information, refer to the SAN Device Configuration > Firmware Management > Firmware upgrade or downgrade considerations chapter in the SAN user manual.
- 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 be alerted about such events. If Call Home filters are configured before migrating from a previous Network Advisor version, there will be no change in behavior. However, if Call Home is configured for the first time or is currently using the default configuration, MAPS-1003 events will trigger Call Home. If this behavior is not desired, Call Home filters must be configured to exclude MAPS-1003 events.
- Zone database entries in a peer zone may be deleted when a user attempts to edit an alias of a principal member in a peer zone if there are 10 or more principal members present in the peer zone.

  This is observed when there are 10 or more principal members present in a peer zone, and if those principal members contain one or more aliases, an attempt to add or delete a member in any of those aliases will not succeed. Under this condition, pressing the **Apply** or **OK** button will delete a random alias member instead of applying new changes; also,

the **Edit Alias** dialog will not close upon pressing the **OK** button. When this happens, if users save (by pressing the **OK**/
Apply button in the **Zoning** dialog) or activate the edited zone configuration (by pressing the **Activate** button in the **Zoning** dialog), then already existing members of the alias will be deleted. Which zone members are 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 the user notices that the **OK** and **Apply** buttons are not working (that is, changes are not applied, and the **OK** button does not close the dialog), then abort the zone edit operation completely by pressing the **Cancel** button on the **Edit Alias** dialog and then pressing the **Cancel** button in the **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.

This issue is tracked by DEFECT000660343 (see the defect details below in this document).

- The SMIA-supported launch in context-based Network Advisor features requires external JRE for the local client.

- Network Advisor does not display some warning messages during FOS firmware downgrade (BNA-800734).
  In particular, Network Advisor does not display the following warning message:
  `"ADDITIONAL_REBOOT_HRPN ="HCL is not supported on downgrade to 8.2.0x or prior firmware versions. Perform additional blade slot power cycle on all SX6 blades post firmware downgrade."`
  The extension platform has a requirement of additional switch reboot or blade power cycle on downgrade from FOS v8.2.1 to v8.2.0 or prior versions to avoid a known issue with DP due to DIMM errors, which can cause disruption to the traffic. To avoid this the 7840 has to be rebooted and the blade on SX6 has to be power-cycled once after downgrade is completed to avoid the DP panic due to DIMM errors.
- When performing zoning operations on the fabric via Network Advisor API (i.e. Network Advisor SMI or REST API), it is not recommended to perform zoning operations concurrently via other interfaces (e.g. FOS RESTCONF, CLI, etc.) as the configurations being applied by the Network Advisor API may overwrite the zoning updates done by other means.

  To find out which application is currently accessing the fabric use the following CLI command:
  `#apploginhistory –show`
- TLS v1.0 and v1.1 protocols are disabled in Network Advisor 14.4.3.
- In FOS 8.2.1b, two new SNMP MIB OIDs (swConnUnitPortTxRate, swConnUnitPortRxRate) were introduced for Tx/Rx rate. The new OIDs are part of FAEXT.MIB and are not supported in Access Gateways. Therefore, BNA 14.4.4 does not show traffic for Access Gateway with FOS versions 8.2.1b or greater. BNA 14.4.4 continues working fine for AGs with firmware versions prior to v8.2.1b.
- The Historical and Real time FC port performance statistics for the traffic utilization related measures are displayed in BNA 14.4.4 as four times higher than the actual values (defect BNA-801049). If users plan to monitor the performance statistics of FC Ports using Brocade Network Advisor 14.4.4, then they are advised to contact the Support team to get the fix-patch for this issue.
- Network Advisor does not support custom port for SFTP/SCP protocols in Product Supportsave and Firmware download features.
- Network Advisor supports Microsoft AD and OpenLDAP AAA servers, same as Fabric OS. When importing collection flows via XML file make sure there are no duplicate entries in the XML file, otherwise, collection import will fail.
- When downgrading Fabric OS to v8.2.0x or prior firmware versions, the user has to perform additional blade slot power cycle on all SX6 blades after downgrade operation is completed. Following warning message is not being displayed in Network Advisor (although it is shown in CLI):
  `“WARNING: HCL is not supported on downgrade to 8.2.0x or prior firmware versions. Perform additional blade slot power cycle on all SX6 blades post firmware downgrade.”`

- In Network Advisor v14.4.4 or later the historical graph may show zero values for Tx/Rx Port Utilization Measures for the Gen 6 switches running FOS version v8.2.1 or later.

9.4.1 Display of Logical Switches

If you create logical switches through the **Logical Switch** dialog, the logical switch displays under undiscovered logical switch in the existing **Logical Switches** panel. You must rediscover the newly created logical switch fabric by going to the **Discovery** dialog and adding the IP address of the chassis using the **Add** dialog.

9.4.2 SSL Connections That Use Certificates with MD5 Signatures

SSL-based product communication will fail if the devices have "weak" authentication certificates. For devices with weak 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`." Java 1.8 used by Brocade Network Advisor 12.x disables the use of certificates with weak authentication. The certificates on such devices must be updated to be compliant with JRE 1.8. For details on updating certificates, refer to the "Secure Sockets Layer protocol" section of the Fabric OS administration guide.

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.

9.4.3 Reset Ports Operation in the Logical Switches Dialog

NOTE: Resetting ports to the default operation is applicable only when the ports are moved from one logical switch to another logical switch through the **Right Arrow** button, that is, from (Chassis Ports Tree/Tree Table) LHS to the (Logical Switches Device Tree) RHS device tree.

It is not applicable when:

- Ports from a logical switch are moved to the default logical switch through the **Left Arrow** button, that is, from (Logical Switches Device Tree) RHS to (Chassis Ports Tree/Tree Table) LHS.
- When a logical switch is deleted, its ports will not be reset to the default before moving to the default logical switch before its deletion.

Ports that are moved to the default logical switch can be reset to the default if they are moved from Chassis Ports Tree/Tree Table LHS to the Logical Switches Device Tree RHS device tree.

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

- In the Brocade 7840 GE ports cannot be reset to the default unless their corresponding VE ports are cleared of their FCIP configurations.

- Resetting the switch to the default operation on the Brocade 7840 may fail due to GE port sharing or if the associated VE port exists in another LS.

9.4.4 Incorrect timestamp for events after Daylight changes

Step-by-step guide

In Network Advisor we are using the java API "java.util.Date" to get the current date and time while persisting events. This API considers DST (Daylight Savings Time) to be included in time based on the time zone and as the decision to exclude the DST from Brazilian time zones was taken recently i.e in April 2019, the java API which we are using is not implemented to take care of that automatically and hence we could see this issue.

Oracle java 8 update 231 has the fix for the issue (java.util.Date computed time is 1 hour ahead of system time with Brazilian time zones). This is a commercial version and Network Advisor is using java 8 update 211.

To address this known issue in API, we have a work around with TZUpdater tool (The TZUpdater tool is provided to allow you to update installed JDK and JRE software with more recent timezone data, to accommodate daylight saving time (DST) changes in different countries. Oracle relies on the timezone data publicly available through IANA's Time Zone Database).

Please find below steps to run this tool:

1. Download TZUpdater tool from below location and extract it to any local folder

https://www.oracle.com/technetwork/java/javase/downloads/tzupdater-download-513681.html

2. Stop all Network Advisor services through SMC.

3. Open command prompt and go to Network Advisor installed jre location.

```
C:\Program Files\Network Advisor 14.4.1\jre64\bin>
```

4. Run TZUpdater tool as below

Syntax: *java -jar "temp_dir\tzupdater.jar" -f*

Example: *java -jar C:\tzupdater-2_3_0\tzupdater-2.3.0\tzupdater.jar -f*

C:\Program Files\Network Advisor 14.4.5\jre64\bin>java -jar c:\tzupdater.jar -f

Using *https://www.iana.org/time-zones/repository/tzdata-latest.tar.gz as source* for tzdata bundle.

5. Now start all BNA services through SMC.

9.5 Important Notes Common for SAN and IP

- In rare cases, due to some interactions with virus scan software, the Network Advisor server start process might continue for 10 to 12 minutes, or it may fail to start the server. If this happens, configure the virus scans to skip scanning Network Advisor files.
- To avoid excessive Telnet/SSH login messages in the Network Advisor master log and event report and in the device CLI console, disable lazy polling by unchecking the **Enable lazy polling** check box in the **IP Discovery Global Settings > Preferences** dialog.
- Starting with 12.0, the supported number of client connections has increased to 25. Refer to the installation guide for details. In addition to those details, the following database memory setting is required:

  - The PostgreSQL's parameter `shared_buffers` memory allocation should be increased to 1024 MB. (This parameter can be set by editing the `<installation_directory>\data\databases\postgresql.conf` file.) Change the following line from: `shared_buffers = 512MB`

    To: `shared_buffers = 1024MB`
  - The server must be restarted.
- In Linux 64-bit machines, connecting to the database through Open office using ODBC will not work. The solution is to connect from the Windows ODBC Client to the 64-bit Linux machine where Network Advisor is running to view the Database tables.
- 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 following configuration must be done in the VSFTPD FTP server before triggering support save by setting the external VSFTPD FTP Linux server (other than the Brocade Network Advisor FTP server):

  `/etc/vsftpd.conf file` and set `"chroot_local_user=YES"`
- A 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 and then copying and installing that client on another machine. For details, refer to the "Client only installation" section of the installation and migration guide.
- An HTTP 500 error message is intermittently displayed when launching the Web Client. A server restart will fix the issue.
- The user must run the `sanperformancestatenable` script from the Brocade Network Advisor home utilities folder to enable/disable performance statistics collection for an SMIA only package installation. The following are the steps to run the script:
  - Windows: Open a command prompt, move to `<BNA_HOME>\utilities`, and run `sanperformancestatsenable.bat dbusername dbpassword enable/disable`.
  - Linux: Open a terminal, move to `<BNA_HOME>\utilities`, and run `sanperformancestatsenable dbusername dbpassword enable/disable`.
- The REST API does not provide FCIP circuit measures for the GigE port.
- Brocade Network Advisor is now enforcing minimum disk space requirements during migration. When the disk space requirements are not met, Brocade Network Advisor displays a message prompting the user to use the script to delete performance data and retry migration.
- SNMP trap auto-registration does not happen for a discovered VCS that is configured with the "Read-Only" community string alone. Registration can be done manually after discovery through the **Product Trap Recipients** dialog.
- When Network Advisor is managing more than 1500 IP products, the user might experience some performance degradation such as delays while launching some dialogs.
- Due to a Microsoft Windows operating system restriction that does not allow services logged in as a Local System user to interact with the desktop, the GUI application cannot be launched using the **Launch a Script** option of **Add Event Action**. Refer the following link for more information:

  http://msdn.microsoft.com/en-us/library/windows/desktop/ms683502%28v=vs.85%29.aspx
- During migration, if insufficient space is detected, a warning message will be displayed with an option to roll back. If the user chooses "No," migration will be aborted. As a result, the source version services will remain uninstalled. For instructions to install the source version services manually, refer to the installation guide.

  The ports listed in Network Advisor installation and migration guide must be open bidirectionally for all the bidirectional protocols in the firewall where the server is installed.
- If the source Network Advisor has more products discovered, it is recommended to stop all services manually from the Network Advisor **Server Management Console** of the older version before initiating migration from the Configuration wizard.
- A service startup failure can be seen in Windows 2008 R2 OS, and the recommendation is to apply the hot fix from http://support.microsoft.com/kb/2577795.
- If you see the "`Signature could not be validated`" error message 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 a mismatch in the signature key could be used in the SSH handshake between the switch and the SCP/SFTP server. Try the following CLI command workaround to address the issue:

– For Fabric OS devices:

```
sw0:FID128:admin> sshutil delknownhost
IP Address/Host name to be deleted: <IP address of the SSH server>
```

– For Network OS devices: Firmware version 3.0 and later

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

– Firmware version 2.1.1b:

```
sw0#execute-script sshdeleteknownhost
IP Address/Host name to be deleted: <IP address of SSH server>
```

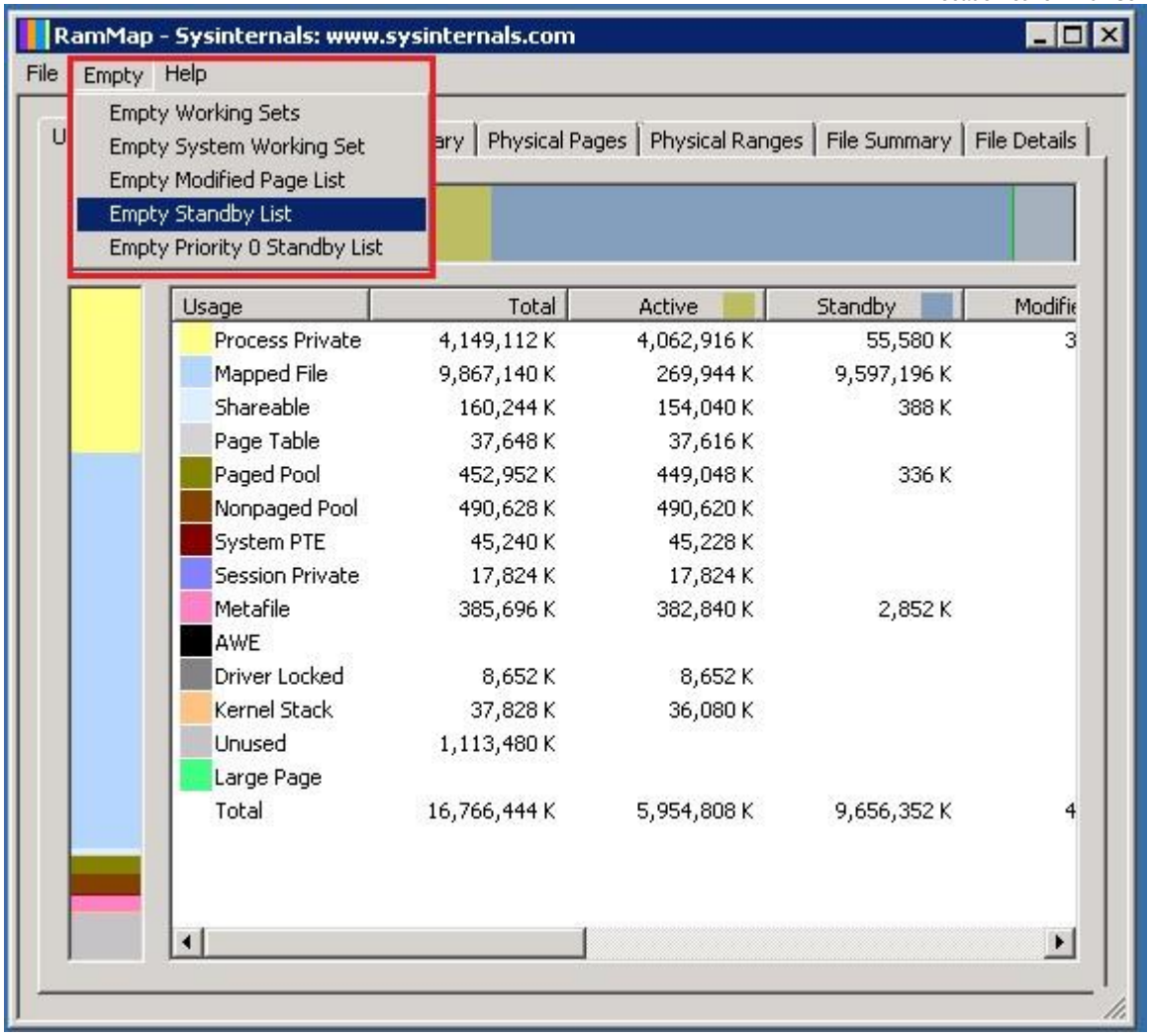
If the above does not work, go to **Server > Options > Software Configuration > FTP/SFTP/SCP**, and uncheck the **SCP/SFTP** option.

- You need to use a different (nondefault) name for the widget when attempting to add the "Top Product Response Time" widget to avoid the "`Monitor could not be added. Duplicate monitor name`" error.
- Patch installer troubleshooting—The patch installer may not launch if the UAC is enabled on Windows 7/8/2008/2008 R2/2012 editions. You must first disable the UAC using the procedure provided in "Chapter G: Troubleshooting - Patch troubleshooting" of the user manual and then launch the patch installer.

  During migration, the Brocade Network Advisor uninstallation process requires 1 GB of physical RAM. Sometimes Windows OS does not clear the released memory and keeps it in standby memory. Use a Microsoft tool like RAM MAP to clean up the unused RAM from the standby list. Download the `RAMMap.zip` file from https://technet.microsoft.com/ en-us/sysinternals/rammap.aspx.

  a. Extract the zip file, and run `runmap.exe`.

  b. Click **Empty > Empty Standby List**.



- The From Email Address attribute is not supported on NOS devices. Similarly, the From Email Address attribute is not supported on FOS devices with pre-8.2.0 firmware.

  However, in the cases above, the From Email Address attribute is enabled and accepts input that is not being saved.

  The Test Email attribute is not supported on NOS and should be grayed out. However, when a mixture of FOS and NOS devices is managed in Network Advisor, the Test Email attribute will be enabled as it is supported on FOS.

  The above behavior has been captured in DEFECT000660376 in this document.

- Any other standalone instance of PostgreSQL should not be present in the system where the Network Advisor application is installed. If such other instance of PostgreSQL exists on the same server, it will be removed along with Network Advisor during the Network Advisor uninstallation.

  The Network Advisor migration operation fails when the database password contains the special character "=" (equal sign), since it is considered an assignment operator by the Windows command prompt. This behavior is seen on Windows platforms in all releases of Network Advisor.

  Workaround: Use only the following special characters in the database password: ! # $ * (DEFECT000660172).

- Historical or real-time performance data does not persist in the database. This issue is observed in the SAN + IP flavor of Network Advisor with the enabled AMP service when monitoring the VDX switch (DEFECT000660471).

- Network Advisor 14.4.4 provides a new utility to split a large size file like supportsave into smaller chunks, for easy transmission over the network.
  Binaries for Linux and Windows platforms are located at `<BNA_INSTALL_HOME>\bin`:

– `fileSplitter.bat/sh` splits large size file into smaller chunks of equal sizes
– `filesMerger.bat/sh` merges all chunks, created using the `fileSplitter` script, into a single file.

Note: The file chunks generated by `fileSplitter` utility cannot be opened with any editor. This utility is only for splitting a big file into smaller chunks and assembling them into a single file.
Refer to `<BNA_INSTALL_HOME>\bin\Readme_FilesMerger.txt` and `<BNA_INSTALL_HOME>\bin\Readme_splitter.txt` for more details on how to use the utility.

Domestic and International Modem-Based Call Home Is No Longer Supported

Alternatively, customers who use the Domestic or International Call Home Modem feature can reconfigure their Call Home to use the Brocade Email option for continued Call Home notifications in the event of a system problem. For more configuration details, refer to the “Call Home” section of the Brocade Network Advisor user manual. Note that EFCM and DCFM customers will also be affected by this change and must reconfigure their Call Home to use the Brocade Email option for continued Call Home notifications in the event of a system problem.

9.5.1 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 and server backup operations.

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

NOTE For networks with large amounts of data to back up, 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.

9.5.2 Installation on Network Mounted Drives Is Not Supported

Installation onto a Windows network mounted drive is not supported; installation is allowed, but the database fails to start.

9.5.3 Client Disconnects

Under a heavy server load or degraded network links, Network Advisor client may get disconnected from the server. The workaround is to restart the client.

9.5.4 Cross-flavor Migration

9.5.4.1 Migrating the Same Version of Network Advisor from OEM1 Version to OEM2 Version

1. Partially uninstall the source Network Advisor OEM1 version.
2. Install the Brocade Network Advisor 14.4.x OEM2 version.
3. In the **copy data and settings** page, browse to the Brocade Network Advisor pre-14.4.x OEM1 version and continue with the migration.

9.5.4.2 Migrating the Brocade Network Advisor (Pre-14.4.x) OEM1 Version to the Brocade Network Advisor 14.4.x OEM2 Version

1. Install the source Brocade Network Advisor OEM1 version.
2. Install the Brocade Network Advisor 14.4.x OEM2 version.
3. In the **copy data and settings** page, browse to the Brocade Network Advisor pre-14.4.x OEM1 version and continue with the migration.

9.5.5 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

9.5.6 Performance Statistics Counters—Calculation Formulae

To calculate the statistics for FC, GE, FCIP, and TE port, we use SNMP to query the respective OIDs, mentioned in the following table.

To calculate 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.

The polling interval for the historical graph is 5 minutes, 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)

Name	y	d	Source Value	Formula
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	N/A	TX = (Delta valueP1P / (1000 * 1000)) / (Polling intervalP2P)
RX	HBA, CNA	HCM API	N/A	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	N/A	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 the 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	N/A	N/A	(ifHCInOctets + ifHCOutOctets) / fcipExtendedLinkCompressedBytes

Delta value1 is the difference of the value retrieved between two consecutive poling cycles.

Polling interval2 is the duration between two polling cycle, in seconds.

9.6 SMI Agent

For Network Advisor that has more than 30K instances, the CIMOM takes more memory to generate CIM instances.

If the user performs Enumerate Instances and the total size is more than 2 MB for all managed fabrics, an out-of-memory issue may result. In this case, the user must increase the CIMOM heap size to fetch a zone database size of 2 MB. Note: For 1.6 MB of zone database (144,600 zone members) with 9 GB of heap size, the Brocade_zonemembershipsettingdata instances are retrieved.

9.6.1 Indications Delivery Depends on the SAN Size and SNMP Registration

The time-to-deliver indication will vary based on the Network Advisor SAN size selected during installation. If a large SAN size is selected, indication delivery time will be longer.

Provider classes may take more time to update the fabric changes if the switches managed in Network Advisor are not registered with SNMP. As this would cause a delay in indication delivery, all switches managed in Network Advisor should be SNMP registered.

9.6.2 CIMOM Heap Size

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

Old Heap Size:

Small

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

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

Medium

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

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

Large

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

Current Heap Size:

Small

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

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

Medium

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

Large

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

9.6.3 Logging for CIMOM

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

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

The logging level, file size, and number of log files can be changed by modifying the following fields: **Log Level**, **File Size**, and **Number of Files** from the Configuration Tool through the **CIMOM** tab.

9.6.4 Service Location Protocol Support

The management application SMI Agent uses the 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.

9.6.5 Management SMI Agent SLP Application Support

Management SMI Agent SLP application support includes the following components:

- The `slpd` script starts the `slpd` daemon.
- The `slpd` program acts as a service agent (SA). A different `slpd` binary executable file exists for UNIX and Windows systems.
- The `slptool` script starts the `slptool` platform-specific program.
- The `slptool` program can be used to verify whether SLP is operating properly. A different `slptool` exists for UNIX and Windows.

By default, the management application SMI Agent is configured to advertise itself as an SA. The advertised SLP template shows its location (IP address) and the WBEM services that 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 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 an 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 output:

```
service:wbem:https://10.0.1.3:5989,65535
service:wbem:http://10.0.1.3:5988,65535
```

This output shows the functionalities of the 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 the 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`

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

9.6.6 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 the 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 that 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 that the SLP service is advertising its WBEM services.
5. Choose one of the following options to verify that 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.

9.6.7 SLP on Windows Systems

This section describes how to verify the SLP daemon on Windows systems.

SLP file locations:

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

Verifying SLP service installation and operation on Windows systems:

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

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

9.7 User Guides

9.7.1 List of Documents

You can download the software and documentation from the myBroadcom 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 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*

9.7.2 Known Documentation Errors

- Copyright © 2019 Broadcom. All Rights Reserved. Broadcom, the pulse logo, Brocade, and the stylized B logo are among the trademarks of Broadcom in the United States, the EU, and/or other countries. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

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

  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, to view the licensing terms applicable to the open source software, and to obtain a copy of the programming source code, please download the open source disclosure documents in the Broadcom Customer Support Portal (CSP). If you do not have a CSP account or are unable to log in, please contact your support provider for this information.

  Use of all versions of Brocade Network Advisor (the "Software") is subject to current the terms and conditions of the Brocade Network Advisor End User License Agreement (the "EULA"), as amended by Brocade from time to time. It is the user's responsibility to understand and comply with the terms of the EULA. By downloading, installing, using, posting, distributing or otherwise making available the Software, you agree to be bound on an ongoing basis by the EULA as updated by Brocade from time to time.

- In the *Brocade Network Advisor Installation and Migration Guide*, the following details are missing:
  In the "Linux swap space requirements" section, change "Greater than 4 GB and less than 8 GB" to "Greater than 6 GB and less than 8 GB".
- In the *Brocade Network Advisor SAN Installation and Migration Guide*, add the following details:
  In the "Linux swap space requirements" section, change "Greater than 4 GB and less than 8 GB" to "Greater than 6 GB and less than 8 GB".

- In the *Brocade Network Advisor SAN AMP Manual* and *Brocade Network Advisor SAN+IP AMP User Manual*:
  - The "Management Application server and Client System clocks are synchronized even if they are in different time zones" statement should be corrected as "Management application server and client system clocks should be synchronized even for different time zones since the user would see the problem in historical data when a customized time is configured in the client system."
  - For upgrading and migration, refer to the following notes:
    Follow these instructions to migrate from 14.2.x/14.3.x to 14.4.x:

    - Start with a source version that is running Brocade Network Advisor 14.2.x/14.3.x with AMP service enabled; AMP running firmware v2.1.0.
    - First migrate the source Brocade Network Advisor 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 Brocade Network Advisor migration).

- The following content should be removed from the *Brocade Network Advisor SAN User Manual* and *Brocade Network Advisor 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
- The *Brocade Network Advisor SAN+IP User Manual* and *Brocade Network Advisor 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. In these cases, the "From Email Address" is enabled and accepts input which is not being saved.
  - The "Test Email" attribute is not supported for Network OS and should be grayed out.
  - When mixture of Fabric OS and Network OS devices is managed in Network Advisor, the "Test Email" will be enabled since it is supported for FOS.
- The following list of Call Home events supersedes the list present in the user manual:

Description	Type	FRU Code/Event Type	Severity	Event Reason Code
Error in registered link incident record (RLIR)	Fabric OS	MS-1009	4	1009
Flash usage is out of range	Fabric OS	FW-1402	3	1402
Faulty or missing power supply	Fabric OS, Network OS	FW-1426	3	1426
Faulty power supply	Fabric OS, Network OS	FW-1427	3	1427
Missing power supply	Fabric OS, Network OS	FW-1428	3	1428
Problem in power supply arrangement	Fabric OS	FW-1429	3	1429
Faulty temperature sensors	Fabric OS, Network OS	FW-1430	3	1430
Faulty fans	Fabric OS, Network OS	FW-1431	3	1431
Faulty WWN cards	Fabric OS, Network OS	FW-1432	3	1432
Faulty CPs	Fabric OS, Network OS	FW-1433	3	1433
Faulty blades	Fabric OS, Network OS	FW-1434	3	1434
Flash usage is out of range	Fabric OS, Network OS	FW-1435	3	1435
Marginal port	Fabric OS	FW-1436	3	1436
Faulty port	Fabric OS	FW-1437	3	1437
Faulty or missing SFPs	Fabric OS	FW-1438	3	1438
Switch is not reachable	FOS, IOS, NOS	Ethernet	3	
Switch is missing from the fabric	FOS, IOS, NOS	SW-Missing	3	
Power supply state changed	Ironware OS	IP30	1	199130
Fan failed	Ironware OS	IP31	1	199131
Temperature alert	Ironware OS	IP36	1	199136
Stacking power supply failed	Ironware OS	IP167	1	1991167
Stacking fan failed	Ironware OS	IP169	1	1991169
Stacking temperature warning	Ironware OS	IP171	1	1991171
High-speed fans needed for chassis	Ironware OS	IP177	4	1991177
System memory out of threshold	Ironware OS	IP181	4	1991181
IP CAM full	Ironware OS	IP1002	1	19911002
Optical monitoring alarm	Ironware OS	IP1004	1	19911004
POS monitoring alarm	Ironware OS	IP1007	1	19911007
Optical incompatibility error	Ironware OS	IP1009	1	19911009

Description	Type	FRU Code/Event Type	Severity	Event Reason Code
Faulty or absent power supplies	Fabric OS, Network OS	MAPS-1021	3	1021
Faulty or absent fans	Fabric OS, Network OS	MAPS-1021	3	1021
Faulty temperature sensors	Fabric OS, Network OS	MAPS-1021	3	1021
Flash usage is out of range	Fabric OS, Network OS	MAPS-1021	3	1021
Faulty ports	Fabric OS, Network OS	MAPS-1021	3	1021
Marginal ports	Fabric OS, Network OS	MAPS-1021	3	1021
Missing SFPs	Fabric OS, Network OS	MAPS-1021	3	1021
Error ports	Fabric OS, Network OS	MAPS-1021	3	1021
Faulty WWN cards	Fabric OS, Network OS	MAPS-1021	3	1021
HA monitoring	Fabric OS, Network OS	MAPS-1021	3	1021
Core blade down	Fabric OS, Network OS	MAPS-1021	3	1021
Faulty or absent blades	Fabric OS, Network OS	MAPS-1021	3	1021
Faulty FRU	Fabric OS, Network OS	EM-1034	4	1034
Faulty FRU	Fabric OS, Network OS	FW-1444	3	1444
Core blade/SFM failures	Fabric OS, Network OS	FW-1447	3	1447
Faulty SFPs	Fabric OS	MAPS-1003	4	1003
Faulty SFPs	Fabric OS	MAPS-2180	3	2180
Faulty SFPs	Fabric OS	MAPS-2181	2	2181
Faulty SFPs	Fabric OS	MAPS-2182	4	2182

- In the SAN user manual, in the **Server Management Console > AAA Settings** tab section, the third item in the **Authorization Preference** drop-down menu for the LDAP server should read **Authentication Server Groups** instead of **LDAP Authorization**.
- IP-related content is still available in the SAN and SAN with AMP user manuals.
- Network Advisor user manuals do not capture the behavior for "From email" attributes in MAPS described in DEFECT000660376 as well as in the “Important Notes Common for SAN and IP” section in this document.
- Despite the statement in the Network Advisor manuals, no additional JRE is required on the Network Advisor server to access the Server Management Console (SMC) or the local client.
- In the *Brocade Network Advisor SAN Installation and Migration Guide*, steps in the “Premigration requirements when migrating from one server” section should be as follows:

  All Network Advisor editions are supported only on 64-bit servers. The following steps are applicable to Windows-to-Windows or Linux-to-Linux migration. If you are migrating from Management application 14.2.X on a server1 to Management application 14.4.Y on a server2, complete the following steps:

  1. Back up the server for 14.2.X using **Options > Server Backup** on server1.
  2. Install Management application 14.2.X (that is, the same version of the Management application that is running on server1) on server2.
  3. Select the **SMC > Restore** tab to restore the backup on server2.
  4. Install Management application 14.4.Y on server2.
     Perform a migration to Management application 14.4.Y (refer to “Data Migration” on page 55 in the Brocade *Network Advisor SAN Installation and Migration Guide*).

Chapter 10: Defects

10.1 TSBs—Critical Issues to Consider Before 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. Review carefully and refer to the complete TSB for relevant issues before migrating to this version of code. On myBroadcom (sign-in required), this product documentation can be found by selecting **Support > Document Library** and 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).

10.1.1 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 Web Tools or Brocade Network Advisor remote client launch will be blocked by Java Security when running against a version of FOS or Brocade Network Advisor that contains an expired Java code signing certificate.

10.2 Closed Defects with Code Changes in Brocade Network Advisor 14.4.5

This section lists software defects with critical, high, and medium technical severity that have been closed with a code change as of 01/13/20 in Brocade Network Advisor 14.4.5.

Defect ID:	BNA-801171		
Technical Severity:	Medium	**Probability:**	null
Product:	Network Advisor	**Technology Group:**	Performance
Reported In Release:	Network Advisor14.4.4	**Technology:**	Historical Data
Symptom:	Network Advisor did not preserve FC ports settings in the Favorits dialog.		
Condition:	Observed for the FC port filter type after re-opening the Favorites dialog.		
Workaround:	The Monitor-->Performance-->Historical Graph will show the favorites correctly.		

Defect ID:	BNA-801133

Technical Severity:	Medium	**Probability:**	Medium
Product:	Network Advisor	**Technology Group:**	Other
Reported In Release:	Network Advisor14.4.4	**Technology:**	Other
Symptom:	After deleting a zone from Zones Panel, the cursor selection is being moved to another zone.		
Condition:	When user attepmts to delete a zone from Zones Panel.		

Defect ID:	BNA-801103		
Technical Severity:	High	**Probability:**	Medium
Product:	Network Advisor	**Technology Group:**	Performance
Reported In Release:	Network Advisor14.4.4	**Technology:**	Real-Time Data
Symptom:	Tx/Rx Utilization is not being shown for the Access Gateway ports.		
Condition:	Observed on Access Gateways running Fabric OS v8.2.1a and later.		

Defect ID:	BNA-801090		
Technical Severity:	Medium	**Probability:**	null
Product:	Network Advisor	**Technology Group:**	Device Monitoring
Reported In Release:	Network Advisor14.4.4	**Technology:**	Third-party tools
Symptom:	Week ciphers were supported in Network Advisor 14.4.4 and earlier releases.		
Condition:	The below ciphers exist in Network Advisor 14.4.4 or earlier: exchange diffie-hellman-group1-sha1 3des-cbc		

Defect ID:	BNA-801034		
Technical Severity:	Medium	**Probability:**	null
Product:	Network Advisor	**Technology Group:**	Fault Management
Reported In Release:	Network Advisor14.4.4	**Technology:**	Call Home

Symptom:	Inventory report generation failed with Error Message: "FAILED: Inventory Report could not sent to EMC-ESRS; Reason: Unauthorized; Reason Code: 401"
Condition:	Observed when tried to generate the report and send it via ESRS application.

Defect ID:	BNA-800978		
Technical Severity:	High	**Probability:**	null
Product:	Network Advisor	**Technology Group:**	Performance
Reported In Release:	Network Advisor14.2.2	**Technology:**	Utilization (SAN)
Symptom:	Switch support save via CLI failed with the "Protocol not configured correctly" error.		
Condition:	When a COMPASS template with FTP/SCP configuration is created and propagated to the switch.		
Workaround:	Use CLI to correct supportftp configuration to change the protocol to lowercase.		

Defect ID:	BNA-800968		
Technical Severity:	Medium	**Probability:**	null
Product:	Network Advisor	**Technology Group:**	Other
Reported In Release:	Network Advisor14.4.3	**Technology:**	Other
Symptom:	When disabling a port the message does not competely indentify the selectded port (i.e. it shows only the port number and omits details such as slot number or port index).		
Condition:	When the user selects the corresponding "port_name" column value to enable/disable the port in the Port Connectivity View dialog.		

Defect ID:	BNA-800966		
Technical Severity:	Medium	**Probability:**	null
Product:	Network Advisor	**Technology Group:**	Management
Reported In Release:	Network Advisor14.2.1	**Technology:**	Configuration Fundamentals

Symptom:	User is not able to connect the SMIA using vROPs.
Condition:	Intermittently observed when multiple threads are running in parallel and JServer gets initialized before setting the required attributes.

Defect ID:	BNA-800958		
Technical Severity:	High	**Probability:**	null
Product:	Network Advisor	**Technology Group:**	Device Management
Reported In Release:	Network Advisor14.4.4	**Technology:**	Device configurations
Symptom:	Network Advisor failed to display switch properties.		
Condition:	Intermittently observed when trying to open switch properties from the chassis group.		

Defect ID:	BNA-801165, BNA-801073, BNA-801080		
Technical Severity:	Medium	**Probability:**	null
Product:	Network Advisor	**Technology Group:**	Performance
Reported In Release:	Network Advisor14.4.4	**Technology:**	Historical Data
Symptom:	The performance graphs are showing incorrect Tx/Rx port utilization values.		
Condition:	Observed for FOS v 8.2.1 and Network Advisor 14.4.4.		

Defect ID:	BNA-801161		
Technical Severity:	Medium	**Probability:**	null
Product:	Network Advisor	**Technology Group:**	Monitoring
Reported In Release:	Network Advisor14.4.4	**Technology:**	Dashboards
Symptom:	Dashboard widgets did not show any data.		
Condition:	Happens rarely when following widgets present in the Dashboard are being refreshed: "Top N Oversubscribed IT Flows" and "Top N IT Flows".		

Defect ID:	BNA-801152		
Technical Severity:	Medium	**Probability:**	null
Product:	Network Advisor	**Technology Group:**	Monitoring
Reported In Release:	Network Advisor14.4.4	**Technology:**	Policy Monitor
Symptom:	Some rules were missing after the distribution of MAPS policy.		
Condition:	Observed on switches running FOS v8.2.1c when the MAPS policy contains ALL_25Km_16GLWL_SFP group. Rules related to this group are being skipped.		

Defect ID:	BNA-801140		
Technical Severity:	Medium	**Probability:**	null
Product:	Network Advisor	**Technology Group:**	Monitoring
Reported In Release:	Network Advisor14.4.4	**Technology:**	Policy Monitor
Symptom:	The monitor database size in Network Advisor keeps increasing.		
Condition:	Occurs occasionally after taking server backup.		

Defect ID:	BNA-800957		
Technical Severity:	Medium	**Probability:**	null
Product:	Network Advisor	**Technology Group:**	Device Monitoring
Reported In Release:	Network Advisor14.4.3	**Technology:**	Flow Vision (SAN)
Symptom:	Dashboard showed "No data to display" message.		
Condition:	Seen intermittently when querying the AMP switch for min/max/avg parameter values.		

10.3 Closed Defects without Code Changes in Brocade Network Advisor 14.4.5

This section lists software defects with critical, high, and medium technical severity that have been closed without a code change as of 01/13/20 in Brocade Network Advisor 14.4.5.

Defect ID:	BNA-800941	**Technical Severity:**	Medium
Reason Code:	Not a Software Issue	**Probability:**	null
Product:	Network Advisor	**Technology Group:**	Application Management
Reported In Release:	Network Advisor14.4.2	**Technology:**	Installation & Migration
Symptom:	Help window shows incorrect version of Network Advisor.		
Condition:	Observed after upgrading from Network Advisor 14.2.1 to 14.4.2.		

Defect ID:	BNA-800857	**Technical Severity:**	Low
Reason Code:	Not a Software Issue	**Probability:**	null
Product:	Network Advisor	**Technology Group:**	Device Management
Reported In Release:	Network Advisor14.3.1	**Technology:**	Zoning
Symptom:	The Error:OutOfMemory thrown during the SMIA call "ActivateZoneSet". Also the zone members in zone are duplicated.		
Condition:	When trying to activate the zoneset with more than 3500 zones in it via SMIA client. Assume we have 2 zone with 2 members in each zone as below: Zone1 > Member1 > Member2 Zone2 > Member3 > Member4 During activation the zone members are recursively added as below. Due to this each zone has size of 1MB which is causing OutOfMemory error. Zone1 > Member1 > Member2 Zone2 > Member1 > Member2 > Member3 > Member4		

Defect ID:	BNA-800570	**Technical Severity:**	Medium
Reason Code:	Will Not Fix	**Probability:**	null
Product:	Network Advisor	**Technology Group:**	Client
Reported In Release:	Network Advisor14.4.2	**Technology:**	Options Dialog
Symptom:	When launching the zoning module within BNA on a Linux server, a grey rectangle appears in a modal (always staying on top of window) view. The box only appears when zoning is opened, and closes when zoning is closed.		
Condition:	This issue is seen only on Linux platforms.		
Workaround:	Launch remote client on Windows platform and use Zoning.		

10.4 Open Defects

This section lists open software defects with critical, high, and medium technical severity as of 01/13/20 in Brocade Network Advisor 14.4.5.

Defect ID:	BNA-801173		
Technical Severity:	Medium	**Probability:**	null
Product:	Network Advisor	**Technology Group:**	Performance
Reported In Release:	Network Advisor14.4.4	**Technology:**	Historical Data
Symptom:	Historical graph may show zero values for Tx/Rx Port Utilization measures.		
Condition:	Observed in Network Advisor 14.4.4 or later for the Gen 6 switches running FOS v8.2.1 or later.		

Revision History

BNA-1445-RN100; January 13, 2020

- Initial release for Brocade Network Advisor 14.4.5
- Added details about changes in Network Advisor License validation
- Removed the Brocade Encryption Switch from the supported hardware list
- Updated “Important Notes” with the following notes:
  - List of supported LDAP servers
  - Clarification about importing flows - XML file should not contain duplicate flows
  - Workaround when incorrect timestamp observed for events after daylight changes
  - Historical graph issue with Tx/Rx Port Utilization for Gen 6 switches.
  - Mandatory additional blade power off on SX6 blades after downgrading Fabric OS to 8.2.0x versions

BNA-1444-RN104; November 25, 2019

- Updated “Important Notes” with the “Important Notes for Changing the IP Address of the Network Advisor Server” section

BNA-1444-RN103; November 14, 2019

- Added EULA paragraph to standard legal statement page.
- Removed following switch models from the Supported SAN Devices section:
  - Brocade 4012 Switch
  - Brocade 4016 Switch
  - Brocade 4018 Switch
  - Brocade 4020 Switch
  - Brocade 4024 Switch
  - Brocade 5410 Embedded Switch
  - Brocade DCX and DCX-4S Director Chassis
  - Brocade DCX-16, DCX-32, DCX-48, DCX-64, FCOE10-24 Port Blades
  - FS8-18 Encryption blade
- Updated “Important SAN Notes” with the statement that Network Advisor does not support custom port for SFTP/SCP protocols in Product Supportsave and Firmware download features.

BNA-1444-RN102; October 15, 2019

- Removed following Fabric OS versions and switch/blade models from the Supported SAN Devices section as they have reached End of Support:
  - Fabric OS 6.0.x
  - Fabric OS 7.0.x
  - Fabric OS 7.1.x
  - Fabric OS 7.2.x
  - Fabric OS 7.3.x
  - Brocade 5300 Switch
  - Brocade 5100 Switch
  - Brocade 8000 Switch
  - VA-40FC Switch
  - FA4-18 application platform blade
  - Brocade FX8-24 Extension Blade
- Removed following adapters from the Supported Adapters section:
  - Brocade 415, 425, 815, 825, 8041, 1010, 1020, 1007, 1741, 1860, 1867, 1869.

BNA-1444-RN101; September 13, 2019

Added support for Fabric OS v8.2.2.

Added details of following defects: BNA-800936, BNA-801049, BNA-801050, BNA-801053 and BNA-800978.

Updated the Important SAN Notes section with the information about known issue with not showing traffic for Access gateways due new SNMP MIB OIDs for Tx/Rx rate in FOS 8.2.1b, and issue with the values of traffic utilization related measures displayed in Historical and Real time FC port performance statistics.

BNA-1444-RN100; March 5, 2019

- Initial release for Brocade Network Advisor 14.4.4.

BNA-1443-RN102; February 4, 2019

- Updated the “Known Documentation Errors” section with the correct steps of premigration when migrating from one server.
- Added details of BNA-800861 defect.

BNA-1443-RN101; September 12, 2018

- Added the following CVEs in the “Security Vulnerability Fixes” section:
  - CVE-2016-2334

  - CVE-2016-2335
  - CVE-2016-7804
- Updated the manual backup procedure in the “Important Notes for Managing the Brocade Analytics Monitoring Platform” section.
- Updated the “Important SAN Notes” section with the following information:
  - TLS v1.0 and v1.1 protocols are disabled in Network Advisor 14.4.3.
  - Recommendation not to simultaneously use the Network Advisor API and other interfaces to perform zoning operations.

BNA-1443-RN100; August 28, 2018

- Initial release for Brocade Network Advisor 14.4.3.

BROCADE
A Broadcom Company