Fabric OS 9.0.1a

Brocade Fabric OS 9.0.1a Release Notes Digest

Version 3.0

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 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 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.

To expedite your call, have the following information immediately available:

1. General Information:

    Technical support contract number, if applicable.

    Switch model.

    Switch operating system version.

    Error numbers and messages received.

    `supportSave` command output and associated files.

    For dual-CP platforms running Fabric OS 6.2 and above, the `supportSave` command gathers information from both CPs and any AP blades installed in the chassis.

    Detailed description of the problem, including the switch or fabric behaviour immediately following the problem and any specific questions.

    Description of any troubleshooting steps already performed and the results.

    Serial console and Telnet session logs.

    Syslog message logs.

2. Switch Serial Number.

   The switch serial number is provided on the serial number label, examples of which follow:

   ```
   FT00X0054E9
   ```

   AVS0305E012

   The serial number label is located as follows:

   Brocade G630, G620, G610, G720 – On the switch ID pull-out tab located on the bottom of the port side of the switch.

   Brocade 7810 – On the pull-out tab on the front left side of the chassis underneath the serial console and Ethernet connection and on the bottom of the switch in a well on the left side underneath (looking from the front).

   Brocade X6-8, X6-4 – Lower portion of the chassis on the non-port side beneath the fan assemblies.

   Brocade X7-8, X7-4 - Lower portion of the chassis on the non-port side beneath the fan assemblies

3. World Wide Name (WWN).

   When the Virtual Fabric feature is enabled on a switch, each logical switch has a unique switch WWN. Use the wwn command to display the switch WWN.

   If you cannot use the wwn command because the switch is inoperable, you can get the primary WWN from the same place as the serial number.

4. License Identifier (License ID).

   There is only one license ID associated with a physical switch or director/backbone chassis. This license ID is required as part of the ordering process for new FOS licenses.

   Use the `license --show -lid` command to display the license ID.

1.2   Related Documentation

White papers, product manuals, user guides, and data sheets are available at www.broadcom.com. Additional product documentation for all supported releases is available at myBroadcom to registered users. Registered users can also find release notes at myBroadcom.

Chapter 2: Locating Product Manuals and Release Notes

The following sections outline how to locate and download Brocade product manuals and release notes from Broadcom and myBroadcom. Although the illustrations show Fibre Channel and Fabric OS (FOS), they work for all Brocade products and operating systems.

2.1   Locating Product Manuals and Release Notes

2.1.1   Locating Product Manuals on Broadcom

Complete the following steps to locate your product manuals on Broadcom.com.

1. Go to https://www.broadcom.com.

2. Enter the product name or the software version number in the **Search** box.
   For example, the following search is for software and documentation files for software version 9.0.

3. Select the **Documents** check box to list only the documents.

   The list of documents available for the release displays.
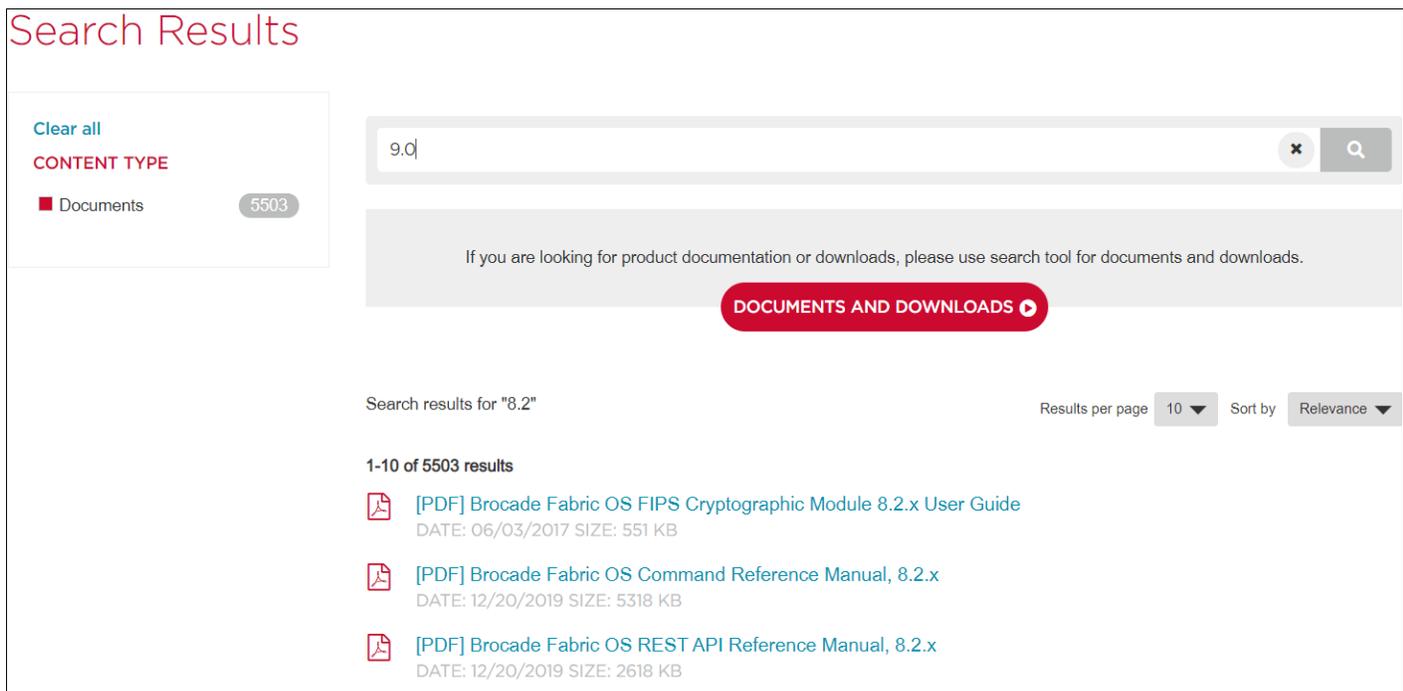
2.1.2   Locating Product Manuals and Release Notes on myBroadcom

Complete the following steps to locate your product manuals on myBroadcom.

1. Go to https://www.broadcom.com/mybroadcom/, click **Login**, and enter your username and password.

   If you do not have an account, click **Register** to set up your account.

2. Select **Customer Support Portal** > **DocSafe (Software/Document Downloads)**.

3. Choose one of the following:

- Enter the product name or the software version number in the **Search** box. For example, the following search is for software and documentation files for software version 9.x.

- Click the **Product Search** box, select **FIBRE CHANNEL NETWORKING**, and select a product from the product list.
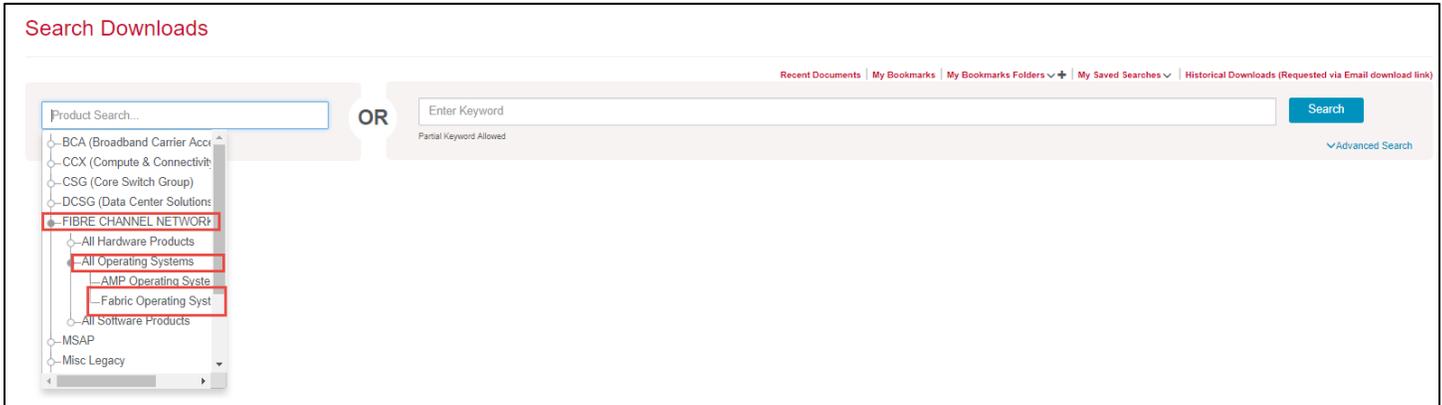
The list of documents and software available for the product displays.

4. Clear the **Software** check box to list only the documents and release notes.

2.2   Document Feedback

Quality is our first concern and we have made every effort to ensure the accuracy and completeness of this document. If you find an error or omission or you think that a topic needs further development, we want to hear from you. You can provide feedback by sending an email to documentation.PDL@broadcom.com. Provide the publication title, publication number, and as much detail as possible, including the topic heading and page number, as well as your suggestions for improvement.

Chapter 3: Overview

Fabric OS v9.0.1a is a maintenance release based on FOS v9.0.0. All hardware platforms and features supported in FOS v9.0.0, 9.0.0a, and 9.0.0b are also supported in FOS v9.0.1a. Fabric OS v9.0.1a includes new optics support, software enhancements, and defect fixes. Note that the **FOS v9.0.1** maintenance release was not made available for production environment use.

Chapter 4: What's New in FOS 9.0.1a

4.1   Hardware

The following section lists new hardware introduced with this release.

4.1.1   New Optical Transceivers

FOS 9.0.1a supports the following new optical transceivers on the noted devices:

- 64Gb/s Fibre Channel SWL SFP (XBR-000462/463) on Brocade G720, X7 (FC64-48)
- 32Gb/s Fibre Channel ELWL SFP (XBR-000478) on Brocade G620, G630, G720, X7 (FC64-48, FC32-X7-48)
- 8Gb/s 80k SmartOptics (8G-ZR-Dxxx-BR1) on Brocade G620, X6 (FC32-48)
- 16Gb/s SmartOptics DWDM secure SFP+ (16G-ER-DxxS-BR2) on Gen 6 platforms and X7 with FC32-X7-48
- 32Gb/s 2km QSFP on Brocade X7 (XBR-000285) (previously supported on Brocade Gen 6)

4.2   Software Features

4.2.1   New Software Features

The following software features are new in this release:

- Flow Vision and IO Insight support for Gen 7 platforms
- Automatic Flow Learning with VM Insight for Gen 6 and Gen 7 platforms
- VM Insight support for FC-NVMe

4.2.2   Modified Software Features

FOS v9.0.1a includes following enhancements:

- LDAP
    - LDAP Global Catalog support
    - LDAP authentication support of sAMAccountName attribute
    - LDAP authorization support using local database
    - LDAPS (LDAP over TLS/SSL) support
- MAPS enhancements
    - Added support for fencing and decommissioning actions for TXP and RXP monitoring

4.2.3   Deprecated Software Features

The following software features are deprecated in this release:

- SNMPv2 is not supported in FOS v9.0.1a but is not blocked. SNMPv2 will be blocked beginning with FOS v9.1.0.

4.3   CLI Command Changes

- The SNMP CLI command `snmpTraps –send` suboption `ip-address` is not supported in FOS v9.0.1a.
- The CLI command `sfpupgrade` is only intended for maintenance operations under the direction of Brocade Support.

4.4   Supported Standards and RFCs

This software conforms to the Fibre Channel standards in a manner consistent with accepted engineering practices and procedures. In certain cases, Brocade might add proprietary supplemental functions to those specified in the standards. For a list of FC standards conformance, visit the following Broadcom SAN Standards website:

https://www.broadcom.com/support/fibre-channel-networking/san-standards/

Chapter 5: Software License Support

5.1   Optionally Licensed Software

Fabric OS v9.0 includes all basic switch and fabric support software, as well as optionally licensed software that is enabled via license keys or license files.

Optionally licensed features include:

Brocade Ports on Demand – This license allows customers to instantly scale the fabric by provisioning additional SFP ports via license key upgrade. (Applies to select switch models.)

Brocade Q-Flex Ports on Demand – This license allows customers to further scale the fabric and increase flexibility by provisioning additional 4x32G QSFP ports via license key upgrade. (Applies to the Brocade G620 and G630 only.)

Brocade Extended Fabrics – This license provides greater than 10 km of switched fabric connectivity at full bandwidth over long distances (depending on the platform, this can be up to 3000 km).

Brocade ISL Trunking – This license provides the ability to aggregate multiple physical links into one logical link for enhanced network performance and fault tolerance. It also includes Access Gateway ISL Trunking on those products that support Access Gateway deployment.

Brocade Fabric Vision – This license enables support for MAPS (Monitoring and Alerting Policy Suite), Flow Vision, and ClearLink (D_Port) when connecting to non-Brocade devices. MAPS enables rules-based monitoring and alerting capabilities, and it provides comprehensive dashboards to quickly troubleshoot problems in Brocade SAN environments. Flow Vision enables host-to-LUN flow monitoring, application flow mirroring for nondisruptive capture and deeper analysis, and a test traffic flow generation function for SAN infrastructure validation. Support for D_Port to non-Brocade devices allows extensive diagnostic testing of links to devices other than Brocade switches and adapters.

NOTE   On Brocade G620, G630, Brocade X6-8, and Brocade X6-4 platforms, this license enables the use of IO Insight capability. The license itself is identified as "Fabric Vision and IO Insight" on these platforms.

FICON Management Server – Also known as CUP (Control Unit Port), this license enables host control of switches in mainframe environments.

Integrated Routing – This license allows any Fibre Channel port in a Brocade X7-4, X7-8, G720, and G620 to be configured as an EX_Port supporting Fibre Channel Routing (FCR).

Integrated Routing Ports on Demand – This license allows any Fibre Channel port in a Brocade 7810, G630, X6-8, or X6-4 to be configured as an EX_Port supporting Fibre Channel Routing. The maximum number of EX_Ports supported per platform is provided in the license.

ICL POD License – This license activates ICL ports on X6 or X7 platform core blades. An ICL license must be installed on the director platforms at both ends of the ICL connection.

> **On the Brocade X6-8:**
>
> The first ICL POD license enables 8 UltraScale ICL QSFP ports on each core blade of the X6-8 director, which are QSFP port numbers 0-3 and 8-11. The second ICL POD license enables all UltraScale ICL QSFP ports on each core blade of the director.
>
> **On the Brocade X6-4:**
>
> On the X6-4, the first ICL POD license enables 4 UltraScale ICL QSFP ports on each core blade of the director, which are QSFP port numbers 0, 1, 4, and 5. The second ICL POD license enables all UltraScale ICL QSFP ports on each core blade of the director.

On the Brocade X7-8:

On the X7-8, the first ICL POD license enables 4 UltraScale ICL QSFP ports on each core blade of the director, which are QSFP port numbers 0, 1, 8, and 9. The second ICL POD license on the X7-8 enables 8 UltraScale ICL QSFP ports on each core blade of the director, which are QSFP port numbers 0-3 and 8-11. The third ICL POD license on the X7-8 enables 12 UltraScale ICL QSFP ports on each core blade of the director, which are QSFP port numbers 0-5 and 8-13. The fourth ICL POD license on the X7-8 enables all UltraScale ICL QSFP ports on each core blade of the director.

On the Brocade X7-4:

On the X7-4, the first ICL POD license enables 4 UltraScale ICL QSFP ports on each core blade of the director, which are QSFP port numbers 0, 1, 4, and 5. The second ICL POD license on the X7-4 enables all UltraScale ICL QSFP ports on each core blade of the director.

Extension Upgrade License – The Extension Upgrade license is available on the Brocade 7810, enabling additional ports, capacity, and features that provide the following: 12 32Gb/s FC ports, 4 tunnels, 6 circuits per tunnel, 2.5Gb/s WAN throughput, Fabric Vision, Extension Trunking, Brocade ISL Trunking, Integrated Routing Ports on Demand, and Brocade Extended Fabrics. This license is shown as a combination of existing FOS licenses that enable the above capabilities and features.

NOTE   FOS v8.2.2 and later supports 6 10Gb/s Ethernet ports in base configuration of Brocade 7810. 10 Gb/s Ethernet ports can be enabled without the Extension Upgrade license.

5.2   Temporary License Support

The following licenses are available in Fabric OS 9.0 as either universal temporary or regular temporary licenses:

- Fabric (E_Port)
- Extended Fabric
- Trunking
- Integrated Routing
- Integrated Routing Ports on Demand
- FICON Management Server (CUP)
- Fabric Vision
- Extension Upgrade

NOTE   Temporary licenses for features available on a per-slot basis enable the feature for any and all slots in the chassis.

Temporary and universal temporary licenses have durations and expiration dates established in the licenses themselves. FOS will accept up to two temporary licenses and a single universal license on a unit. Universal temporary license keys can be installed only once on a particular switch, but they can be applied to as many switches as desired. Temporary use duration (the length of time for which the feature will be enabled on a switch) is provided with the license key. All universal temporary license keys have an expiration date after which the license can no longer be installed on any unit.

Temporary or universal temporary license for Extension Upgrade do not enable additional ports on 7810.

Chapter 6: Hardware Support

6.1   Supported Devices

The following devices are supported in this release:

- Brocade X7-8 Director
- Brocade X7-4 Director
- Brocade X6-8 Director
- Brocade X6-4 Director
- Brocade G720 Switch
- Brocade G630 Switch
- Brocade G620 Switch
- Brocade G610 Switch
- Brocade G648 Blade Server SAN I/O Module
- Brocade MXG610 Blade Server SAN I/O Module
- Brocade 7810 Extension Switch

6.2   Supported Blades

6.2.1   X6-8 and X6-4 Blade Support

Fabric OS 9.0 software is fully qualified and supports the blades for the X6-8 and X6-4 as noted in the following table.

Blades	FOS v9.0 Support
FC32-48 32G FC blade	Supported.
SX6 Gen 6 Extension blade	Supported. Up to a maximum of four blades of this type.
FC32-64 32G FC/FCoE blade	Supported.

6.2.2   X7-8 and X7-4 Blade Support

Fabric OS 9.0 software is fully qualified and supports the blades for the X7-8 and X7-4 as noted in the following table.

Blades	FOS v9.0 Support
FC32-X7-48 32G X7 FC blade	Supported.
FC64-48 64G FC blade	Supported
FC32-48 32G FC blade	Supported.
SX6 Gen 6 Extension blade	Supported. Up to a maximum of four blades of this type.
FC32-64 32G FC/FCoE blade	Supported.

6.3   Supported Power Supplies

For the list of supported power supplies for Brocade X6 and power supply requirements, refer to the Brocade X6 Director Technical Specifications section of *Brocade X6-8 Director Hardware Installation Guide* and *Brocade X6-4 Director Hardware Installation Guide*.

For the list of supported power supplies for Brocade X7 and power supply requirements, refer to the *Brocade X7 Director Technical Specification*.

6.4   Supported Optics

For a list of supported fibre optic transceivers that are available from Brocade, refer to the latest version of the *Brocade Transceiver Support Matrix* available online at www.broadcom.com.

Chapter 7: Software Upgrades and Downgrades

7.1   FOS Image Filenames

Image Filename	Description
v9.0.1a.zip	Fabric OS v9.0.1a for Windows
v9.0.1a.tar.gz	Fabric OS v9.0.1a for Linux
v9.0.1a.md5	Fabric OS v9.0.1a MD5 Checksums
v9.0.1a_all_mibs.tar.gz	Fabric OS v9.0.1a SNMP MIBs
v9.0.1a_yang.tar.gz	Fabric OS v9.0.1a YANG
v9.0.1a_releasenotes_v2.0.pdf	Fabric OS v9.0.1a Release Notes

The image files can be downloaded from https://www.broadcom.com/mybroadcom, with the exception of YANG files which are available on https://www.broadcom.com.

7.2   Migration Path

This section contains important details to consider before migrating to or from this FOS release.

7.2.1   Migrating from FOS 9.0.0

Brocade X7 and G720, upgrades from FOS v9.0.0 to FOS v9.0.1a are disruptive. Disruptive upgrade from FOS v9.0.0 to v9.0.1a using the optional -s parameter with the `firmwaredownload` command is supported. Non-disruptive upgrade from FOS v9.0.0 to FOS v9.0.1a on other platforms is supported.

Brocade X6 and G630 platforms upgraded from any FOS v8.x release to FOS v9.0.0 or v9.0.0a must first upgrade to FOS v9.0.0b prior to migrating to FOS v9.0.1a.

7.2.1.1   Migrating from FOS 8.2

Any Brocade platform listed in the **Supported Device** section running any FOS 8.2 version can be non-disruptively upgraded to FOS 9.0.1a.

7.2.1.2   Migrating from FOS 8.1

Any Brocade platform listed in the **Supported Device** section running any FOS 8.1 version must be upgraded to FOS 8.2.x firmware before it can be non-disruptively upgraded to FOS 9.0.1a.

7.3   Upgrade/Downgrade Considerations

Disruptive upgrades to Fabric OS 9.0.1a are allowed and are supported from FOS 8.1.x (up to a two-level migration) using the optional -s parameter with the `firmwaredownload` command.

On Gen 7 platforms, firmware downgrades from FOS v9.0.1a are not allowed when 64G optics are installed.

On a Brocade G610, firmware downgrades from FOS 9.0.1a to FOS 8.2.0x or earlier versions are not allowed.

On a Brocade G620 with the `switchShow` command displaying "switchType" field identified as 162.5, the minimum required FOS version is v8.2.1a. Firmware downgrades to FOS 8.2.1 or earlier versions are not allowed.

On a Brocade G620 with `switchType` as 183 or a Brocade G630 with `switchType` as 184, the minimum required FOS version is FOS v9.0.0. Firmware downgrades to FOS v8.2.x or earlier versions are not allowed.

On any Brocade SAN switch platform, firmware upgrade to FOS v9.0.0 or later must acknowledge and accept the EULA before FOS can be installed. On any Brocade SAN switch platform running FOS v9.0.0 or later, firmware upgrade or downgrade must acknowledge and accept the EULA before FOS can be installed.

On a Brocade X6 director with SX6 blades and port channels configuration, firmware downgrades from FOS v9.0.0 or later to FOS v8.2.x should downgrade to 8.2.2c or 8.2.1e first to avoid CP crash.

On Brocade X7 director and G720 switch, non-disruptive upgrade from FOS 9.0.0 to this release is not supported. On these platforms, upgrade from FOS 9.0.0 using the optional `-s` parameter with the `firmwaredownload` command is supported. In addition, firmware downgrade from this release to FOS v9.0.0 on these platforms is blocked. Performing `firmarecleaninstall` to FOS v9.0.0 on these platforms should be avoided.

On Brocade 7810 and Brocade X6 director with SX6 blade with following optics part number installed, firmware downgrade from this release to FOS v8.2.2b or earlier is blocked:

- 32Gb/s Fibre Channel SWL SFP (part number 57-1000485-01)
- 32Gb/s Fibre Channel LWL SFP (part number 57-1000486-01)
- 16Gb/s Fibre Channel SWL SFP (part number 57-1000487-01)
- 16Gb/s Fibre Channel LWL SFP (part number 57-1000488-01)
- 16Gb/s Fibre Channel ELWL SFP (part number 57-1000489-01)

Refer to the *Brocade Fabric OS Software Upgrade User Guide* for detailed instructions on non-disruptive and disruptive upgrade procedures.

Chapter 8: Limitations and Restrictions

This chapter contains information that you should consider before you use this Fabric OS release.

8.1   Scalability

All scalability limits are subject to change. Limits may be increased once further testing has been completed, even after the release of this version of the Fabric OS software. For current scalability limits for Fabric OS software, refer to the Brocade SAN Scalability Guidelines for Brocade Fabric OS 9.X document.

8.2   Compatibility/Interoperability

8.2.1   Brocade SANnav Management Portal Compatibility

Brocade SANnav Management Portal and Global View are new SAN management software offerings for Brocade SAN environments. There are two distinct SANnav product offerings:

- Brocade SANnav Management Portal
- Brocade SANnav Global View

Brocade SANnav Management Portal allows management of one or more SAN fabrics that are in the same or different geographical locations and supports up to a maximum of 15,000 physical SAN ports. For environments that are larger than 15,000 ports, users can deploy multiple SANnav Management Portal instances.

Brocade SANnav Global View is a higher-level management application that provides visibility, summarization and seamless navigation across multiple SANnav Management Portal instances. Users can drill-down to any individual SANnav Management Portal instance from SANnav Global View to perform detailed monitoring, investigation, and troubleshooting.

The SANnav Management Portal 2.1.1 supports managing SAN switches running Fabric OS up to v9.0.1a. Compatibility with FOS versions can be found in the SANnav Management Portal 2.1.1 Release Notes.

The SANnav Management Portal 2.1.1 supports firmware migration from FOS v8.2.1d or later and from FOS v8.2.2a or later to FOS v9.0.0 or later, which requires FOS EULA acceptance. Migration directly from FOS v8.2.2 or from FOS v8.2.1c or earlier versions to FOS v9.0.x using SANnav is not supported. Switches must migrate to FOS v8.2.1d or later or to FOS v8.2.2a or later as a first step, then migrate to FOS v9.0.0 or later as the final step.

8.2.2   Brocade Network Advisor Compatibility

Brocade Network Advisor does not support managing SAN switches running Fabric OS v9.0.0 or later. Brocade Network Advisor Release Notes provide details on supported FOS versions.

8.2.3   Web Tools Compatibility

Web Tools supports firmware migration from FOS v8.2.1d or later and from FOS v8.2.2a or later to FOS v9.0.0 or later. To migrate from FOS v8.2.2 or from FOS v8.2.1c or earlier versions to FOS v9.0.0x using Web Tools, switches must migrate to FOS v8.2.1d or later or to FOS v8.2.2a or later as a first step, then to FOS v9.0.0 or later as the final step.

NOTE   WebTools will always show English language irrespective of Browser or Operating System language setting.

8.2.4　Fabric OS Compatibility

- The following table lists the earliest versions of Brocade software supported in this release, that is, the earliest supported software versions that interoperate. Use the latest software versions to get the greatest benefit from the SAN.

- To ensure that a configuration is fully supported, always check the appropriate SAN, storage, or blade server product support page to verify support of specific code levels on specific switch platforms before installing on your switch. Use only Fabric OS versions that are supported by the provider.

- For a list of the effective end-of-availability dates for all versions of Fabric OS software, refer to the *Brocade Software End of Availability Notice* published to the Brocade Product End-of-Life web page https://www.broadcom.com/support/fibre-channel-networking/eol.

- For the latest support and posting status of all release of Brocade Fabric OS, refer to the *Brocade Software: Software Release Support and Posting Matrices* published to the Brocade Product End-of-Life web page https://www.broadcom.com/support/fibre-channel-networking/eol.

Supported Products	Fabric OS Interoperability
Brocade 5424, 5430, 5431, 5432, 5450, 5460, 5470, 5480, NC-5480	FOS 7.4.2 or later (Not compatible in the same fabric. Must use FCR or connect as AG)
Brocade 300	FOS 7.4.2 or later (Not compatible in the same fabric. Must use FCR or connect as AG)
Brocade 7800	FOS 7.4.2 or later (Not compatible in the same fabric. Must use FCR)
Brocade DCX 8510-8/DCX 8510-4	FOS 8.1.0 or later
Brocade DCX 8510-8/DCX 8510-4 with FC16-64 blade	FOS 8.1.0 or later
Brocade 6505, 6510, 6520, 7840	FOS 8.1.0 or later
Brocade 6542	FOS 8.1.0 or later
Brocade 6543	FOS 8.1.0 or later
Brocade 6547, 6548, M6505, 6545, 6546	FOS 8.1.0 or later
Brocade 6558	FOS 8.1.0 or later
Brocade G610	FOS 8.1.0 or later
Brocade G620 (switchType 162)	FOS 8.1.0 or later
Brocade G620 (switchType 183)	FOS 9.0.0 or later
Brocade G630 (switchType 173)	FOS 8.2.0 or later
Brocade G630 (switchType 184)	FOS 9.0.0 or later
Brocade 7810	FOS 8.2.1 or later
Brocade X6-8/X6-4	FOS 8.1.0 or later
Brocade X6-8/X6-4 with FC32-64 blade	FOS 8.2.0 or later
Brocade G720	FOS 9.0.0 or later
Brocade X7	FOS 9.0.0 or later

Brocade MXG610[1]	FOS 9.0.0 or later [2]
Brocade G648[3]	FOS 9.0.0 or later[2]

8.2.5   SNMP Support

Fabric OS 9.0.1 documents the supported MIBs in the *Brocade Fabric OS MIB Reference Manual*. For information about SNMP support in Fabric OS software and how to use MIBs, refer to the *Brocade Fabric OS Administration Guide for Fabric OS 9.0.X*.

8.2.6   Obtaining MIBs

You can download the MIB files required for this release from the Downloads area of the myBroadcom site. To download the Brocade-specific MIBs, you must have a user name and password. Perform the following steps.

1.   Go to https://www.broadcom.com/mybroadcom/, click **Login**, and enter your username and password.

If you do not have an account, click **Register** to set up your account.

2.   Select **Customer Support Portal** > **DocSafe (Software/Document Downloads)**.

3.   Enter the product name or the software version number in the **Search** box. For example, the following search is for software and documentation files for software version 9.0.

Search Downloads

	Recent Documents | My Bookmarks | My Bookmarks Folders ∨ ✚ | My Saved Searches ∨ | Historical Downloads (Requested via Email download link)
Product Search... **OR** 9.0	Search
Partial Keyword Allowed	∨Advanced Search

4.   When the list of file appears, clear the **Documents** box.

5.   Navigate to the link for the MIBs package and download the file to your drive.

Distribution of standard MIBs has been stopped. Download the required standard MIBs from the http://www.oidview.com/ or http://www.mibdepot.com/ or https://www.simpleweb.org/ietf/mibs/ .

8.2.7   REST API Support

Fabric OS 9.0.0 documents the supported REST API functions in the *Brocade Fabric OS REST API Reference Manual*.

8.2.7.1   Obtaining YANG Files

YANG is a standard data modelling language that defines the data sent over the FOS REST API. Each FOS REST API module is defined in a YANG module file with a .yang name extension. To download the Brocade FOS-specific YANG files from the Broadcom website, perform the following steps:

1.   Go to https://www.broadcom.com/

.

---

[1] Brocade MXG610 is also supported with FOS v8.1.0_lnx2 release.

[2] Support merged from embedded FOS releases to mainline FOS releases.

[3] Brocade G648 is also supported with FOS v8.2.0_gft release.

2. Select **Group "Fibre Channel Networking", Family "Fibre Channel Networking"** and search for keyword **"YANG".**

3. The YANG files can be located under the Programming Guide category.

4. Navigate to the link for the Fabric OS package file, either for Windows or for Linux, and download it to your disk.

5. Unzip or untar the Fabric OS package file; the `yang.tar.gz` file contains the collection of YANG module files that this FOS release version supports. Untar the `yang.tar.gz` file to obtain individual YANG module files.

Alternatively, download the YANG files for a specific FOS version from https://github.com/brocade/yang.

8.3   Important Notes

8.3.1   Access Gateway

- The 32G links with 4x32G QSFP ports (port 48 to port 63) do not have default mappings. These ports will be disabled by default when a Brocade G620 is enabled for Access Gateway mode or when the configuration is set to the default.
- Attempts to remove failover port mapping from N_Port number 0 on an Access Gateway fail. This problem does not exist on other N_Port numbers.
- Brocade G620 with switchType 183, G630 with switchType 184, and FC32-X7-48 blades do not support N-port connection from 4Gbps Access Gateway.

8.3.2   Brocade Analytics Monitoring Platform

FOS 9.0.x supports vTap on Brocade legacy Gen 6 platforms to be monitored by the Brocade Analytics Monitoring Platform. The supported Brocade platforms include: G610, G620, G630, X6-4, and X6-8.

8.3.3   ClearLink Diagnostics (D_Port)

Fabric OS 9.0 supports D_Port tests between two Brocade switches and between Brocade switches and Gen 5 (16Gb/s) and Gen 6 (32Gb/s) Fibre Channel adapters from QLogic and Emulex. The following are specific adapter models and driver versions supported by Brocade with Fabric OS 9.0 for ClearLink.[4]

	Emulex 16G Adapter	Emulex 32G Adapter	Emulex Gen 7 Adapter	QLogic 16G Adapter	QLogic 32G Adapter
Adapter Model	LPe16002B-M6	LPe32002-M2	LPe35002 LPe35004	QLE2672	QLE2742
Adapter Firmware	12.6.182.8	12.6.182.8	12.6.182.8	v8.08.203	v8.08.231
Adapter Driver	12.6.165.0	12.6.165.0	12.6.165.0	STOR Miniport 9.3.3.20	STOR Miniport 9.3.3.20

---

[4] Adapter firmware or driver versions that are later than the ones listed in the table may not work.

D_Port tests will fail between a port with a 64G optic on a switch or director operating with FOS v 9.0.1a and a port on a G720, X7, G620 (switchType 183), or G630 (switchType 184) operating with FOS v9.0.0x. Any of these platforms operating with FOS v9.0.0x should be upgraded to FOS v9.0.1a or later prior to running D_Port tests to a 64G optic.

8.3.4   Diagnostic POST

- If Diagnostic POST is enabled, `supportSave` should not be started until the POST tests are completed after a switch or director boots up. Starting `supportSave` collection when POST tests are still running can result in unpredictable behaviour.
- Running `systemverification` with the increased `no.of.runs` parameter in a Director with an FC32-64 blade can cause test failures to be reported. Limit the number of runs to less than four (4).

8.3.5   Ethernet Management Interface

- The recommended interface speed configuration for a Brocade G620 is 1G auto-negotiate. If a G620 is configured for 10/100M Gb/s forced-speed and fails to establish a link, use a cross-over cable.
- If a Brocade switch management interface is running at 10 Mb/s, certain FOS operations such as `firmwaredownload` may fail.
- The 10Gb/s management interface on CPX6 blades is not supported.
- Half-duplex mode is not supported since FOS v8.1.x and is blocked.
- The `ethif --reseterror` command option is not supported in FOS v9.0.

8.3.6   Extension

Extension between a Brocade 7810 or SX6 running FOS v9.0 and a Brocade 7840 is supported only if the 7840 is running FOS 8.2.1 or later. The following table documents the combinations.

Site1 Switch/Blade	Site1 Firmware	Site2 Switch/Blade	Site2 Firmware
7840	8.2.1 or later	7840	8.2.1 or later
SX6	9.0.0 or later	7840	8.2.1 or later
7810	9.0.0 or later	7840	8.2.1 or later

8.3.7   FCoE

The following topologies for FCoE on the FC32-64 are not supported with FOS 9.0.x:

- Cisco UCS server directly connected to the FC32-64 without a Fabric Interconnect module.
- Cisco UCS server with a Fabric Interconnect module connected to the FC32-64 via a Nexus 5000 series switch in between. Neither running FCoE NPV mode nor L2 switching mode on the Nexus 5000 is supported.
- FCoE devices are supported in edge-to-edge fabric topology. They are not supported in edge-to-backbone fabric topology over FCR configurations.

8.3.8   FC-NVMe

- FC-NVMe is supported in edge-to-edge fabric topology with device type information (e.g. Initiator or Target) over FCR configurations.
- FC-NVMe is supported in edge-to-backbone fabric topology without device type information over FCR configurations.

8.3.9   FICON

For FICON-qualified releases, refer to the Additional Considerations for FICON Environments section of the Appendix for details and notes on deployment in FICON environments. (This appendix is included only for releases that have completed FICON qualification.)

8.3.10   Forward Error Correction

- FEC is mandatory with Gen 6 and Gen 7 Fibre Channel operating at 32Gb/s or higher bandwidth. This means that the `portcfgfec` command applies only to ports that are running at 16Gb/s or 10Gb/s.
- FEC capability is not supported with all DWDM links. This means that FEC may need to be disabled on 16Gb/s or 10Gb/s ports when using DWDM links with some vendors. This is done using the `portcfgfec` command. Failure to disable FEC on these DWDM links may result in link failure during port bring-up. Refer to the *Brocade Fabric OS 9.x Compatibility Matrix* for supported DWDM equipment and restrictions on FEC use.

8.3.11   MAPS

MAPS monitoring of UCS server login does not support the FENCE action even though the `mapsrule` command does not block the configuration.

8.3.12   Security

- FOS v9.0 requires passwords for **admin** and **user** accounts to be changed from default password string "password". In the following scenarios, default password may still be present in FOS v9.0. It is recommended to change the password in this scenario or at the next login prompt:
  - A default password is used in an earlier FOS version. FOS is upgraded from the earlier FOS version to FOS v9.0.x.
  - A default password is used in an earlier FOS version on active CP. The standby CP runs FOS v9.0.x and becomes active due to HA failover.
  - A default password is used in an earlier FOS version. Password is distributed from the earlier FOS version to FOS v9.0.x.
- It is recommended to reconfigure shared secrets for F_Port authentication between Access Gateway and switch before firmware upgrade to FOS v9.0.x. The shared secrets should be configured as given in the following table.

Access Gateway FOS Version	Edge Switch FOS Version	Shared Secret Configuration
Pre-v9.0.0	9.0.0 or later	AG local secret = Switch local secret AG peer secret = Switch peer secret
9.0.0 or later	9.0.0 or later	AG local secret = Switch peer secret AG peer secret = Switch local secret

- It is recommended to reconfigure shared secrets for F_Port authentication between HBAs and a switch before the switch is upgraded to FOS v9.0.0 or later. Without reconfiguration, shared secrets configured in earlier FOS versions will fail F_Port authentication when a device port resets. The shared secrets should be configured as given in the following table.

FOS Version	Shared Secret Configuration
Pre-v9.0.0	Device local secret = Switch local secret Device peer secret = Switch peer secret
9.0.0 or later	Device local secret = Switch peer secret Device peer secret = Switch local secret

- FOS v9.0 does not support F_Port authentication to Marvell QLogic BR series (Former Brocade Product Line) HBAs as these HBAs only support legacy Brocade F_Port authentication. For these devices to connect to FOS v9.0, F_Port authentication must be disabled.

- FOS v9.0 does not support F_Port trunking when F_Port authentication is enabled.

- When FIPS-Inside is enabled in FOS v9.0, only integrity test will run. Self-tests will not run.

- If users configure any duplicated Virtual Fabric (VF) list with `ldapcfg –mapattr <ldaprole>` command, only the first mapping from the list will be used during LDAP authentication and authorization.

- FOS 9.0 default cipher string will support additional ciphers. To maintain equivalent ciphers as in versions earlier than 9.0.0, please use the cipher string '!ECDH:!DH:HIGH:-MD5:!CAMELLIA:!SRP:!PSK:!AESGCM:!AESCCM:!ARIA:DES-CBC3-SHA' in the secCryptoCfg templates.

- If users had configured syslog cipher in FOS 8.1.0b or later, then firmware downgraded the switch to FOS 8.1.0a, the switches are recommended upgrade to 8.1.0b or later first before upgrading to FOS v9.0.0 or later.

- FOS 9.0 requires role mapping or VSA attributes to be configured for LDAP user authentication in a VF enabled switch. In a non-VF switch, `ldapcfg --maprole` is mandatory. It should be configured before upgrading to FOS v9.0 to avoid login failure for LDAP users.

- Users must specify the domain of an LDAP server when adding the LDAP server to the remote AAA configuration of a switch.

- Self-signed certificates generated in FOS v9.0.0 for HTTPS may report warnings when used with some applications. The certificate may need to be re-generated after upgrade to FOS v9.0.0a using the command `seccertmgmt generate -cert https`.

- Optional certificate extensions, such as BasicConstraints, KeyUsage, and ExtendedKeyUsage are ignored when a certificate containing these is imported in basic mode. During session establishment, the extensions are validated. Hence, invalid extensions will be rejected and result in session failure.

- Login of LDAP users using Distinguished Name (DN) will be supported only for the users created in container "Users" of the domain configured in the switch, even though the switch is configured with Global Catalog (GC) port of the server. Login using User Principal Name (UPN) and sAMAccountName will be supported irrespective of the domain and OU on which the user is created.

8.3.13   Zoning

- If there are TI Zones or unsorted zones in a configuration file downloaded by `configdownload` and the zones do not already exist in the zoning database when `configdownload` runs, the membership list of any zones in the configuration file will be automatically sorted. If the TI Zones or unsorted zones that are downloaded already exist in the zone database, then the member lists will remain unsorted. As a result, when a switch is enabled after `configdownload`, port segmentation may occur due to adjacent switches having the same zones with unsorted membership lists. To avoid this condition, users should not run `cfgClear` before `configdownload`. Users can recover from segmentation by executing `cfgDisable`, `cfgClear`, and `cfgSave` operations to clear the zoning database from one side of the segmented fabric. Note that these steps should only be performed if the zone database is the same on the `configdownload` switch as it is on the rest of the fabric. After segmented ISL ports are re-enabled, zone merge can proceed.

- After an X6 director completes the field migration to upgrade to X7 director, (Domain, Index) (D,I) zones must be converted to the new index assigned to X7 directors that follow unified addressing mode assignment.

8.3.14   Brocade X6 Field Migration

- Field migration of a Brocade X6 to an upgraded X6 for Gen 7 director is supported with firmware upgrade to FOS v9.0.0x or FOS v9.0.1x. Refer to the *Brocade X6 Field Migration Guide* for step by step instructions.

- During field migration of Brocade X6 to a field upgraded X6 with Gen 7 support, the `portcfgupload` file will contain `portcfgtrunkport` commands for ICLs. A warning message is displayed to indicate that the command is not valid for ICL ports because trunking cannot be disabled on ICLs. This warning will not affect the ICLs and is harmless.

8.3.15   Miscellaneous

- Brocade X7 directors have pre-installed Brocade Trusted FOS (TruFOS) Certificates. Although TruFOS Certificates do not currently enable any features or functionality, certificate status is available in the `license --show` command output, and MAPS monitors and alerts for upcoming expiration in default policies. New or updated TruFOS Certificates can be obtained by contacting your support provider.

- On a switch configured with Virtual Fabrics, SNMP will dispatch the traps/informs only from Virtual Fabrics that the user associated with the SNMPv3 traps/informs the receiver has access to.

- After a power supply unit is removed from a Brocade G620, the `historyshow` command may miss the entries for this FRU removal or insertion event. In addition, the RASLog error message EM-1028 may be logged when the power supply is removed. This condition can be corrected by power-cycling the switch.

- After running offline diagnostics mode 1 on QSFP ports, a Brocade G620 must be rebooted before operational use.

- After running offline diagnostics with `portledtest`, `portloopbacktest`, or `turboramtest` commands on FOS v9.0.x, Brocade G630 with swtichType 184 must be rebooted before operational use.

- All links in an ICL QSFP connection on a Brocade X6 Director must be configured to the same speed using the `portcfgspeed` command from one of the following supported speeds: 16Gb/s, 32Gb/s, or ASN. To connect an ICL from an X6 with a 4x32GFC breakout optic (P/N 57-1000351-01) or a 4x16G FC optic to a 4x16G FC optic in a DCX 8510, the X6 port's speed must be set to 16Gb/s.

- Brocade G630 LEDs illuminate amber and green during power-up.

- The CLI command option `snmpconfig` -set `accesscontrol` is planned to be deprecated in the next major release.

- When replacing a FC32-64 blade with a FC32-48 blade, flexport and FCoE configurations should be removed before the FC32-64 blade is removed.

- Enhanced checks are performed on optics during firmware upgrade to FOS v9.0.0. Firmware download is blocked if unsupported optics are discovered. The scanning of the optics takes a few minutes to complete. The amount of time it takes is dependent on the number of ports on a switch. On a fully loaded eight (8) slot director, it can take up to five (5) minutes to complete. In addition, ports with optics that fail the enhanced checks in FOS v9.0 will not be able to come online due to the optics as invalid module.

- Brocade G620 with `switchType` 183 and G630 with `switchType` 184 do not support the following legacy optical modules:

  - 16G SWL (HAA1, HAA2 serial number)
  - 16G LWL (HDA1, HDA2, HDA3 serial number)
  - 32G QSFP SWL (ZTA serial number)

    The following examples show the `sfpShow` CLI outputs with the serial numbers of the legacy optical module

    ```
    sfpshow <port> -f
    ...
    Serial No: HAA11213107BTY2
    ...

    sfpshow <port> -f
    ....
    Serial No: HDA318014000DN1
    ....

    sfpshow <port> -f
    ....
    Serial No: ZTA11517000001K
    ```

- All user ports in a Gen 7 ICL QSFP port must be assigned to the same logical switch when Virtual Fabric is configured. Port 0 of the ICL QSFP must be enabled first before port 1, port 2, and port 3 within the same QSFP be enabled. If port 0 of the Gen 7 ICL QSFP becomes offline, port 1, port 2, and port 3 of the QSFP will become offline as result.

▪ The output of CLI command `sfpShow` or any other interfaces to retrieve information from Gen 7 SWL QSFP (Part Number 57-1000490) and LWL QSFP (Part Number 57-1000491) does not match the Part Numbers on the media sticker labels. The output shows Gen 6 Part Number (57-1000351 for SWL or 57-1000480 for LWL). This does not affect operation of the optics.

▪ When a fabric with FOS v9.0.0 is connected to a fabric with pre-FOS v9.0.0, RASLOG message FABR-1001 is generated as shown in the following example. This is an expected message.

    `[FABR-1001], 35, FID 128, WARNING,, port 62, incompatible VC count`

▪ FOS v9.0 has disabled directory listing in CLI shell. As a result, entering <tab><tab> key does not list all CLIs available. Users can enter help command to list the commands. The shell tab completion by entering the first letter followed by <tab> key is supported.

▪ The FCR support of "Long Distance Fabric" mode conflict cannot coexist with long distance port configuration. If long distance mode (LD, LS, or LE) is enabled on the EX_Port and the EX_Port detected Backbone Fabric's "Long distance fabric" configuration is different from the connected Edge Fabric's "Long distance fabric" configuration, then the EX_Port will be disabled.

▪ If "Long Distance Fabric" is enabled on a switch via the `configure` command, it is recommended to upgrade the switch from FOS v8.2.x directly to FOS v9.0.0a or later. If the "Long Distance Fabric" configuration is enabled on an E_Port or EX_Port, firmware upgrade or downgrade to FOS v9.0.0 will effectively cause the "Long Distance Fabric" configuration to be disabled.

▪ If an HTTPS certificate is installed on a switch in FOS v9.0, HTTP access is blocked by default as HTTPS access is supported.

▪ When `portloopbacktest` mode1 test runs on multiple Gen 7 ICL ports with multiple iterations, the test may fail. The workaround is to run the test on one ICL port at a time with reduced number of iterations.

▪ Running long distance LE mode between any blades or switches among FC32-X7-48, FC64-48, or G720 with port QoS mode enabled and `vc_translation_link_init` mode enabled may result in frame timeouts. The workaround for this problem is to use LS or LD mode for long distance.

Chapter 9: Security Vulnerability Fixes

This section lists the Common Vulnerabilities and Exposures (CVEs) that have been addressed. Each CVE is identified by the CVE ID number. For the latest security vulnerabilities disclosures, please visit Brocade Security Advisories web page at https://www.broadcom.com/support/fibre-channel-networking/security-advisories

Brocade Fabric OS versions v9.0.0

CVE-2018-6449

Host Header Injection vulnerability in the http management interface in Brocade Fabric OS could allow a remote attacker to exploit this vulnerability by injecting arbitrary HTTP headers.

Brocade Fabric OS versions v9.0.1

CVE-2020-11656, CVE-2020-13632, CVE-2020-13631, CVE-2020-13435, CVE-2019-19646, CVE-2019-16168, CVE-2019-19645, CVE-2020-13434, CVE-2020-13630

Various SQLite issues seen in SQLite versions through 3.31.1

Brocade Fabric OS versions v9.0.1a

CVE-2021-27792.

The request handling functions in the web management interface of Brocade Fabric OS versions do not properly handle malformed user input, resulting in a service crash.

CVE-2021-27791.

The function used to parse the Authentication header in the Brocade Fabric OS Web application service fails to properly process a malformed authentication header from the client, resulting in reading memory addresses outside the intended range.

CVE-2021-27790.

The command "ipfilter" in Brocade Fabric OS uses an unsafe string function to process user input.

CVE-2021-27789.

A vulnerability in the Brocade Fabric OS could allow an authenticated CLI user to abuse the history command to write arbitrary content to files.

CVE-2020-15388

The Web application of Brocade Fabric OS contains debug statements that expose sensitive information to the program's standard output device.

CVE-2020-15386

Brocade Fabric OS may observe high CPU load during security scanning, leading to a slower response to CLI commands and other operations.

CVE-2020-15383

Running security scans against the SAN switch can cause "config" and "secnotify" processes within the firmware to consume all memory leading to a denial of service impact, possibly including a switch panic.

CVE-2020-1971

The X.509 GeneralName type is a generic type for representing different types of names.

CVE-2020-1967

Server or client applications that call the SSL_check_chain() function during or after a TLS 1.3 handshake may crash due to a NULL pointer dereference resulting from incorrect handling of the "signature_algorithms_cert" TLS extension.

CVE-2020-11023

In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code.

CVE-2020-11022

In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code.

Chapter 10: Defects

10.1   Open in FOS 9.0.1a

Defect ID	Description
FOS-821746	Edge to edge routing was not working and frames dropped on E-port or EX-port.
FOS-823368	Flow's IO rate (number of IOs per second) and throughput (number of IOs bytes transferred per second) is diluted for READ when the device has only WRITE traffic and vice versa.
FOS-823433	In ISL between G720 or FC64-48 (64G optic) to a G630 (32G optic) may take longer time to converge at 32G speed. This is applicable when the G630 switch is running pre-FOS 9.0.1
FOS-823777	REST POST brocade-security/security-certificate-action returns generic error message "Operation Failed" on failure to import CA and identity certificates.
FOS-823842	CLI 'seccertmgmt show -ca -server <application>' does not display multiple CA certificates imported for an application.
FOS-824480	RAS message indicates verification failure of CA certificate on a switch with an expired FCAP switch certificate.
FOS-824516	ACL defined DB is cleared when the active policy is empty and 'distribute -p SCC|DCC|FCS -d <domains>' CLI is executed for peer domains.
FOS-824646	When AD legacy configuration for user authorization is set on the TACACS+ server and authorization translates to default FID128.
FOS-824735	Password distribution ('distribute' CLI) to AG switch results in "Error: Operation failed. Unknown error code - 9" message.
FOS-824778	Missing error handling when applying an invalid hex value to a 'mibcapability' configuration.
FOS-824782	Statistic counter for TELNET_POLICY ('secStatsShow' CLI) increments during SSH login failure.
FOS-824828	The D-Port tests may fail on one or more channels of a 32G QSFP port.
FOS-824948	SNMP swSsn OID returned as "none" instead of WWN on G610.
FOS-825008	Observed error "Error in operation" in response to "extncfg --config -clear -slot #"
FOS-825189	For SNMP oid ifName and ifAlias, interface names/Alias follows different naming format for FC and GE ports in respective output.

FOS-825192	SNMP OID "ifAlias" does not return a value for FCIP tunnels (VE port) when SNMP GET/WALK operations are executed.
FOS-825197	Audit log "SEC-3021" displays "username" as NONE when authentication fails.
FOS-825202	Audit log is not generated when LDAP authorization fails in non-VF mode.
FOS-825237	Occasional glitches reported in total byte count and total IO count when an external script pulls data at the same time flow statistics are being updated in the backend.
FOS-825360	"flow --show sys_flow_monitor" reports FC Statistics for some flows and no FC Statistics for other flows
FOS-825390	User logout messages are not consistent when there are a large number of user accounts on the setup.
FOS-825404	FC stats report 0 on the target port.
FOS-825413	'fipscfg --zeroize' CLI does not clear the authentication and privacy keys for SNMPv3 users for indexes 7 to 12.
FOS-825419	Switch allows import of FCAP certificate with WWN, in the Common Name field of certificate, different from switch WWN.
FOS-825527	SNMPv3 trap configuration is successful without user configuration.
FOS-825559	Audit log "SEC-3021" displays username as NONE.
FOS-825615	Flow monitoring reports valid IO statistics but FC statistics (Rx Frames Count, Rx Frames/second, Rx Bytes Count, Throughput and Average Frame size) are all reported with zero values.
FOS-825732	During warm recovery on an Access Gateway, FOS enables F-ports that are disabled by the user.
FOS-825768	swSfpPoweronHrs is returned as zero for some ports, whereas CLI displays a non-zero value.
FOS-825769	When IPv6 is defined in access control list, that particular IP is blocked for SNMP GET/SET operation
FOS-825815	Kernel panic in DP during fcippathtest
FOS-825841	QOS zoning based priority and SDDQ quarantine of flows from the port towards a slow-drain device are effective when CSCTL is enabled in the portcfg for the port.
FOS-826921	Following messages are printed on the console: INIT: Switching to runlevel: 6 IP Address update to trap sessions failed. IP Address update to trap sessions failed.
FOS-827149	"snmptraps --show" CLI command displays all traps even though only a sub-set of them are supported.

FOS-827216	MAPS default rule names are suffixed by the threshold, but the two rules have a discrepancy between the rule name and the threshold
FOS-827227	SNMP swConnUnitFECUnCorrectedCounter OID shows more port entries than what is present on the Chassis.
FOS-827409	Switch or chassis encounters an hafailover and results in a bring up failure after "ssl attributes" section of "configurechassis" CLI command
FOS-827757	Minimum quiet time for SFP monitoring system rules can be configured as 2 minutes for all the platforms.

10.2   Closed with Code Changes in FOS 9.0.1a

Defect ID	Description
FOS-813525	Fibre channel port statistics counters report large values such as "4294967295" after statistics reset.
FOS-813847	WebTools Name Server view does not show WWN Company ID for OUI 34:80:0d
FOS-815401	WebEm Netstat Metric value does not match the CLI value
FOS-816201	Date and audit logs in auditdump output shows timezone as "Localtime" when timezone is set in old format
FOS-817406	Blade does not initialize after a blade insert and raslog BL-5204 with reason=62.
FOS-819550	User login fails without error
FOS-819632	On firmware migration from 8.2.2 to 9.0.0 with 256 accounts, there will be 257 accounts due to maintenance and SSH/telnet fails for last account
FOS-819951	CLI command portledtest shows the test as passed but LEDs still continue to glow in any color.
FOS-819966	sys_flow_monitor dashboard displays port speed as 0 for host and target of the monitored flow.
FOS-820016	sys_flow_monitor dashboard is not reporting statistics on active flows and the state of the flow is deactivated after switchdisable and switchenable operation.
FOS-820266	Deletion of LDAP server IP configuration fails for IPV6
FOS-821501	Observed raslog NS-1012 "Detected duplicate WWPN".
FOS-821689	Customer unable to access storage after host F-port is enabled.

FOS-822104	User may experience FCIP ingress traffic stopped due to no more internal credits available and associated C3-1014/C3-1015 RASLOG messages on a 7840 platform or C4-1014/C4-1015 RASLOG messages in a chassis with an SX6 blade. In the case of an SX6 blade, the blade will be faulted after multiple attempts to recover internal credits.
FOS-822312	Performance degradation for FICON flows after FOS upgrade to FOS 8.2.1 or higher
FOS-822935	Occasional, a 32G LW optics port cannot come online.
FOS-822941	After a finite number of outstanding Fastwrite (FW) sequences FW processing will not generate a transfer ready sequence, but rather will shuttle the exchange (pass through mode). This will result in the pass through IOs experiencing higher IO response time when compared to the FW sequences. The FW sequence IOs will complete in as little as 1 Round Trip Time (RTT), whereas the pass through IOs will complete no sooner than 2 RTTs.
FOS-823710	Host cannot see Lun after device login.
FOS-825365	Enhancement to provide periodic raslog warning messages on the impending End Of Support (EOS) for the System and remove auditdump from EOS blocked commands.
FOS-825388	FCIP Tunnel up, but all I/O stops flowing over the tunnel and application timesout.
FOS-825441	After hareboot or reboot, POD license is not activated.
FOS-825673	Port is disabled with the reason of: Disabled (LD SFP is not supported in AG mode)
FOS-825683	Unable to upgrade FPGA due to sanity check failure.
FOS-825731	Audit/Raslog message[SEC-3050] is not generated after using CLI 'sshutil rekeyinterval' on a switch.
FOS-825979	SNMP service crashes and restarts.
FOS-826163	Fanshow/sensorshow shows "Below minimum" instead of "Faulty".
FOS-826171	TCL shows tunnel ID as -1 after modifying it for the target VE using ECM. Also IP-Extension traffic will not flow over the tunnel.
FOS-826186	MAPS 'logicalgroup --show' CLI displays more number of flows than that is present on the switch
FOS-827154	Enabling persistent PID on a switch can cause NPIV devices not to log in due to FDISC reject. In this case the I-Series will do an immediate LOGO. Once this happens, we do not preserve that PID. Instead, the same PID is handed out to the next device that logs in. It appears the host is misbehaving, but the switch is not handling the situation correctly.

10.3   Closed without Code Changes in FOS 9.0.1a

Defect ID	Description
FOS-809191	Brocade 7810 extension switch's secondary NTP server does not go to active state after the active NTP server goes down.
FOS-810530	Zone merge slow performance and failure on that switch that has defzone all access defined. Along with this behavior IPC drops RASLOGs events and/or termination of process nsd maybe seen.
FOS-816124	The raslog TS-1002 floods console indicating continuous toggling of active clock server between LOCL and external
FOS-816612	SX6 extension blade reboots when the standby CP is replaced.
FOS-817433	Error message "portPeerBeacon is not supported by the other end" with AG mode F-Ports.
FOS-818010	EDC and RDF registrations will complete successfully, however, the registered values are not retained when viewed using the "fabricNotification" CLI.
FOS-818869	inet6 address family not supported in 'netstat' command. S8Gen7:FID128:admin> netstat -A inet6 -nr Address family `inet6' not supported. S8Gen7:FID128:admin> netstat --help
FOS-819368	Config replay not working when using PATCH on /brocade-maps/group
FOS-820163	VLAN and MTU Size is not displayed in FCIP circuit view
FOS-820214	GET on /brocade-maps/monitoring-system-matrix/monitoring-system/IP_PKTLOSS/group-type/circuit returns 400 error message
FOS-821090	weblinkerfcgd core files are generated on the switch.
FOS-821268	Observed a weblinker process termination when generating certificate for HTTPS and flash space eventually went to over 90%.
FOS-823433	In ISL between G720 or FC64-48 (64G optic) to a G630 (32G optic) may take longer time to converge at 32G speed. This is applicable when the G630 switch is running pre-FOS 9.0.1

Revision History

Version	Summary of changes	Publication date
1.0	Initial version of document	3/10/2021
2.0	Added note to the Miscellaneous section clarifying TruFOS Certificate references	4/12/2021
3.0	Added the section "Security Vulnerability Fixes."	6/4/2021