BROCADE
A Broadcom Inc. Company

Fabric OS 8.2.1a

Brocade Fabric OS 8.2.1a Release Notes

Release Notes

Version 2.0

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

Online	Telephone
For non-urgent issues, the preferred method is to go to MyBrocade (my.brocade.com) and then go to one of the following sites: • My Cases • Software Downloads • Licensing tools • Knowledge Base	Required for Severity 1-Critical and Severity 2-High issues: • North America: 1-800-752-8061 (Toll-free) • International: 1-669-234-1001 (Not toll-free) Toll-free numbers are available in many countries and are 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.
- Broadcom Supplemental Support augments your existing OEM support contract, providing direct access to Brocade expertise. For more information, 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 behavior 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:

The serial number label is located as follows:

Brocade 6520, 6510, 6505, G630, G620, G610 – On the switch ID pull-out tab located on the bottom of the port side of the switch.

Brocade 7840, 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 DCX 8510-8 – Bottom right of the port side.

Brocade DCX 8510-4 – Back, upper left under the power supply.

Brocade X6-8, X6-4 – Lower portion of the chassis on the nonport 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 `licenseIdShow` command to display the license ID.

1.2 Related Documentation

White papers, data sheets, and the most recent versions of Brocade software and hardware manuals are available at www.broadcom.com.

Product documentation for all supported releases is available at www.broadcom.com and at MyBrocade to registered users. After logging into MyBrocade, click the **Support** tab and select **Document Library** to access documentation. Locate documentation by product or by operating system.

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

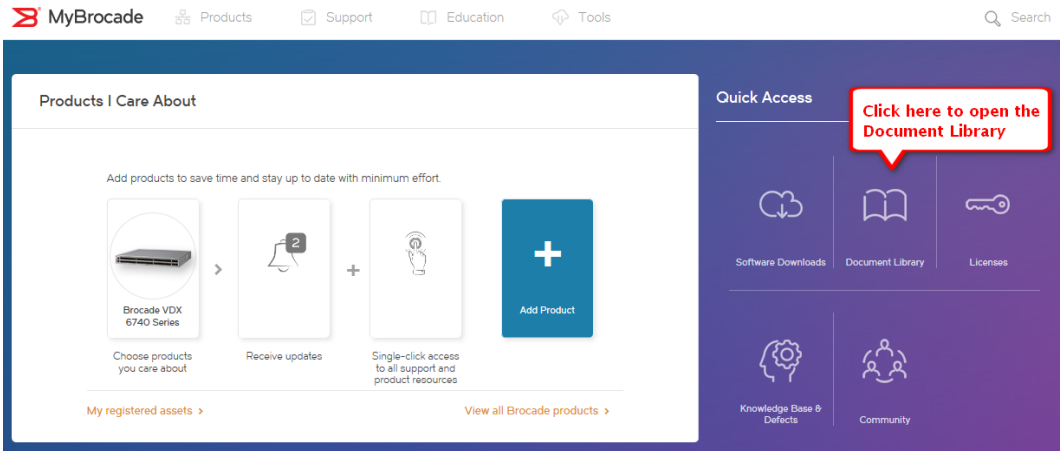
Chapter 2: Locating Product Manuals and Release Notes

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

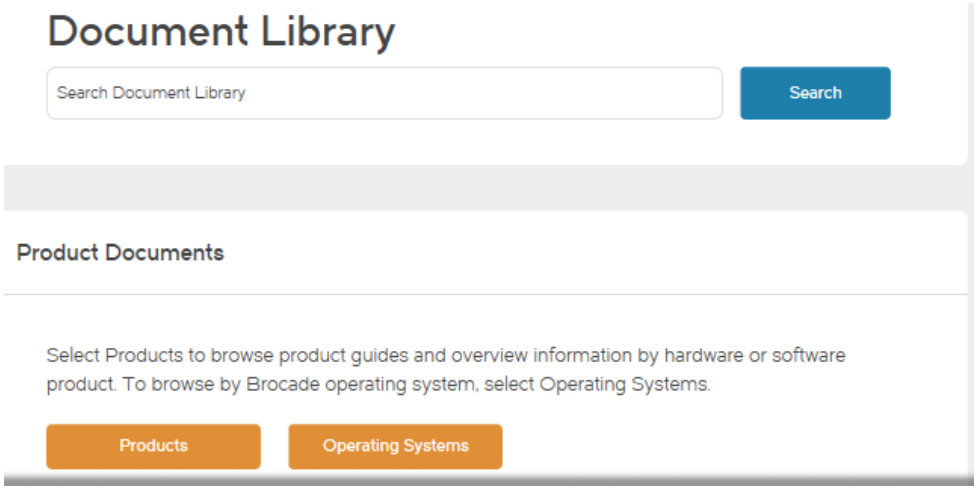
2.1 Locating Product Manuals

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

1. Open http://my.brocade.com and log in. If you do not have a login, registration is free. Click **Register Now** and follow the directions.
2. Once you have logged in, the product manuals can be found by clicking **Document Library**.

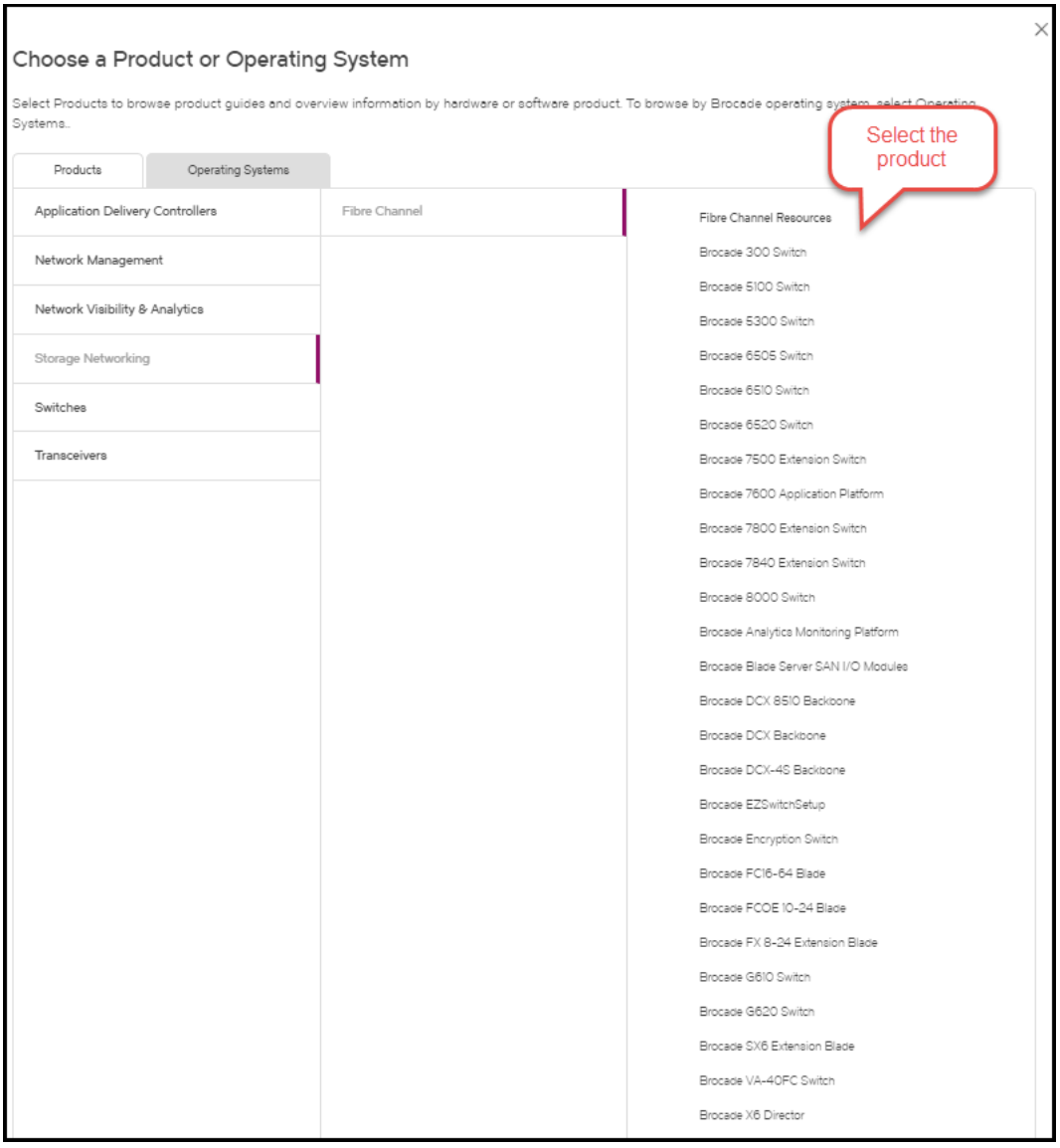


3. Select **Products** to browse product guides and overview information, or select **Operating Systems** to browse by Brocade operating system. Alternatively, you can enter a term in the search bar.

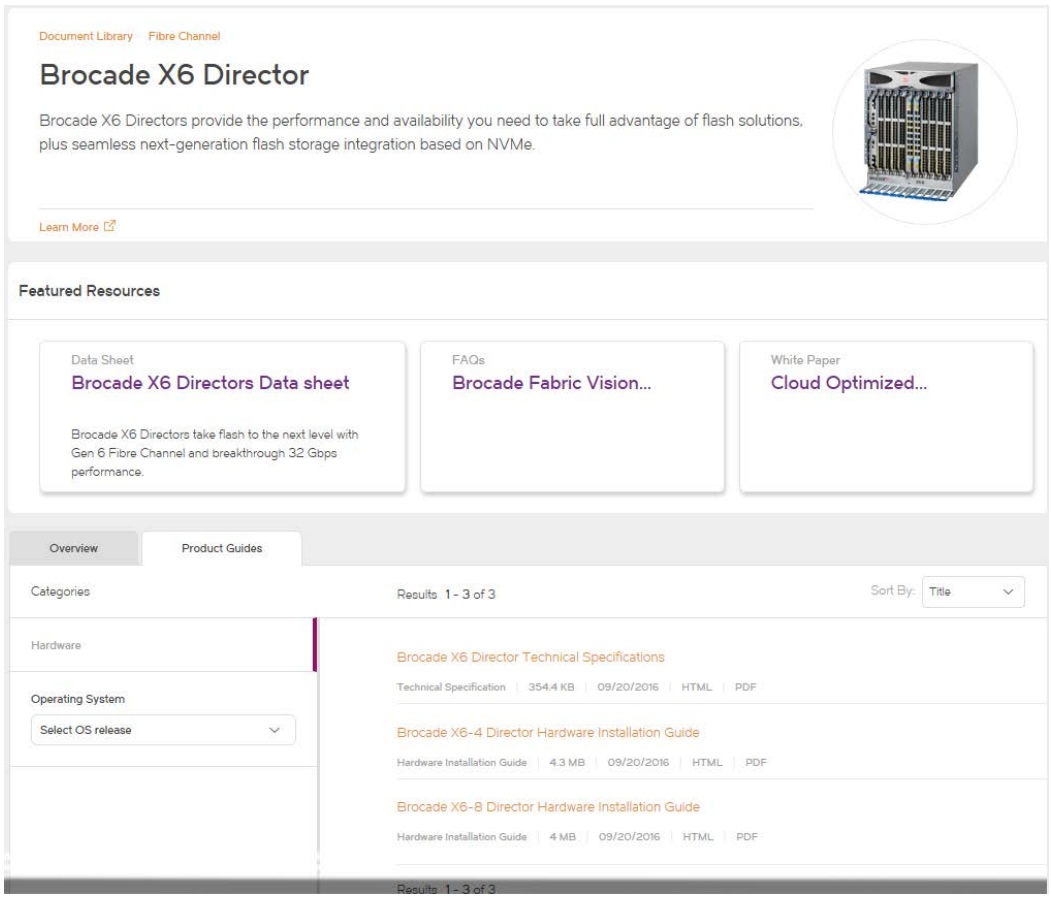


2.1.2 Selecting by Product

1. Click **Products, Storage Networking**, and then **Fibre Channel**. Choose your product from the **Fibre Channel Resources** list.



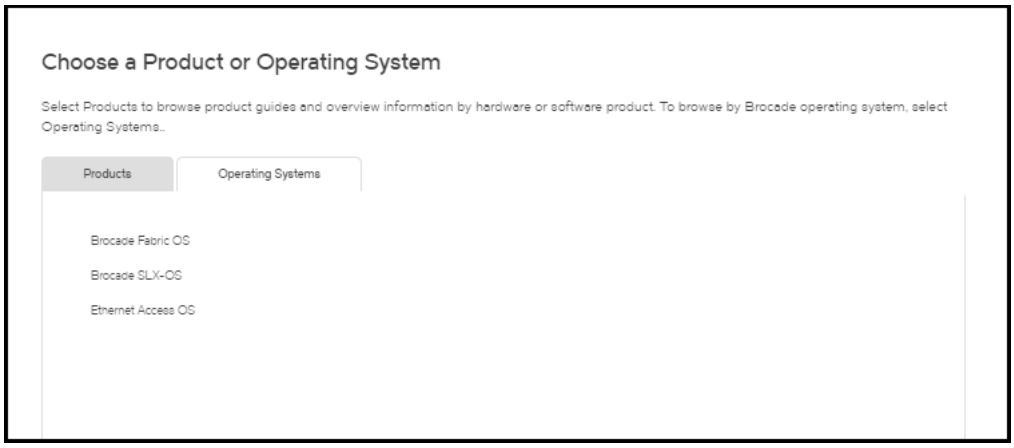
The Document Library for that product displays



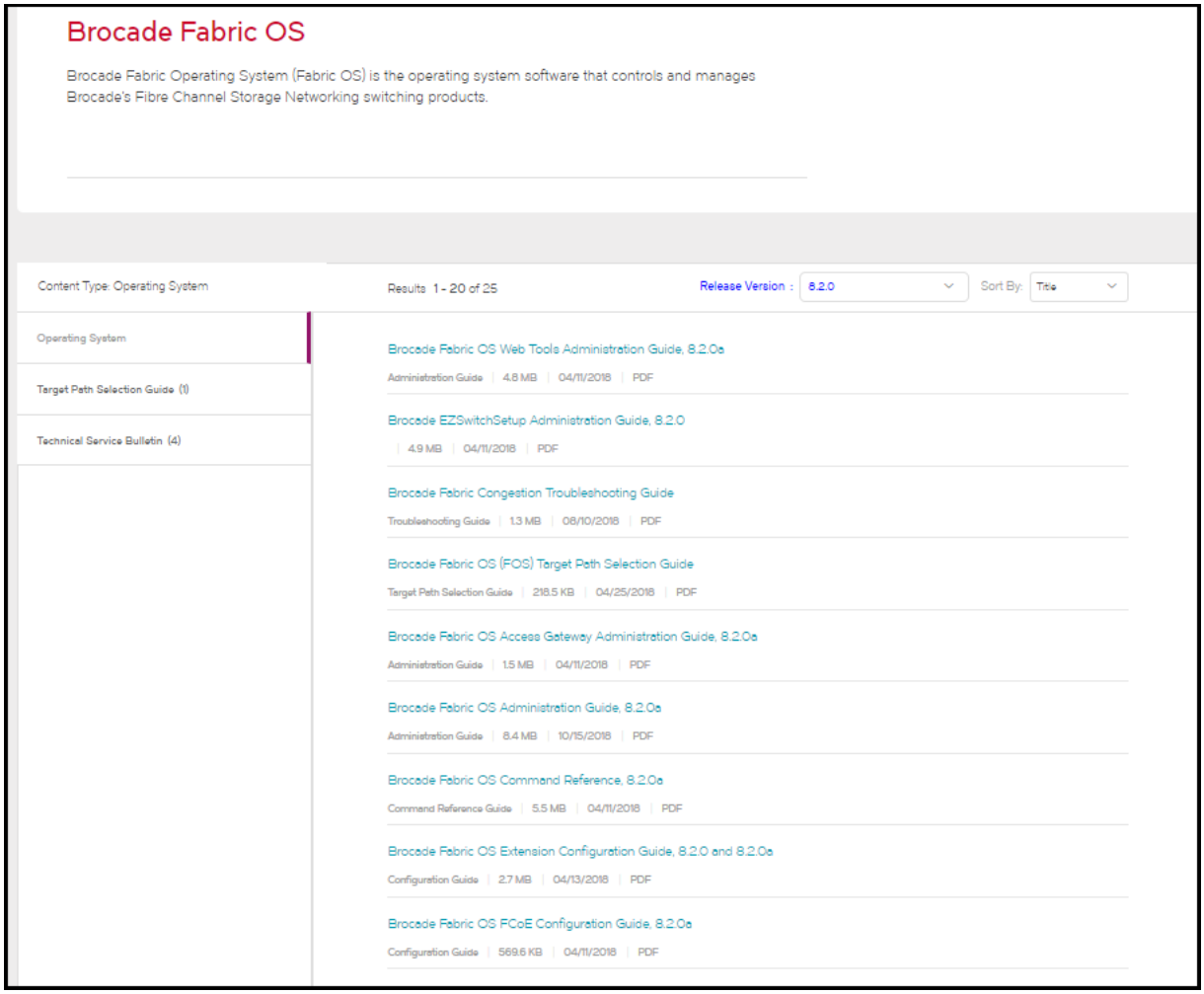
2. Click the link for the document that you want to read, and then open or save it. You may have to scroll inside the results to see the document that you want.

2.1.3 Selecting by Operating System

1. Click **Document Library**.
2. Click **Operating Systems**, and from the displayed panel, choose **Brocade Fabric OS**.



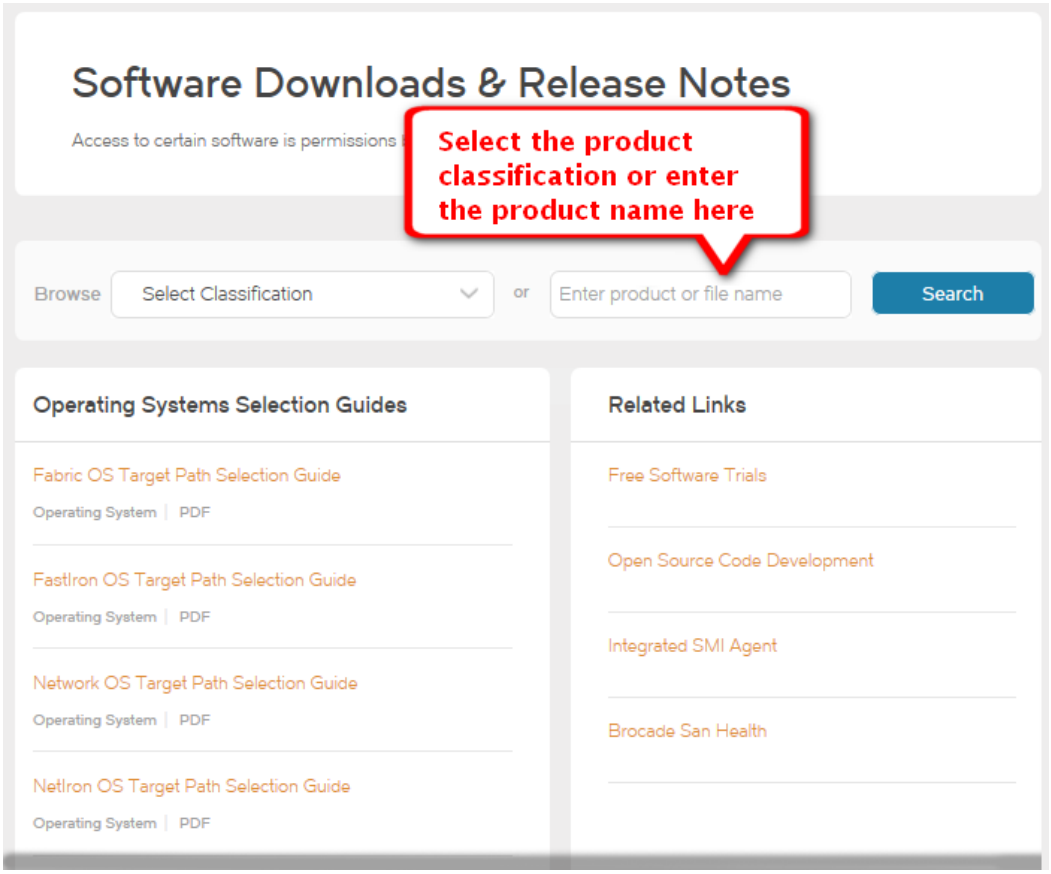
3. View the results on the Brocade Fabric OS Document Library page. Scroll down the results to see the document that you want. Click the document that you want to read, and then open or save it.



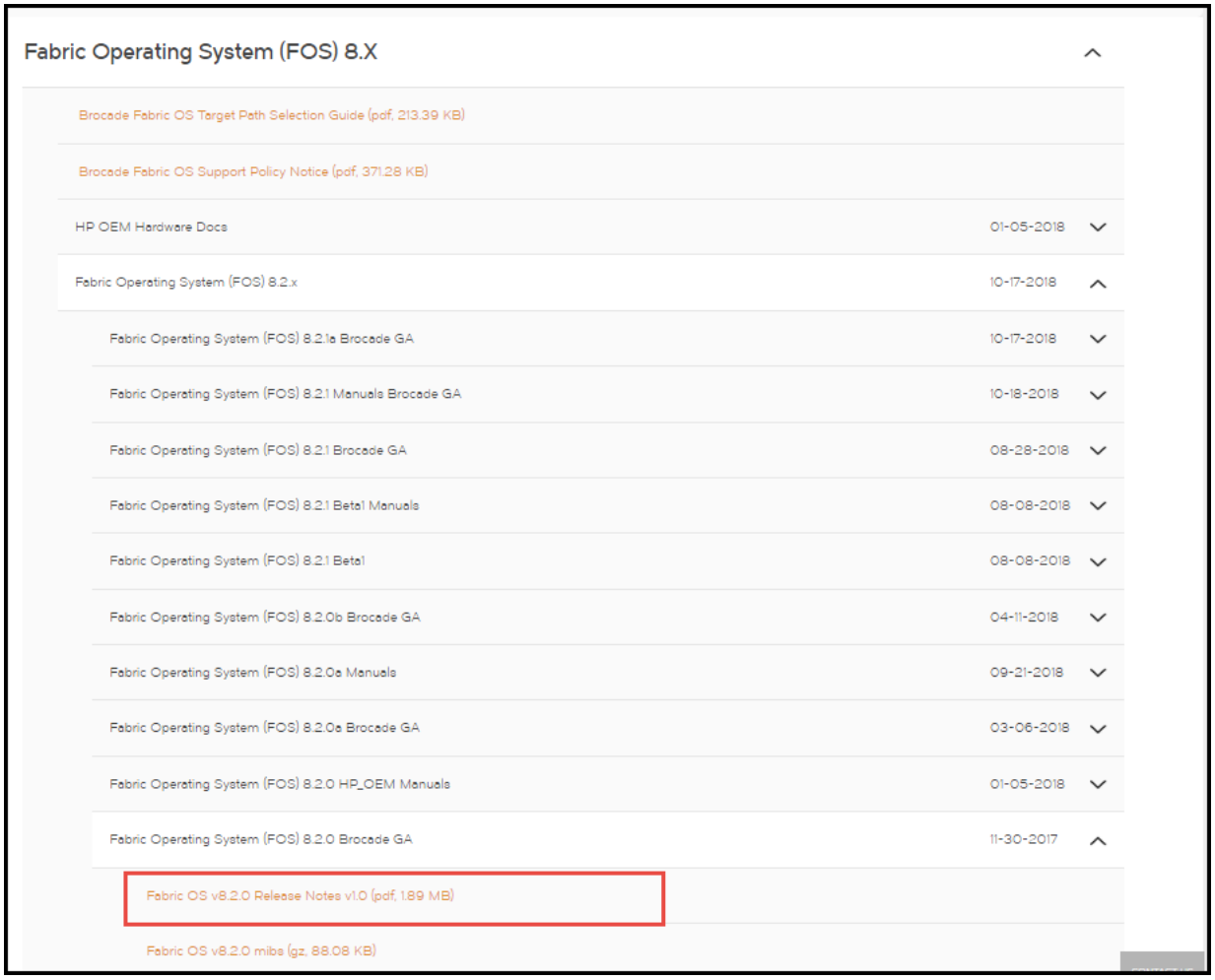
2.2 Locating Release Notes

Complete the following steps to locate the release notes for your product on MyBrocade.com.

1. Open http://my.brocade.com and log in. If you do not have a login, registration is free. Click **Register Now** and follow the directions.
2. Select **Support** > **Licenses & Downloads** > **Software & Driver Downloads**.
3. Select the product type or enter the product name in the search field, and click **Search**.



4. Release notes are available under the software version. Click the down arrow to expand and show more results.



2.3 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 8.2.1a is a patch release based on Fabric OS 8.2.1. All hardware platforms and features supported in FOS 8.2.1 are also supported in FOS 8.2.1a. This release contains minor enhancements and fixes for defects listed at the end of this document.

Chapter 4: What's New in FOS 8.2.1a

4.1 Software Features

The following sections list new, modified, and deprecated software features for this release.

4.1.1 Modified Software Features

This release includes the following enhancements to existing features and supports:

- Trunking for encryption ports on the FC32-48 port blade.
- MAPS default monitoring rules for 32Gb/s Fibre Channel 25 KM ELWL SFP (customer P/N XBR-000278).
- Brocade G620 switches that use new flash memory chip. The Brocade G620 switches with the new flash memory chip are identified by the `switchShow` command listing of "`switchType`" value as 162.5.

Chapter 5: What's New in FOS 8.2.1

5.1 Hardware

The following sections list new hardware introduced with this release and hardware that is no longer supported with this release.

5.1.1 New Devices

Product Name	Device Name
Brocade 7810	Gen 6 (32Gb/s) Distance Extension Switch

5.1.2 New Blades

None.

5.1.3 New Optical Transceivers

FOS 8.2.1 supports the following new optical transceiver on the noted devices:

32Gb/s Fibre Channel 25 KM ELWL SFP (customer P/N XBR-000278) on the Brocade G620, G630, FC32-48, and SX6 blade.

5.1.4 Deprecated Hardware

None.

5.2 Software Features

The following sections list new, modified, and deprecated software features for this release.

5.2.1 New Software Features

The following software features are new in this release:

- Counterfeit License Protection
- REST API with New RESTCONF Modules
- Management Interface Rate Limiting

5.2.1.2 Counterfeit License Protection

FOS 8.2.1 introduces counterfeit license protection (CLP) on the Brocade 6505, 6510, G610, G620, and 7810 to prevent misuse of the `licenseAdd` command. CLP performs the following actions based on the number of times that the `licenseAdd` command is invoked:

- RASLOG WARNING message when 25 invalid `licenseAdd` operations are detected within a 24-hour period.
- RASLOG CRITICAL message when 40 invalid `licenseAdd` operations are detected within a 24-hour period.
- Shuts down a switch when 50 invalid `licenseAdd` operations are detected within a 24-hour period.

A switch that is shut down due to CLP detection will no longer be able to boot to a functional state. Customers may request a replacement unit from their support provider.

5.2.1.3 REST API with New RESTCONF Modules

FOS 8.2.1 expands REST API support from that supported in FOS 8.2.0a with the following new features and corresponding RESTCONF modules:

- Physical chassis, FRU, and optical transceiver: brocade-chassis, brocade-fru, brocade-media
- Switch configuration: brocade-fibrechannel-configuration
- SupportSave: brocade-operation-supportsave, brocade-operation-showstatus
- Trunking: brocade-fibrechannel-trunk
- RASLOG and syslog configuration: brocade-logging
- System security: brocade-security
- System time zone and time server: brocade-time
- Monitoring and Alerting Policy Suite (MAPS): brocade-maps

FOS 8.2.1 enhances the following existing RESTCONF modules:

- brocade-fibrechannel
- brocade-fibrechannel-switch
- brocade-access-gateway

For a detailed description of the new modules and attributes, refer to the *Brocade Fabric OS REST API Reference Manual* for FOS 8.2.1.

5.2.1.4 Management Interface Rate Limiting

FOS 8.2.1 implements hardware-based ingress rate limiting on the management interface of X6 directors to prevent denial of service (DOS) attacks through the Ethernet management interface. When this feature is enabled, hardware performs ingress rate limiting when a DOS attack on the Eth0 or Eth3 management interface is detected. Normal management application traffic from Web Tools, SNMP, and Brocade Network Advisor is not affected when there is no DOS attack. These applications may appear sluggish when a DOS attack is detected.

5.2.2 Modified Software Features

The following software features have been enhanced in this release:

- MAPS (Monitoring and Alerting Policy Suite)
- Access Gateway
- Fabric Services
- System Security
- configure Command

- Extension
- Power supply microcontroller firmware utility
- Miscellaneous

5.2.2.1 MAPS Enhancements

5.2.2.1.1 UCS/FI Login Imbalance Monitoring

FOS 8.2.1 adds MAPS monitoring of Cisco UCS Fabric Interconnect (FI) connections to Brocade switches in NPV mode. MAPS monitors the distribution of UCS servers over the uplinks between FI and Brocade switches to remain balanced over time. When MAPS detects an imbalance, it alerts the SAN administrator of the condition or triggers an automatic rebalance action.

5.2.2.1.2 Miscellaneous

5.2.2.1.2.1 Default Rule Change

FOS 8.2.1 replaces the default rule names in FOS 8.2.0x in the following table with the new default rule names:

FOS 8.2.0x Rule Names	FOS 8.2.1 Rule Names
defALL_DPIP_EXTN_FLOW_C	defALL_DPIP_EXTN_FLOW_P_90
defALL_DPIP_EXTN_FLOW_M	defALL_DPIP_EXTN_FLOW_P_80
defALL_DPIP_EXTN_FLOW_A	defALL_DPIP_EXTN_FLOW_P_65
defALL_DPIP_EXTN_FLOW_MAX	defALL_DPIP_EXTN_FLOW_P_TOTAL

NOTE The default rules will be automatically converted to the new rule names during firmware upgrade from FOS 8.2.0x to FOS 8.2.1 or later. User-defined rules of the IP_EXTN_FLOW monitoring system must be changed manually to follow the new rule name format.

5.2.2.1.2.2 Alert Severity Change

FOS 8.2.1 changes the alert severity from ERROR to CRITICAL for the following default rule:

defALL_E_PORTSC3TXTO_20 ALL_E_PORTS(C3TXTO/MIN>20) RASLOG

FOS 8.2.1 changes the alert severity from WARNING to ERROR for the following default rule:

defALL_FANFAN_STATE_FAULTY ALL_FANS(FAN_STATE/NONE==FAULTY) RASLOG

5.2.2.2 Access Gateway Enhancements

5.2.2.2.1 Slow-Drain Device Quarantine on AG

FOS 7.4 and later support Slow-Drain Device Quarantine (SDDQ) to mitigate congestion due to slow-drain devices connected to switches in native mode. FOS 8.2.1 enhances SDDQ support on AG to be able to quarantine slow-drain devices connected to Access Gateway.

5.2.2.2.2 Port NPIV Configuration

FOS 8.2.1 adds support of the `portCfgNpivPort` command for a switch in AG mode. With this support, administrators can enable or disable NPIV mode for a port when a switch is in Access Gateway mode.

5.2.2.3 Fabric Services Enhancements

5.2.2.3.1 GZS and GAZS Commands

FOS 8.2.1 adds support of the Get Zone Set (GZS) and Get Active Zone Set (GAZS) commands under FC-GS-8 for zone servers. GZS queries for Zone Set Database, whereas GAZS queries for Active Zone Set (or Effective Configuration Set).

5.2.2.3.2 Impaired Port Enhancements

FOS 8.2.1 enhances the impaired port feature introduced in FOS 8.2.0. With FOS 8.2.0, an impaired port can be used as a principal link, which is used in fabric-related events, even though there are parallel nonimpaired links available. With FOS 8.2.1, when a principal link is impaired and parallel links exist, an alternate link will be selected as the principal link.

5.2.2.4 System Security Enhancements

5.2.2.4.1 Minimum Password Difference

FOS 8.2.1 adds the new `-minDiff to passwdcfg` CLI command to enable SAN administrators to configure the password policy to require the minimum number of characters that must be different between a current password and a new password.

5.2.2.4.2 Session Logout Message

FOS 8.2.1 displays a logout message for SSH or Telnet session logout, exit, or timeout on the standard session terminal window.

5.2.2.4.3 rootAccess Command Change

FOS 8.2.1 adds the `-force` option to the `rootAccess` command to bypass the interactive prompt of the command execution.

5.2.2.4.4 HTTPS KeepAlive

FOS 8.2.1 adds support of HTTP server connection KeepAlive. The server KeepAlive is supported only with secure HTTPS connections to switches. The KeepAlive support may be enabled with the command `mgmtapp --enable keepalive` in FOS 8.2.1 or later.

5.2.2.5 configure Command Enhancements

FOS 8.2.1 introduces options to the `configure` CLI command to allow a number of switch configuration parameters to be set without going through the interactive CLI menu. For details, refer to the *Brocade Fabric OS Command Reference Manual* for FOS 8.2.1.

5.2.2.6 Extension Enhancements

FOS 8.2.1 supports dynamic LAG (LACP) on Gigabit Ethernet LAN ports on extension platforms.

5.2.2.7 Power Supply Microcontroller Firmware Utility

Some power supply models for Brocade Gen 6 platforms support field upgrade of the firmware image used by their microcontrollers. FOS 8.2.1 introduces the `psutil` CLI command for field upgrade of the power supply microcontroller

firmware. The power supply firmware is packaged as part of FOS 8.2.1 and later. Administrators can use the `psutil` command to check the power supply firmware version and when necessary upgrade to the version.

5.2.2.8 Miscellaneous Enhancements

FOS 8.2.1 includes the following miscellaneous enhancements:

5.2.2.8.1 chassisName Command

FOS 8.2.1 enhances the `chassisName` command to increase the name length from 15 characters to 31 characters on the DCX 8510 and X6 directors.

5.2.2.8.2 ISL R_RDY in Base Switch

FOS 8.2.1 supports the `portcfgislmode` command to configure ISL R_RDY mode on the ISLs in a base switch, that is, the XISLs. With this enhancement, devices that support R_RDY mode can also be used on XISLs.

5.2.2.8.3 sfpShow -link Enhancement

FOS 8.2.1 displays the alert thresholds for peer port optics through the `sfpShow -link` option. The alert thresholds are displayed for voltage, temperature, Tx Bias, Tx Power, and Rx Power metrics. The alert thresholds are displayed for peer port optics only.

5.3 CLI Command Changes

The following sections list new, modified, and deprecated commands for this release.

5.3.1 New Commands

The following commands are new in this release:

- bladePortMap
- deviceLogin
- factoryFanShow
- psUtil

5.3.2 Modified Commands

Refer to the Modified Commands section of the *Brocade Fabric OS Command Reference Manual* for Fabric OS 8.2.1.

5.3.3 Deprecated Commands

The *Brocade Fabric OS Command Reference Manual* documents all FOS commands that are officially supported. Any commands not listed in the command reference for a specific release are not supported and may be subject to removal without notification. Refer to the Deprecated Commands section in the *Brocade Fabric OS Command Reference Manual* for Fabric OS 8.2.1.

5.4 Security Vulnerability Fixes

This section lists the Common Vulnerabilities and Exposures (CVEs) that have been addressed in FOS v8.2.1.

- **CVE ID: CVE-2018-6433 -** A vulnerability in the secryptocfg export command of Brocade Fabric OS versions before 8.2.1, 8.1.2f, 8.0.2f, 7.4.2d could allow a local attacker to bypass the exports file access restrictions and initiate a file copy from the source to a remote system.
- **CVE ID: CVE-2018-6434 -** The Web management interface of Brocade Fabric OS versions before 8.2.1, 8.1.2f, 8.0.2f, 7.4.2d doesn't send cookies with secure flag. This could allow attackers to intercept or manipulate a victim user's session ID
- **CVE ID: CVE-2018-6435 -** A Vulnerability in the seccryptocfg command available from the Brocade Fabric OS command line interface (CLI) versions before 8.2.1, 8.1.2f, 8.0.2f, 7.4.2d could allow a local attacker to escape the restricted shell and, gain root access to the device.
- **CVE ID: CVE-2018-6436 -** A Vulnerability in the firmwaredownload command available from the Brocade FabricOS command line interface (CLI) versions before 8.2.1, 8.1.2f, 8.0.2f, 7.4.2d could allow a local attacker to escape the restricted shell and, gain root access to the device.
- **CVE ID: CVE-2018-6437 -** A Vulnerability in the help command available from the Brocade Fabric OS command line interface (CLI) versions before 8.2.1, 8.1.2f, 8.0.2f, 7.4.2d could allow a local attacker to escape the restricted shell and, gain root access to the device.
- **CVE ID: CVE-2018-6438 -** A Vulnerability in the supportsave command available from the Brocade Fabric OS command line interface (CLI) versions before 8.2.1, 8.1.2f, 8.0.2f, 7.4.2d could allow a local attacker to escape the restricted shell and, gain root access to the device.
- **CVE ID: CVE-2018-6439 -** A Vulnerability in the configdownload command available from the Brocade Fabric OS command line interface (CLI) versions before 8.2.1, 8.1.2f, 8.0.2f, 7.4.2d could allow a local attacker to escape the restricted shell and, in some cases, gain root access to the device.
- **CVE ID: CVE-2018-6440 -** A vulnerability in the proxy service of Brocade Fabric OS versions before 8.2.1, 8.1.2f, 8.0.2f, 7.4.2d could allow remote unauthenticated attackers to obtain sensitive information and possibly cause a denial of service.
- **CVE ID: CVE-2018-6441 -** A vulnerability in the Secure Shell implementation in Brocade Fabric OS versions before 8.2.1, 8.1.2f, 8.0.2f, 7.4.2d could allow a local attacker to provide arbitrary environment variables, which can be used to bypass the restricted configuration shell.
- **CVE ID: CVE-2018-6442 -** A vulnerability in the webtools firmware update section of Brocade Fabric OS versions before 8.2.1, 8.1.2f, 8.0.2f, 7.4.2d could allow remote authenticated attackers to execute arbitrary commands as the root user, leading to complete persistent take-over of the target device.

5.5 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 6: Software License Support

6.1 Optionally Licensed Software

Fabric OS 8.2 includes all basic switch and fabric support software, as well as optionally licensed software that is enabled using license keys.

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 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 DCX 8510-8, DCX 8510-4, Brocade 6510, Brocade 6520, Brocade 7840, or Brocade G620 to be configured as an EX_Port supporting Fibre Channel Routing (FCR). This eliminates the need to add an FR4-18i blade or use a Brocade 7500 for FCR purposes, and it also provides either quadruple or octuple the bandwidth for each FCR connection (when connected to another 16Gb/s- or 32Gb/s-capable port).

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. This eliminates the need to add an FR4-18i blade or use a Brocade 7500 for FCR purposes, and it also provides octuple the bandwidth for each FCR connection (when connected to another 32Gb/s-capable port).

Advanced Extension – This license enables two advanced extension features: FCIP Trunking and Adaptive Rate Limiting. The FCIP Trunking feature allows multiple IP source and destination address pairs (defined as FCIP circuits) via multiple 1GbE or 10GbE interfaces to provide a high-bandwidth FCIP tunnel and failover resiliency. In addition, each FCIP circuit supports four QoS classes (Class-F, High, Medium, and Low Priority), each as a TCP connection. The Adaptive Rate Limiting feature provides a minimum bandwidth guarantee for each tunnel with full utilization of the available network bandwidth without impacting throughput performance under a high-traffic load. This license is available on the DCX 8510-8/DCX 8510-4 for the FX8-24 on an individual slot basis. The upgrade license on Brocade 7810 includes this license to enable 10GbE ports.

10GbE FCIP/10G Fibre Channel – This license enables the two 10GbE ports on the FX8-24 and/or the 10G FC capability on FC16-xx blade ports supported on DCX 8510 platforms except for the FC16-64 blade. On the Brocade 6510 and Brocade 6520, this license enables 10G FC ports. The upgrade license on Brocade 7810 includes this license to enable six 10GbE ports. This license is not applicable to the Brocade 7840, Brocade G620, or Brocade X6 platforms.

On the FX8-24:

With this license installed and assigned to a slot with an FX8-24 blade, two additional operating modes (in addition to 10x1GbE ports mode) can be selected:

10x1GbE ports and 1x10GbE ports
or
2x10GbE ports

On the FC16-xx:

Enables 10G FC capability on an FC16-xx blade in a slot that has this license.

On the Brocade 6510 and Brocade 6520:

Enables 10G FC capability on Brocade 6510 and Brocade 6520 switches.

This license is available on the DCX 8510-8 and DCX 8510-4 on an individual slot basis.

Advanced FICON Acceleration – This licensed feature uses specialized data management techniques and automated intelligence to accelerate FICON tape read and write and IBM Global Mirror data replication operations over distance, while maintaining the integrity of command and acknowledgement sequences. This license is available on the Brocade 7840 and the Brocade DCX 8510-8 and DCX 8510-4 for the FX8-24 on an individual slot basis.

ICL POD License – This license activates ICL ports on DCX 8510 or X6 platform core blades. An ICL license must be installed on the director platforms at both ends of the ICL connection.

On the Brocade DCX 8510-8 and X6-8:

The first ICL POD license enables 16 (half of the total) UltraScale ICL QSFP ports on the DCX 8510-8 or X6-8 Directors, enabling 8 ICL ports on each core blade. These are QSFP port numbers 0, 1, 2, 3, 4, 5, 6, and 7 on the DCX 8510-8; while on the X6-8, the QSFP port numbers are 0, 1, 2, 3, 8, 9, 10, and 11. The second ICL POD license enables the remaining 16 UltraScale ICL QSFP ports on the directors. These are QSFP port numbers 8, 9, 10, 11, 12, 13, 14, and 15 on each core blade of the DCX 8510-8; while on the X6-8, these are QSFP port numbers 4, 5, 6, 7, 12, 13, 14, and 15 on each core blade.

Note that the trunk boundaries are different between CR32-8 core blades on the X6-8 and CR16-8 core blades on the DCX 8510-8.

On the Brocade DCX 8510-4 and X6-4:

ICL POD licenses are different between X6-4 and DCX 8510-4 Directors. On the X6-4, the first ICL POD license enables 8 (half of the total) UltraScale ICL QSFP ports on the director, enabling 4 ICL ports on each core blade, which are QSFP port numbers 0, 1, 4, and 5. The second ICL POD license on the X6-4 enables the remaining 8 UltraScale ICL QSFP ports on the director, which are QSFP port numbers 2, 3, 6, and 7 on each core blade. On the DCX 8510-4, a single ICL POD license enables all 16 UltraScale ICL QSFP ports on the director.

Enterprise ICL (EICL) License – The EICL license is required on a Brocade DCX 8510 chassis when that chassis is connected to four or more Brocade DCX 8510 chassis via ICLs. This license is not applicable to X6 Directors.

This license requirement does not depend upon the total number of DCX 8510 chassis that exist in a fabric, but only on the number of other chassis connected to a DCX 8510 via ICLs. This license is recognized/displayed when operating with FOS 7.0.1 and is enforced by FOS 7.1.0 and later.

NOTE The EICL license supports a maximum of nine (9) DCX 8510 chassis connected in a full-mesh topology or up to twelve (12) DCX 8510 chassis connected in a core-edge topology. Refer to the *Brocade SAN Scalability Guidelines* document for additional information.

WAN Rate Upgrade 1 License – The WAN Rate Upgrade 1 license provides additional WAN throughput up to 10Gb/s on a Brocade 7840. The base configuration for a Brocade 7840 without this license provides WAN throughput up to 5Gb/s.

WAN Rate Upgrade 2 License – The WAN Rate Upgrade 2 license provides unlimited WAN throughput (up to the hardware limit) on a Brocade 7840. WAN Rate Upgrade 2 licenses also enable the use of two 40GbE ports on a Brocade 7840. The 40GbE ports cannot be configured without the WAN Rate Upgrade 2 license. A WAN Rate Upgrade 1 license must be installed on a Brocade 7840 before a WAN Rate Upgrade 2 license is installed. A WAN Rate Upgrade 1 license cannot be removed before the WAN Rate Upgrade 2 license has been removed.

NOTE The WAN Rate Upgrade 1 and WAN Rate Upgrade 2 licenses apply only to Brocade 7840 platforms. They control the aggregate bandwidth for all tunnels on that Brocade 7840. The entire capacity controlled by the licenses can be assigned to a single tunnel, or a portion of the capacity can be assigned to multiple tunnels. The total bandwidth aggregated for all tunnels should not exceed the limits established by the licenses.

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, 6 10Gb/s Ethernet 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.

6.2 Temporary License Support

The following licenses are available in Fabric OS 8.2.1 as either universal temporary or regular temporary licenses:

- Fabric (E_Port)
- Extended Fabric
- Trunking
- High Performance Extension
- Advanced Performance Monitoring
- Fabric Watch
- Integrated Routing
- Integrated Routing Ports on Demand
- Advanced Extension
- Advanced FICON Acceleration
- 10GbE FCIP/10GFibre Channel
- FICON Management Server (CUP)
- Enterprise ICL
- Fabric Vision
- WAN Rate Upgrade 1
- WAN Rate Upgrade 2

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.

Chapter 7: Hardware Support

7.1 Supported Devices

The following devices are supported in this release:

- G610, G620, G630, X6-4, X6-8
- 6505, 6510, 6520, DCX 8510-4, DCX 8510-8
- M6505,6542, 6543, 6545, 6546, 6547, 6548, 6558
- 7810, 7840

7.2 Supported Blades

7.2.1 DCX 8510-8/DCX 8510-4 Blade Support

Fabric OS 8.2.1 software is fully qualified and supports the blades for the DCX 8510-8 and DCX 8510-4 as noted in the following table:

Blades	OS Support
FC16-32, FC16-48 16G FC blades	FOS 7.0 or later.
FC16-64 blade[1, 2]	FOS 7.3 or later.
FC8-64 64-port 8-Gb port blade	Not supported.
FC8-32E, FC8-48E	Not supported.
FCIP/FC Router blade (FR4-18i)	Not supported.
Virtualization/Application blade (FA4-18)	Not supported.
Encryption blade (FS8-18)	Not supported.
Extension blade (FX8-24)	FOS 7.0 or later. Up to a maximum of four blades of this type.
FCoE/L2 CEE blade FCOE10-24	Not supported.

[1] 8510 core blade QSFPs, part numbers 57-1000267-01 and 57-0000090-01, are not supported in the FC16-64. The QSFPs supported in the FC16-64, part number 57-1000294-02, is supported on 8510 core blades.
[2] E_Port connections on the FC16-64 blade have the following restriction: connecting a QSFP port between an FC16-64 blade and an ICL QSFP port on a core blade is not supported.

7.2.2 X6-8/X6-4 Blade Support

Fabric OS 8.2.1 software is fully qualified and supports the blades for the X6-8 and X6-4 as noted in the following table. None of the legacy blades (16G or lower speed) are supported in the Gen 6 chassis.

Blades	OS Support
FC32-48 32G FC blade	FOS 8.0.1 or later.
SX6 Gen 6 Extension blade	FOS 8.0.1 or later. Up to a maximum of four blades of this type.
FC32-64 32G FC/FCoE blade	FOS 8.2.0 or later. A maximum of two blades of this type is supported when four SX6 blades are present in the same X6-8 chassis.

NOTE The QSFP supported in the FC16-64, part number 57-1000294-02, is also supported on X6 core blades under the condition that the port speed must be configured at a fixed 16Gb/s. Otherwise, the optics will fault.

7.3 Supported Power Supplies

7.3.1 Brocade G620 Power Supplies

The following table lists the power supplies for the Brocade G620 that are supported in this release:

Part Number	Description	Compatible Devices
XBRG250WPSAC-F	Power supply and fan assembly, nonport-side air exhaust	Brocade G620
XBRG250WPSAC-R	Power supply and fan assembly, nonport-side air intake	Brocade G620

7.3.2 Brocade G630 Power Supplies

The following table lists the power supplies for the Brocade G630 that are supported in this release:

Part Number	Description	Compatible Devices
XBR-1500WPSAC-F	Power supply and fan assembly, nonport-side air exhaust	Brocade G630
XBR-1500WPSAC-R	Power supply and fan assembly, nonport-side air intake	Brocade G630

7.3.3 DCX 8510-8 Power Supply Requirements

7.3.3.1 Typical Power Supply Requirements for Blades in DCX 8510-8 Backbones

(For a specific calculation of power draw with different blade combinations, see Appendix A, Power Specifications, in the *Brocade DCX 8510-8 Backbone Hardware Reference Manual.*)

Configured Number of Ports	Blades	Type of Blade	DCX 8510-8 @110 VAC (Redundant Configurations)	DCX 8510-8 @200–240 VAC (Redundant Configurations)	Comments
Any combination of 8-Gb or 16-Gb ports with QSFP ICLs	FC16-32, FC16-64	Port Blade	4 Power Supplies	2 Power Supplies	200–240 VAC: 1+1 Power Supplies 110 VAC: 2+2[3] Power Supplies
256 16-Gb ports + QSFP ICLs	FC16-32, FC16-48 (Maximum of fully populated FC16-32 blades), FC16-64	Port Blade	4 Power Supplies	2 Power Supplies	200–240 VAC: 1+1 Power Supplies 110 VAC: 2+2[3] Power Supplies Max 8 FC16-32 port blades
192 16-Gb ports & max 2 intelligent blades (FX8-24) with QSFP ICLs	FC16-32, FC16-48, FC16-64, FX8-24	Port / Intelligent Blade	4 Power Supplies	2 Power Supplies	200–240 VAC: 1+1 Power Supplies 110 VAC: 2+2[3] Power Supplies Max four FC16-48 port blades and max 2 intelligent blades
336 16-Gb ports + QSFP ICLs	FC16-48 (Maximum of seven FC16-48 blades, with one empty port blade slot)	Port Blade	4 Power Supplies	2 Power Supplies	200–240 VAC: 1+1 Power Supplies 110 VAC: 2+2[3] Power Supplies Max 7 FC16-48 port blades
384 16-Gb ports + QSFP ICLs	FC16-48	Port Blade	Not Supported	4 Power Supplies	200–240 VAC: For DCX 8510-8, four (2+2)[3] 220 VAC Power Supplies are required.
384 16-Gb ports + QSFP ICLs	FC16-64	Port Blade	4 Power Supplies	2 Power Supplies	200–240 VAC: 1+1 Power Supplies 110 VAC: 2+2[1] Power Supplies
Any combination of 8-Gb or 16-Gb ports and intelligent blades with QSFP ICLs	FC16-32, FC16-48, FX8-24	Intelligent Blade / Combination	Dependent on the configuration. Requires a power calculation for the specific configuration.	2 or 4 Power Supplies, depending on the configuration	For DCX 8510-8, four (2+2)[3] 220 VAC Power Supplies are required when any special-purpose blades are installed.

[3] When a 2+2 power supply combination is used, the users are advised to configure the MAPS setting for switch Marginal State to be one Bad Power Supply.

Configured Number of Ports	Blades	Type of Blade	DCX 8510-8 @110 VAC (Redundant Configurations)	DCX 8510-8 @200–240 VAC (Redundant Configurations)	Comments
512 16-Gb ports	FC16-64	Port Blade	4 Power Supplies	2 Power Supplies	200–240 VAC: 1+1 Power Supplies 110 VAC: 2+2[3] Power Supplies
512 16-Gb ports + QSFP ICLs	FC16-64	Port Blade	4 Power Supplies	2 Power Supplies	200–240 VAC: 1+1 Power Supplies 110 VAC: 2+2[3] Power Supplies

7.3.4 DCX 8510-4 Power Supply Requirements

7.3.4.1 Typical Power Supply Requirements for Blades in DCX 8510-4 Backbones

(For a specific calculation of power draw with different blade combinations, refer to Appendix A, Power Specifications, in the *Brocade DCX 8510-4 Backbone Hardware Reference Manual*.)

Configured Number of Ports	Blades	Type of Blade	DCX 8510-4 @110 VAC (Redundant Configurations)	DCX 8510-4 @200–240 VAC (Redundant Configurations)	Comments
96 ports max with QSFP ICLs	FC16-32	Port Blade	2 Power Supplies	2 Power Supplies	1+1 redundancy with 110 or 200–240 VAC power supplies
Any combination of 8-Gb or 16-Gb ports and intelligent blades with QSFP ICLs	FC16-32, FC16-48, FC16-64, FX8-24	Intelligent Blade / Combination	Not Supported	2 Power Supplies	200–240 VAC: 1+1 Power Supplies

7.3.5 Brocade X6 Power Supplies

The following table lists the supported power supplies for Brocade X6 and recommended microcontroller firmware versions in this release:

Part Number	Description	Compatible Devices	Recommended Microcontroller Firmware Version
XBR-X6-RACNPIPSU-0104	AC power supply and fan assembly, nonport-side air intake	Brocade X6	Primary FW version: 3.4 Sec LLC FW version: 3.2 Sec COM FW version: 3.1
XBR-X6-RACNPEPSU-0104	AC power supply and fan assembly, nonport-side air exhaust	Brocade X6	Primary FW version: 3.4 Sec LLC FW version: 3.2 Sec COM FW version: 3.1
XBR-X6-HVNPIPSU-0104	High voltage AC/DC power supply and fan assembly, nonport-side air intake	Brocade X6	N/A

XBR-X6-HVNPEPSU-0104	High voltage AC/DC power supply and fan assembly, nonport-side air exhaust	Brocade X6	N/A

7.3.6 X6-8 Power Supply Requirements

7.3.6.1 Typical Power Supply Requirements for Blades in X6-8 Directors

(For a specific calculation of power draw with different blade combinations, refer to the Power Consumption section in the *Brocade X6-8 Director Hardware Installation Guide.*)

Configured Number of Ports	**Blades**	**Type of Blade**	**X6-8 @100–120 VAC (Redundant Configurations)[4]**	**X6-8 @200–240 VAC (Redundant Configurations)[4,5]**
144 32Gb/s ports + QSFP ICLs	FC32-48	Port Blade	3 or 4 Power Supplies (2+1 or 2+2 redundancy)	2 Power Supplies (1+1 redundancy)
384 32Gb/s ports + QSFP ICLs	FC32-48	Port Blade	Not Supported	3 or 4 Power Supplies (2+1 or 2+2 redundancy)
Any combination of 32Gb/s ports and Extension blades with QSFP ICLs	FC32-48, FC32-64, SX6	Port Blade Extension Blade	Not Supported	3 or 4 Power Supplies (2+1 or 2+2 redundancy)

7.3.7 X6-4 Power Supply Requirements

7.3.7.1 Typical Power Supply Requirements for Blades in X6-4 Directors

(For a specific calculation of power draw with different blade combinations, refer to the Power Consumption section in the *Brocade X6-4 Director Hardware Installation Guide.*)

Configured Number of Ports	**Blades**	**Type of Blade**	**X6-4 @100–120 VAC (Redundant Configurations)[5]**	**X6-4 @200–240 VAC (Redundant Configurations)[5]**
Any combination of 32Gb/s ports and Extension blades with QSFP ICLs	FC32-48, FC32-64, SX6	Port Blade Extension Blade	Not Supported	2 Power Supplies (1+1 redundancy)

[4] For N+1 or N+N redundancy, N PSUs must be available for the system to support the load. In other words, failure of up to 1 PSU in an N+1 configuration or N PSUs in an N+N configuration will not impact the system's operation.
[5] For 1+1 redundancy, 1 PSU must be available for the system to support the load. In other words, failure of up to 1 PSU will not impact system's operation.

7.3.8 Supported Optics

For a list of supported fiber-optic transceivers that are available from Brocade, refer to the latest version of the *Brocade Optics Family Data Sheet* available online at www.broadcom.com.

Chapter 8: Software Upgrades and Downgrades

8.1 Image Filenames

Download the following images from www.mybrocade.com.

Image Filename	Description
v8.2.1a.zip	Fabric OS 8.2.1a for Windows
v8.2.1a.gz	Fabric OS 8.2.1a for Linux
v8.2.1a.md5	Fabric OS 8.2.1a Checksum
v8.2.1a.tar.gz	Fabric OS 8.2.1a MIBs
v8.2.1a_releasenotes_v2.0.pdf	Fabric OS 8.2.1a Release Notes v2.0

8.2 Migration Path

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

8.2.1 Migrating from FOS 8.1

Any Brocade platform running any FOS 8.1.0a or later version can be nondisruptively upgraded to FOS 8.2.1a.

NOTE A nondisruptive firmware upgrade from FOS 8.1.0 to FOS 8.2.1a on the Brocade G610 is not supported.

8.2.2 Migrating from FOS 8.0

Any Brocade platform and supported blades in the **DCX 8510-8/DCX 8510-4 Blade Support** table and the **X6-8/X6-4 Blade Support** table running any FOS 8.0 firmware must be upgraded to FOS 8.1.x firmware before it can be nondisruptively upgraded to FOS 8.2.1a.

8.3 Upgrade/Downgrade Considerations

Any firmware activation on a DCX 8510-8 or DCX 8510-4 with an FX8-24 blade installed will disrupt I/O traffic on the FCIP links.

Disruptive upgrades to Fabric OS 8.2.1a are allowed and are supported from FOS 8.0.x (up to a two-level migration) using the optional `-s` parameter with the `firmwaredownload` command.

Firmware downgrades from FOS 8.2.1a to FOS 8.2.0x or earlier versions on the Brocade G610 or 6505 are not allowed.

On a Brocade G620 with the `switchShow` command displaying “switchType” field identified as 162.5, firmware downgrades from FOS 8.2.1a to earlier versions are not allowed.

Chapter 9: Limitations and Restrictions

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

9.1 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 8.X* document available at www.broadcom.com.

9.2 Compatibility/Interoperability

9.2.1 Brocade Network Advisor Compatibility

Brocade Network Advisor is available with flexible packaging and licensing options for a wide range of network deployments and for future network expansion. Brocade Network Advisor 14.4.1 is available in the following editions:

- SAN-only
- IP-only
- SAN+IP

For SAN management, Network Advisor 14.4.1 is available in three editions:

- **Network Advisor Professional** – A fabric management application that is ideally suited for small-size businesses that need a lightweight management product to manage their smaller fabrics. It manages two FOS fabrics at a time and up to 300 switch ports. It provides support for Brocade FC switches, Brocade HBAs/CNAs, and Fibre Channel over Ethernet (FCoE) switches.
- **Network Advisor Professional Plus** – A SAN management application designed for medium-size businesses or departmental SANs for managing up to 36 physical or virtual fabrics (FOS) and up to 2560 switch ports. It supports Brocade director products (for example, X6-4, DCX 8510-4/DCX-4S, 48Ks), FC switches, Fibre Channel over IP (FCIP) switches, Fibre Channel Routing (FCR) switches/Integrated Routing (IR) capabilities, Fibre Channel over Ethernet (FCoE)/DCB switches, and QLogic and Emulex HBAs/CNAs.
- **Network Advisor Enterprise** – A management application designed for enterprise-class SANs for managing up to 100 physical or virtual fabrics and up to 15,000 switch ports. Network Advisor Enterprise supports all the hardware platforms and features that Network Advisor Professional Plus supports, and it adds support for the Brocade directors (X6-8, DCX 8510-8/DCX) and Fiber Connectivity (FICON) capabilities.

More details about new enhancements for Brocade Network Advisor can be found in the Network Advisor 14.4.1 release notes, Network Advisor 14.4.0 user guide, and Network Advisor 14.4.1 installation, migration, and transition guides.

NOTE

- Brocade Network Advisor 14.4.1 or later is required to manage switches running Fabric OS 8.2.1 or later.
- The Brocade Network Advisor seed switch should always have the highest FOS version used in the fabric.

9.2.2 Web Tools Compatibility

Fabric OS 8.2.1 is qualified and supported with Oracle Java version 8 update 181. See the "Important Notes" section for more details.

9.2.3 SMI Compatibility

It is important to note that host SMI-S agents cannot be used to manage switches running Fabric OS 8.2.1. If you want to manage a switch running Fabric OS 8.2.1 using the SMI-S interface, you must use the Brocade Network Advisor integrated SMI agent.

9.2.4 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-life dates for all versions of Fabric OS software, visit the following Brocade website: https://www.broadcom.com/support/fibre-channel-networking/eol.

Supported Products	Fabric OS Interoperability
Brocade 200E, 4012, 4016, 4018, 4020, 4024, 4100, 4424, 4900, 5000, 7500, 7500e, 48K	No support for interoperability in the same fabric or Access Gateway connection — must use FCR.
Brocade 5410, 5424, 5430, 5431, 5432, 5450, 5460, 5470, 5480, NC-5480, VA-40FC	7.3.1 or later
Brocade DCX, DCX-4S, 300, 5100, 5300	7.3.1 or later
Brocade DCX with FS8-18 blade(s), Brocade Encryption Switch	7.3.1 or later
Brocade 7800, DCX and DCX-4S with FCOE10-24 or FX8-24 blades	7.3.1 or later
Brocade 8000	7.1.2 or later[6]
Brocade DCX/DCX-4S with FA4-18 blade(s)	No support for interoperability in the same fabric — must use FCR[7].

[6] The Brocade 8000 is not supported with Fabric OS 7.2.x or later.
[7] The FA4-18 is not supported in a DCX/DCX-4S that is running Fabric OS 7.0 or later.

Supported Products	Fabric OS Interoperability
Brocade DCX 8510-8/DCX 8510-4	FOS 7.3.1 or later
Brocade DCX 8510-8/DCX 8510-4 with FC16-64 blade	FOS 7.3.1 or later
Brocade DCX 8510-8 with FCOE10-24 blade	FOS 7.3.1 or later
Brocade 6505, 6510, 6530, 7840	FOS 7.3.1 or later
Brocade 6542	FOS 8.0.2 or later[8]
Brocade 6543	FOS 7.4.1 or later
Brocade 6547, 6548, M6505, 6545, 6546	FOS 7.3.1 or later
Brocade 6558	FOS 8.0.1 or later[8]
Brocade G610	FOS 8.1.0 or later
Brocade G620	FOS 8.0.0 or later
Brocade G630	FOS 8.2.0 or later
Brocade 7810	FOS 8.2.1 or later
Brocade X6-8/X6-4	FOS 8.0.1 or later
Brocade X6-8/X6-4 with FC32-48 blade or SX6 blade	FOS 8.0.1 or later
Brocade X6-8/X6-4 with FC32-64 blade	FOS 8.2.0 or later
Brocade 48000 with FA4-18 blade(s), Brocade 7600	Not Supported
Mi10k, M6140 (McDATA Fabric Mode and Open Fabric Mode)	Not Supported

Multi-Protocol Router Interoperability	
Brocade 7500, 7500e	Not Supported
McDATA SAN Routers 1620 and 2640	Not Supported

9.2.5 SNMP Support

Fabric OS 8.2.1 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 8.2.1.

[8] Support merged from embedded FOS releases.

9.2.5.1 Obtaining MIBs

You can download the MIB files required for this release from the downloads area of the MyBrocade site. To download the Brocade-specific MIBs from the Brocade Technical Support website, you must have a user name and password. Perform the following steps to obtain the MIBs that you want.

1. In your web browser, go to http://my.brocade.com.
2. Log in with your user name and password.
3. Under the **Support** menu, click **Software & Driver Downloads**.
4. On the **Software Downloads & Release Notes** page, select **All Operating Systems** from the **Browse** menu.
5. Select **Fabric Operating System (FOS)**, and then navigate to the release.
6. Navigate to the link for the MIBs package and either open the file or save it to disk.

NOTE Distribution of standard MIBs has been stopped. Download the required standard MIBs from the http://www.oidview.com/ or http://www.mibdepot.com/ website.

9.2.6 REST API Support

Fabric OS 8.2.1 documents the support REST API functions in the *Brocade Fabric OS REST API Reference Manual*.

9.2.6.1 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 Brocade Technical Support website, you must have a user name and password. Perform the following steps to obtain the YANG files that you want.

1. On your web browser and go to http://my.brocade.com.
2. Log in with your user name and password.
3. Under the **Support** menu, click **Software & Driver Downloads**.
4. On the **Software Downloads & Release Notes** page, select **All Operating Systems** from the **Browse** menu.
5. Select **Fabric Operating System (FOS)**, and then navigate to the release.
6. Navigate to the link for the Fabric OS package file, either for Windows or for Linux, and save it to disk.
7. 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.

9.3 Important Notes

9.3.1 FCoE

The following topologies for FCoE on the FC32-64 are not supported with FOS 8.2.1:

- 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.

9.3.2 FC-NVMe

- FOS 8.1.0 or later is required to support FC-NVMe devices.
- FOS 8.2.1 does not support FC-NVMe over FCR configurations.

9.3.3 In-flight Encryption and Compression

- FOS 8.2 supports in-flight encryption and compression on the Brocade 6510, 6520, DCX 8510, G620, G630, and FC32-48 port blade. In-flight encryption or compression on the Brocade G620 and G630 is supported with FOS 8.2.0a or later.
- To enable in-flight encryption on the Brocade G620, SFP ports 44 to 47 must be disabled. If ports 44 to 47 have been configured for in-flight compression with FOS 8.1.x or earlier, a firmware upgrade to FOS 8.2.0a or later will be blocked until in-flight compression is moved to other ports in the switch.
- FOS 8.2.1a or later is required to support trunking for encryption ports on the FC32-48 port blade.
- Disable encryption ports on an FC32-48 port blade before a nondisruptive firmware upgrade to FOS 8.2.1 or later, and enable the ports after the firmware upgrade. If you do not perform this step, unexpected disruption may occur on these encryption ports.

9.3.4 VM Insight

- VM Insight is supported on the Brocade G610, G620, G630, and X6 running FOS 8.1.0 and later. Brocade Gen 5 Fibre Channel platforms support frames with the optional FC Application Header for VM Insight to pass through. The Brocade 7840 and SX6 running FOS 8.1.0 support the Application Header in the FCP emulating tunnel. The FCP emulating tunnel or FICON emulation is not supported in other extension platforms or earlier firmware. Nonemulating tunnel on extension platforms support pass through of the Application Header.
- VM Insight is not supported across FCR, but frames with the Application Header may traverse through FCR.
- FOS 8.2.0 supports VM performance metrics in flows on the ingress F_Port only. The Brocade G610 and G620 support FC metrics. Brocade X6 Directors support both FC metrics and SCSI IO metrics.
- Legacy static flow does not monitor SCSI IOPS statistics for frames with the Application Header.
- Duplicate subflow entries are displayed after a switch HA failover or multiple restarts of VM traffic without clearing the status. The workaround is to use the `flow --reset sys_mon_all_vms` command.
- FOS 8.2.0 does not support VM Insight for FC-NVMe traffic.

9.3.5 ClearLink Diagnostics (D_Port)

- Fabric OS 8.2 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 tested by Brocade with Fabric OS 8.2 for ClearLink.[9]

	Emulex 16G Adapter	Emulex 32G Adapter	QLogic 16G Adapter	QLogic 32G Adapter
Adapter Model	LPe16002B-M6	LPe32002-M2	QLE2672	QLE2742
Adapter Firmware	11.4.204.20	11.4.142.23	v8.05.44	v8.05.44
Adapter Driver	11.4.142.23	11.4.204.8	STOR Miniport 9.1.17.21	STOR Miniport 9.1.17.21

- The D_Port long-duration test can be run only on one port at a time.
- Long-duration electrical loopback tests are not supported.
- D_Port tests on 4x32GFC breakout QSFP optics (P/N 57-1000351-01) and 128GFC non-breakout QSFP optics (P/N 57-1000331-01) have the following restrictions:
- D_Port for these modules in X6 ICL ports is supported without electric or optical loopback tests.
- D_Port on any user port connected by a QSFP require all four user ports within the same QSFP to be in D_Port mode.
- D_Port tests require all user ports in a QSFP to be in the same logical switch.
- Dynamic or On-Demand D_Ports are not supported on the user ports in these modules.
- If a D_Port test between a Brocade switch and an Emulex adapter is stopped shortly after the test has started, the adapter firmware may display "`No FC Cables connecting the port to switch`." The workaround is to restart the D_Port test until completion.

9.3.6 Forward Error Correction

- FEC is mandatory with Gen 6 Fibre Channel operating at 32Gb/s. 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 8.x Compatibility Matrix* for supported DWDM equipment and restrictions on FEC use.

9.3.7 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.

9.3.8 Ingress Rate Limiting

- Fabric OS 8.2 does not support ingress rate limiting on Brocade Gen 6 (G610, G620, G630, or X6) platforms.

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

9.3.9 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 for the Brocade X6 Director and Brocade 7840 is not supported and is blocked.
- External default route to the private IPv4 Class B network of 172.16.0.0/16 is unreachable over the management interface due to the existence of a more specific route from an internal Virtual Fabric ID address of 172.16.0.61/16 for FID 128. The solution is to delete the external default route or change it to a more specific address. The Virtual Fabric address will no longer block management access to the IPv4 Class B address range of 172.16.0.0/16.

9.3.10 Extension

- IP extension (IPEXT) between a Brocade 7840 and an SX6 blade is supported only if the 7840 is running FOS 8.0.1 or later. FCIP extension between a Brocade 7840 with FOS 7.4 and an SX6 blade with FOS 8.0.1 or later is supported. Extension between a Brocade 7840 or SX6 and a Brocade 7810 is supported only if the 7840 or SX6 is running FOS 8.2.0 or later. The following table documents the combinations.

Site1 Switch/Blade	Site1 Firmware	Site2 Switch/Blade	Site2 Firmware	Supported
7840	8.0.1 or later	7840	7.4.x or later	Both FCIP and IPEXT traffic
SX6	8.0.1 or later	7840	7.4.x	FCIP traffic but not IPEXT traffic
SX6	8.0.1 or later	7840	8.0.1 or later	Both FCIP and IPEXT traffic
SX6	8.0.1 or later	SX6	8.0.1 or later	Both FCIP and IPEXT traffic
7840	8.2.0 or later	7810	8.2.1 or later	Both FCIP and IPEXT traffic
SX6	8.2.0 or later	7810	8.2.1 or later	Both FCIP and IPEXT traffic

- Do not to configure the HA VE pair (VE16, VE26), (VE17, VE27), (VE18, VE28), and so on, where each VE in the pair is in a different LS with a different traffic policy (port-based routing and exchange-based routing). The workaround is to configure different HA VE pairs such as (VE16, VE27), (VE17, VE26), and so on when putting each VE pair in a different LS with a different traffic policy.
- When Non-Terminate TCP (NT-TCP) is enabled on traffic control lists (TCLs) and a firmware downgrade to FOS 7.4.1d is attempted on the Brocade 7840, the downgrade will be blocked. Users must remove NT-TCP from the TCLs with NT-TCP enabled in order to downgrade the firmware. After the firmware is downgraded to FOS 7.4.1d, users can re-enable the NT-TCP flag.
- Nondisruptive firmware downloads for IP extension support nondisruption to IP traffic for all terminate TCP connections. UDP and non-terminate TCP traffic may be disrupted during HCL.
- After firmware downgrade completion, the Brocade 7840 needs a switch reboot and the SX6 needs a blade power-cycle. HCL is not supported on firmware downgrades.

  When downgrading from FOS 8.1.0a to an earlier release during HCL, the following message may be seen. This message can be ignored and has no functional impact.

  ```
  [ESM-1100], 343, SLOT 1 FID 128, WARNING, switch0, esm_cfg_ip.c:2226 Could not get PMTU info from cfgdb
  ```

- If a Brocade 7840 or Brocade X6 Director with an SX6 blade in a non-VF is assigned a fabric ID other than 128, then during a heavy traffic load, the back-end ports on the 7840 and SX6 may encounter credit loss, which can result in traffic disruption over the VE ports. This is tracked as Defect 660208.

9.3.11 Brocade Analytics Monitoring Platform

- FOS 8.2.0 and later support vTap on Brocade Gen 5 and Gen 6 platforms to be monitored by the Brocade Analytics Monitoring Platform. The supported Brocade platforms include: 6505, 6510, 6520, DCX 8510, 6543, 6545, 6546, 6547, 6548, M6505, 6558, G610, G620, G630, X6.
- vTap is not supported on QSFP ports (port 96 to 127) on the Brocade G630 in Virtual Fabric (VF) mode. It is supported in non-VF mode only.
- If QSFP ports (port 96 to 127) on a Brocade G630 switch are part of the sys_analytics_vtap flow definition, the mirrored frames from these QSFP ports will be discarded for some duration after an HA reboot or after a sys_analytics_vtap flow de-activation.
- The Analytics Switch Link (ASL) connection is not supported on QSFP ports (port 96 to 127) on the Brocade G630. Enabling ASL on these ports will segment the link.
- vTap and auto-discovered AF_Ports do not support high availability. In the event that an AF_Port is rediscovered by a fabric switch after a domain change on the attached Analytics Monitoring Platform and is followed by an `hafailover` or `hareboot` of the fabric switch, the remote AF_Port information will be stale and vTap flows cannot be activated. In this case, use one of the following workarounds:
- Manually configure the AF_Port after `hafailover` or `hareboot`.
- Disable and then enable the AF_Port on the Analytics Monitoring Platform.
- Deactivate the vTap flow before the firmware download, hafailover, or hareboot, and activate the vTap flow again.
- vTap and CS_CTL are mutually exclusive on a fabric switch. If CS_CTL is enabled on one port, the entire switch cannot enable vTap. An F_Port trunk supporting CS_CTL must have all ports in the trunk group enabling CS_CTL. Similarly, in order to enable vTap, all ports in an F_Port trunk must have CS_CTL disabled. In addition, the master port of a trunk should remain the same between CS_CTL enabling and disabling. If this sequence is not followed, vTap may remain active even after CS_CTL is enabled on an F_Port, or the error message "`Disable QoS zones error`" may be observed when enabling vTap. A suggested method is to use the following sequence:
    1. When enabling CS_CTL mode, enable it on all slave ports, followed by enabling it on the master port, noted as port M.
    2. When disabling CS_CTL mode, disable all active ports in the trunk, except the master port M. Disable CS_CTL mode on port M. Enable all ports in the trunk followed by disabling CS_CTL mode on the remaining ports.
    3. When CS_CTL is enabled on a port without any connection, after rebooting and disabling CS_CTL, vTap cannot be enabled. The workaround is to enable the port as a SIM port after disabling CS_CTL and then to toggle the port and remove the SIM port configuration.
- vTap and in-flight encryption or compression compatibility are supported only on the following platforms: Brocade DCX 8510, X6, G620, G630, and 6520. On DCX 8510 and 6520 platforms, the chassis configuration "vTap and Encryption/Compression Coexistence Mode" must be enabled when ports with vTap enabled and ports with in-flight encryption or compression enabled belong to the same ASICs. Refer to the hardware installation guides for these platforms for the port-to-ASIC mapping boundary.
- When "vTap and Encryption/Compression Coexistence Mode" is enabled, the total IOPS on the same ASIC is limited to 250,000. If the IOPS exceeds the limit, the vTap flow will be deactivated.
- When "vTap and Encryption/Compression Coexistence Mode" is enabled, the effective default zone access mode must not be "All Access."
- Running the `flow --show sys_analytics_vtap` command when vTap and QoS High compatibility mode is enabled but the vTap flow is not active may display the following message incorrectly: "`Enable vTap and QoS High Priority Zone Compatibility Mode to active vTap flow. Please use the configurechassis command to enable this compatibility mode.`" This is tracked as Defect 604429.

- After a `configuredownload` followed by `switchenable` or a flow statistics reset on the Brocade X6 and G620, MAPS may incorrectly report a VTAP IOPS > 250,000 violation.
- AMPOS 2.2.0 or later is required to support FC32-64 blades. Users should upgrade the Brocade Analytics Monitoring Platform to AMPOS 2.2.0 or later before adding FC32-64 blades to the X6.

9.3.12 Flow Vision

- Flow Vision supports only logical group names that begin with alphabetic characters.
- Frame count statistics of a Flow Monitoring flow may stop incrementing after a `statsclear` command. To work around the problem, users may run the `slotstatsclear` command. To recover from such condition, users should run the following steps:
  (a) Disable all flows in the logical switch.
  (b) Delete the problem flow.
  (c) Create a new flow to replace the problem flow.
  (d) Activate the new replacement flow.
  (e) Verify the new replacement flow.
  (f) Enable all other flows.
- IO Insight metrics are supported on ingress and egress ports on the Brocade X6 and on egress ports on Brocade G620 and G630 switches. They are not supported on Brocade G610 switches.
- Activating a Flow Monitoring flow on an egress port on the Brocade G610 with the `-frametype` parameter may cause a resource not available error.
- FC-NVMe flow IO Insight metrics are supported with a Flow Monitoring flow on a port defined on the Brocade G630 and FC32-64 blade only. Users must use the `-nsid` parameter with the `flow --create` command to monitor FC-NVMe flows. Either a valid Name Space ID (NSID) must be used or the `all` keyword must be used to select all valid NSIDs.
- When a flow is created with the `-frametype` parameter, FC-NVMe traffic is included in the metrics for the following SCSI frame types: SCSI, SCSITur, SCSIXferrdy, and SCSIGoodStatus.
- Flow Mirroring is not supported on QSFP ports (port 96 to 127) on the Brocade G630 with Virtual Fabric (VF) mode. It is supported in non-VF mode only.
- Mirror ports are not supported on QSFP ports (port 96 to 127) on the Brocade G630. Enabling a mirror port on these ports will disable the ports.
- If a flow is imported to MAPS and configured with incorrectly configured flow metrics thresholds, a high frequency violation of the thresholds may result in very slow display of the RASLOG alerts for the violations.

9.3.13 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.)

9.3.14 MAPS

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

9.3.15 Miscellaneous

- If the ambient temperature is above the recommended operational limit, the power supply units may shut down, in particular when the ambient temperature is above 62°C for Brocade X6 Directors. This will result in the switch being shut down without any warning. Refer to the *Brocade G620 Hardware Installation Guide* and the *Brocade X6-8/X6-4 Hardware Installation Guide* for the recommended ambient temperature limits for the switches.
- 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.
- 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.
- When the zoning database size exceeds the maximum supported limit, 2 MB for directors and 1 MB for fixed-port switches, a firmware upgrade from FOS 8.0.x to FOS 8.1.0a or later may be blocked. Users should run the `cfgSize` command to make sure that the "Zone DB max size" is not exceeded.
- ASN is not supported with 4x32GFC breakout optics (P/N 57-1000351-01).
- When connecting 4x32G FC breakout optics (P/N 57-1000351-01) to 32Gb/s SFP peer ports on Gen 6 platforms, ports may auto-negotiate to 16Gb/s after `switchdisable` and `switchenable` on the Gen 6 platforms with 32Gb/s SFP ports. To avoid this issue, the Gen 6 platforms with 32Gb/s SFPs should be upgraded to FOS 8.2.0 or later or to FOS 8.1.2b or later. This issue is more likely to occur when the Gen 6 platforms with 32Gb/s SFPs are X6 directors.
- Brocade G630 LEDs illuminate amber and green during power-up.
- When launching Web Tools over an HTTPS connection and a security warning message for an untrusted certificate pops up, the pop-up message should be responded to within 20 seconds.
- When upgrading to FOS 8.1.0b or later and HTTPS is enabled, administrators must have the Certificate Authority (CA), intermediate, and root certificates installed to ensure that the chain of certificate validation is successful. HTTPS will be disabled in FOS 8.1.0b or later if the chain of certificate validation fails. To verify if the CA is correct and the CA chain validation is successful, issue the following command on a Linux server:

  ```
  openssl verify -CAfile ca.pem servercert.pem
  ```

  In the example above, `ca.pem` is the CA certificate and `servercert.pem` is the switch certificate. If the switch certificate is signed by the intermediate certificate, use the completed chain CA certificate; otherwise, use the root certificate.
- 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.

Chapter 10: Defects

10.1 Closed with Code Changes in FOS 8.2.1a

Defect ID:	FOS-804745		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1	**Technology:**	Configuration Fundamentals
Symptom:	RASLog [C3-1021]"Encryption Compression Block error" and IFL link will not come online when enabling ISL_RDY mode and Encryption on IFL links		
Condition:	An Ex-Port to E-Port link (IFL) will flap continuously, when both Encryption and ISL_RDY mode are enabled on the Ex-Port. The port will not come online.		
Workaround:	Use either ISL RDY mode or Encryption on a Ex-Port, but not both on the same port.		

Defect ID:	FOS-804650		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1	**Technology:**	Virtual Fabrics
Symptom:	Software verify will be seen for each port that is attempted to be moved between partitions.		
Condition:	Issue observed when moving FC32-64 blades between Logical partitions.		
Recovery:	Software verify messages observed on console is harmless. The movement operation will complete without any side effects.		

Defect ID:	FOS-804224		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.2.1	**Technology:**	FCIP
Symptom:	Observed ESM-1101 during a SX6 blade slotpower off with one of the following: esm_cfg_sys.c:1586 esm_portcfg_clear() failed rc:176 esm_slot.c:1603 failed to release GE:10/ge2 rc:176 .		
Condition:	ESM-1101 event can occur during a slotpoweroff of an SX6 blade.		
Recovery:	These are warning messages and are self-recovering		

Defect ID:	FOS-804203		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Virtualization
Reported In Release:	FOS8.2.1	**Technology:**	Virtual Fabrics
Symptom:	System panic may occur, although rarely, while collecting supportsave on a GEN6 chassis systems		
Condition:	Supportsave collection operation may trigger the system panic		
Recovery:	System will reboot after panic to recover. Due to hafailover, the standby CP will take over as active CP and assist in the smooth operation of the system		

Defect ID:	FOS-804131		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.2.1	**Technology:**	WAN Performance Analysis Tools
Symptom:	portcmd --wtool stop-all error message isn't clear that its only intended for Automated WAN Tool sessions.		
Condition:	When attempting to stop User WAN Tool sessions with portcmd --wtool stop -all command		

Workaround:	Use "portcmd --wtool <wt-id> stop" command to stop User WAN Tool sessions

Defect ID:	FOS-804126		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1	**Technology:**	CLI - Command Line Interface
Symptom:	GE speed mismatch between 'switchshow' output and 'portcfgge --show' output. Also unable to change port speed to 1G or issue 'portcfgdefault'. Configuration replay errors seen during switch bootup and if the port is configured as a LAN 10G port, it may come up as a WAN port after a reboot		
Condition:	On 7810, if GE port speed is set to 10G on any GE port and reboot is performed after a time based license has expired		
Workaround:	Install a valid license prior to rebooting the switch.		
Recovery:	Install a new valid license, which is not expired, and reboot the switch. Alternatively the port can be recovered by disabling / enabling autonegotiation using 'portcfgge <ge-port> --disable -autoneg' followed by 'portcfgge <ge-port> --enable -autoneg'.		

Defect ID:	FOS-804124		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.2.1	**Technology:**	WAN Performance Analysis Tools
Symptom:	Unable to enable a WAN Tool session		
Condition:	When configured WAN Tool sessions exceed the supported limits, while all sessions are in a disabled state, results in the inability to enable WAN Tool session in this state.		
Workaround:	Keep the number of configured WAN Tool sessions for a DP within the supported limit.		
Recovery:	Delete WAN Tool sessions on a DP to within the supported amount. Then attempt to enable the session in question.		

Defect ID:	FOS-804072		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1	**Technology:**	Management GUI
Symptom:	WebTools displays incorrect property members for peerzones		
Condition:	When peerzone is empty after removing peerzone alias using WebTools		
Workaround:	Ensure that the peerzone is not empty after removing the alias. The issue does not occur if member exist in the peer zone after alias removal.		

Defect ID:	FOS-804069		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1	**Technology:**	Software Installation & Upgrade
Symptom:	System-description attribute of "lldp --show" command incorrectly displays FOS 8.2.1 version.		
Condition:	Issue may be observed after non-disruptive downgrade from FOS v8.2.1 to v8.2.0 firmware version.		
Workaround:	Before firmware downgrade, system-description attribute can be modified to display correct firmware version using "lldp --config -sysdesc <string>" command.		
Recovery:	After firmware downgrade, system-description attribute can be modified to display correct firmware version using "lldp --config -sysdesc <string>" command		

Defect ID:	FOS-803885		
Technical Severity:	Medium	**Probability:**	null
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.2.1	**Technology:**	Extended Fabrics
Symptom:	Removing the IP from a circuit that has SLA returns error for the wtool and can leave the circuit in a out-of-sync state, which may cause future modifications to fail.		
Condition:	Removing a local-ip address or remote-ip address from a circuit that also has an SLA configured.		
Workaround:	Remove the SLA from the circuit first, then remove the IP address.		

Defect ID:	FOS-803705		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS8.1.0	**Technology:**	Port Bring-up
Symptom:	For the New CLI Command PortcfgCleanAddress (that can configure on a port-by-port basis to enable Clean Address Bit) Configuration is disabled by default.		
Condition:	If the Clean Address Bit configuration is enabled for the port, then the FLOGI response on this port shall always have the "Clean Address Bit" set.		
Workaround:	Do not use the new CLI without vendor guidance. Please contact Technical Support first when the setting is desired.		
Recovery:	Do not use the new CLI without vendor guidance. Please contact Technical Support first when the setting is desired.		

Defect ID:	FOS-803283		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS8.0.2b	**Technology:**	Trunking

Symptom:	Duplicate PID observed on ports that were once part of F_Port trunks.
Condition:	The area bound to F-port trunks can be lost if the F-port trunk is disabled during hafailover.
Workaround:	Make sure at least one F-port in each F-port trunk is online during hafailover.
Recovery:	Do the following on every logical switch: 1. Identify which F-ports share PIDs. 2. portdisable all F-ports that share PIDs. 3. If the ports are a F-port trunk, 'porttrunkarea --disable' those ports. 4. If the ports are single F-ports, 'portaddress --unbind' those ports. 5. After both 3) and 4) above are done, then proceed. 6. Create the F-port trunks again: 'porttrunkarea --enable' 7. portenable the single F-port.

Defect ID:	FOS-803259		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.2.1	**Technology:**	FCIP - Fibre Channel over IP
Symptom:	During the config replay portion of hafailover / HCL indicating that an error has occurred displays [ESM-1101], ERROR, esm_ha.c:8289 esm_ipaddr_add() failed (rc:25)		
Condition:	When a switch is in the middle of a warm recovery (such as a ha reboot) and a slot is power cycled, the configuration may not be replayed or pushed to the slot. This will leave the slot in a state where it may have an incomplete or no configuration.		
Workaround:	Do not attempt to power cycle a blade during any kind of CP boot operation. This includes removing and reinstalling the blade.		
Recovery:	An additional power cycle of the slot in question will recover the configs.		

Defect ID:	FOS-660425		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS8.1.2a	**Technology:**	Routing
Symptom:	Hosts unable to see target in a deactivated TI zone setup		

Condition:	Logical switch has a failover-disabled TI Zone that is deactivated. Paths in the fabric attempt to use the E-ports in the deactivated TI Zone.
Workaround:	After deactivating the TI Zone, disable all E-ports that have the same destination as the E-port with the DC-only route. Then enable them all to clear the condition.
Recovery:	Disable all E-ports that have the same destination as the E-port with the DC-only route. Then enable them all to clear the condition.

Defect ID:	FOS-658940		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS7.2.1_HIL3	**Technology:**	Fibre Channel Services
Symptom:	Devices connected to an Access Gateway can be inadvertently logged out and not function normally.		
Condition:	This occurs when a misbehaving device tries to abort an exchange that is already closed.		
Recovery:	Try to bounce the port; This may not always work.		

Defect ID:	FOS-658796		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.0.2c	**Technology:**	Fastwrite
Symptom:	FCIP Open Systems Tape Pipelining (OSTP) Read/Write timeout errors.		
Condition:	During OSTP operations, if the server requests retransmit of read data and status (due to frame loss or FC CRC errors), the ELS-REC and SRR sequences complete, but the server never confirms receipt of the data and the status and the I/O is eventually timed out with an Abort Sequence.		

Defect ID:	FOS-632433		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Security
Reported In Release:	FOS7.4.1e	**Technology:**	LDAP - Lightweight Directory Access Protocol
Symptom:	LDAP user role mapped to user created switch defined role results in failed access in shell.		
Condition:	This may be seen following an upgrade to FOS7.4.1d or higher.		

10.2 Closed with Code Changes in FOS 8.2.1

Defect ID:	FOS-803808		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	System
Reported In Release:	FOS8.1.2	**Technology:**	Optics
Symptom:	A trend in the deterioration of optics signals that point to impending failure of the corresponding optics. This is a new enhancement to proactively monitor and flag such optics that show signs of signal weakening over time.		
Condition:	There may be no obvious symptom or signs of any link level errors for these properly functioning and online SFPs. But a trend in signal deterioration over time hints at impending failure. This trend is flagged in internal Raslogs.		
Workaround:	The user will need to monitor these internal raslogs for signs of further degradation of these operating parameters and proactively replace them to prevent impending disruptive failure of such optics.		

Defect ID:	FOS-803782		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Monitoring/RAS
Reported In Release:	FOS8.2.1	**Technology:**	supportShow

Symptom:	Supportsave does not have portshow for ports present in logical switch
Condition:	This problem exists with FOS8.2.0x

Defect ID:	FOS-803522		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS8.1.2a	**Technology:**	Trunking
Symptom:	Devices may encounter link down events.		
Condition:	default deskew values may cause the OOO frame delivery to the end device and if the end device cannot handle the OOO frame, it may cause the link down and link up.		
Workaround:	Instead of using trunked E-ports, use individual E-ports.		
Recovery:	The device recovers by itself, but may impact traffic.		

Defect ID:	FOS-803424		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.1.2	**Technology:**	FTRACE
Symptom:	The FCIP platforms and FCIP Extension blades include a Fibre Channel trace capability that captures some FC user payload. The trace is used to perform problem analysis for customer issues. However, the user data that is included in the traces is not needed for debug purposes, but it was inadvertently not excluded from the trace capture in the original design of the trace facility. All other FOS switches do NOT collect any user data.		
Condition:	When select Fibre Channel frames are passed through an FCIP tunnel between switches in a fabric.		

Defect ID:	FOS-803406		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management

Reported In Release:	FOS8.1.2	**Technology:**	Configuration Fundamentals
Symptom:	Support NEW OUIs that will be used on future platforms		
Condition:	This is a new development to add support for the NEW OUI		

Defect ID:	FOS-803349		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS7.4.2b	**Technology:**	Management GUI
Symptom:	In Web Tools, "Print Effective Zone Configuration" windows shows empty on Zone Admin, even though effective configuration exists.		
Condition:	This is encountered when using Web Tools.		
Workaround:	Use CLI instead of Web Tools.		

Defect ID:	FOS-803337		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.0.2d	**Technology:**	CLI - Command Line Interface
Symptom:	Switch panic after running CLI "nodefind" with an invalid WWN.		
Condition:	When WWN input exceeds a valid WWN length.		
Workaround:	Input a valid WWN		

Defect ID:	FOS-803195		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS8.2.0a	**Technology:**	Name Server
Symptom:	CLI nsshow has device discovered as Unknown or invalid device type.		

Condition:	Various vendors' devices are not discovered properly by name server, and GPN_FF queries are rejected with "no FC-4 types", rather than "no FC-4 features" .

Defect ID:	FOS-802874		
Technical Severity:	High	**Probability:**	null
Product:	Fabric OS	**Technology Group:**	FICON
Reported In Release:	FOS7.4.1d9	**Technology:**	FICON emulation
Symptom:	Tape restoring job was abend with following message: "N 0020000 #K1 18162 14:51:46.62 JOB00083 00000090 IEC537I BLOCK COUNTS: TLABEL=307, DCB=308 M 0020000 #K1 18162 14:51:46.62 JOB00083 00000090 IEC023I 237-04,IFG0552R,YTVRSG03,DFDSS,FROM,0C4".		
Condition:	This may be seen when host read-forward command chain with multiple large data-chained commands. Tape records being read are very small (less than size of first read command).		

Defect ID:	FOS-802842		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	System
Reported In Release:	FOS8.1.2a	**Technology:**	CLI
Symptom:	Firmwareshow and other CLI commands take a long time to complete and firmwaredownload may abort from timeout.		
Condition:	This may occur after dnsconfig is enabled without a proper DNS server on X6 directors.		
Workaround:	Update DNS configuration with proper entries or temporarily remove the DNS configuration (dnsconfig --delete) before upgrade.		

Defect ID:	FOS-802162		
Technical Severity:	Low	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Extension
Reported In	FOS8.2.1	**Technology:**	FCIP

Release:			
Symptom:	IPEXT L2COS and IPEXT DSCP values don't persist across reboots, this behavior is observed on IP Extension platforms.		
Condition:	This will occur when a hybrid tunnel is configured and at least one of the circuits has L2COS and/or DSCP marking values configured for the IP priorities. These values will not persist across hareboot/hafailover/reboot events.		
Recovery:	These values can be reconfigured manually after the reboot.		

Defect ID:	FOS-802018		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.2.1	**Technology:**	Flow Vision
Symptom:	Observed "MP-5003: Continuous memory increase detected in appsrvrd".		
Condition:	After running VM IO, when VMID deregister without flow monitoring installed.		
Workaround:	Use hareboot or hafailover to recover memory until an upgrade to a fixed release.		

Defect ID:	FOS-801322		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.2.1	**Technology:**	Extended Fabrics
Symptom:	Switch G610 will experience frame timeout drops due to the incorrect VCs being use for frame traffic. This problem will impact end to end traffic flow in long distance QoS mode on ISLs.		
Condition:	When using G610 switch, any ISL that is configured with long distance Qos Mode.		
Workaround:	Update to the FOS version with the fix or avoid using QoS mode on the long distance ISL.		

Defect ID:	FOS-801305		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1	**Technology:**	Management GUI
Symptom:	Web Tools does not allow user to change the password and it shows an error message "Invalid username and password".		
Condition:	The user cannot change password from Web Tools once the account's password is expired.		

Defect ID:	FOS-800980		
Technical Severity:	High	**Probability:**	null
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS8.1.2a	**Technology:**	Routing
Symptom:	Standby CP hung. Most of the time, standby CP reboot and recover by itself without any impact; However, occasionally, the issue may impact active CP causing traffic failure.		
Condition:	This seems to occur on directors running FOS8.1.0 or later while access time-of-the-day related functions on standby CP.		
Recovery:	When there is traffic impact, recover switch by manually reboot the hung standby CP.		

Defect ID:	FOS-800934		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.1.2b	**Technology:**	CLI - Command Line Interface
Symptom:	User cannot run any command on switch, and encounters an error: "shmInit: shmget failed: No space left on device"		
Condition:	It happens after multiple supportsave test run.		
Workaround:	hareboot/hafailover		

Defect ID:	FOS-660466		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Virtualization
Reported In Release:	FOS7.4.1d	**Technology:**	Access Gateway
Symptom:	Devices connected to AG cannot come online.		
Condition:	When device comes online and performs Class2 login to AG immediately. Device receives two ACK_1 responses which causes the device to enter a defective state and/or reset.		
Workaround:	Configure device for Class3 communication. If Class3 is not supported or allowed by the customer, try making the device re-login, or reboot the device, or disable/enable the AG port connected to the device.		

Defect ID:	FOS-660399		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.0.2c	**Technology:**	RAS - Reliability, Availability, and Serviceability
Symptom:	supportshow / supporsave ouput reflects a missing display line "CURRENT CONTEXT -- X, X" in the output of some CLI commands such as switchshow in FOS 8.x and higher versions.		
Condition:	This is encountered when running supportshow or supportsave in FOS 8.x or higher versions.		

Defect ID:	FOS-660387		
Technical Severity:	High	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS7.4.2a	**Technology:**	Extended Fabrics
Symptom:	In-flight encryption fails on E-port to EX-port when disabling ISL R_RDY mode.		
Condition:	This may be encountered on FCR with ISL R_RDY enabled		

Defect ID:	FOS-660313		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.0.1b	**Technology:**	CLI - Command Line Interface
Symptom:	Switch panic after daemon running out of threads.		
Condition:	When running script doing multiple iterations of CLIs per second, such as such as 'switchshow'.		
Workaround:	Insert delay between commands.		

Defect ID:	FOS-660290		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.1.0_LNX	**Technology:**	Web Tools
Symptom:	HTTPs does not work when DHCP is configured.		
Condition:	This issue is seen rarely when using DHCP.		
Recovery:	Restart weblinker or hareboot the switch for recovery.		

Defect ID:	FOS-660258		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.1.0c	**Technology:**	Hardware Monitoring
Symptom:	X6 platform may experience intermittent PSU failures		
Condition:	This may be encountered when the PSU controllers' firmware versions are down Rev.		
Recovery:	First upgrade the FOS firmware to a version with a fix for this defect. Check each PSU controllers version using the CLI command: psutil --version -p <psu number> If any PSU is down Rev then upgrade the PS firmware using CLI command psutil --upgrade -p		

	<psu number> Upon completion of PSU upgrade use CLI command psutil --version -p <psu number> to confirm that the PSU Controllers firmware versions are updated to the latest versions shown below: 1. PRI (Primary Controller) Version 3.4 2. LLC (Digital LLC Controller) Version 3.2 3. COM (Communications controller) Version 3.1

Defect ID:	FOS-660213		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.1.0a	**Technology:**	Hardware Monitoring
Symptom:	Software 'verify' error during portloopbacktest.		
Condition:	This results from a race condition encountered on G620 platform		
Recovery:	Rerun the test could pass. It does not happen always.		

Defect ID:	FOS-660156		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.1.0c	**Technology:**	FCIP - Fibre Channel over IP
Symptom:	FICON Aborted Sequences on a 7840 or SX6 FICON XRC Emulation Enabled tunnel		
Condition:	This issue occurs in a small timing window. If the LCU sends CE status which is accepted, then the LCU sends DE status and then sends Attention status to the channel before the DE exchange is closed.		

Defect ID:	FOS-660134		
Technical Severity:	Medium	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.2.0	**Technology:**	Hardware Monitoring
Symptom:	Third party call home system unable to process inventory report files		

Condition:	Inventory report file submitted in *.json when expecting *.xml

Defect ID:	FOS-660017		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.1.2a	**Technology:**	Extended Fabrics
Symptom:	After configdownload, SSL CA certificate name is listed in the config parameter in the CLI configure command, though certificates are removed from the switch.		
Condition:	1. Install the SSL certificates on the switch. 2. Configupload from the switch 3. Remove the SSL certificates on the switch. 4. Configdownload to the switch with the configuration uploaded in step (2).		

Defect ID:	FOS-659935		
Technical Severity:	Medium	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.1.2a	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	SNMP response time via switch serial console, telnet, or ssh may be slow and snmpwalk may fail to complete.		
Condition:	This may be observed when performing an snmpwalk.		

Defect ID:	FOS-659528		
Technical Severity:	Low	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS7.4.1d	**Technology:**	CLI - Command Line Interface
Symptom:	The output from configshow / configupload may show some random characters as config key		

Condition:	This may be seen after making a configuration change using other config commands such as tstimezone

Defect ID:	FOS-659099		
Technical Severity:	Medium	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.1.2	**Technology:**	MAPS - Monitoring and Alerting Policy Suite
Symptom:	Misleading warning "Invalid Quiet time. Quiet Time should be greater than timebase" is displayed when invalid quiet is configured for MAPS rules with NONE timebase.		
Condition:	It happens with all MAPS rules with NONE timebase when an invalid quiet time which is less than sample time is configured.		

Defect ID:	FOS-658992		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.1.2a	**Technology:**	High Availability
Symptom:	Software verify error detected after hareboot on G610		
Condition:	Rare locking sequence race condition during hareboot caused software verify.		

Defect ID:	FOS-658812		
Technical Severity:	High	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Other
Reported In Release:	FOS8.1.1a	**Technology:**	Other
Symptom:	Legacy Brocade HBA or FOS Access Gateway 16G ports with FEC enabled only gets 8 credits		
Condition:	This is encountered for trunked F-PORT		

Defect ID:	FOS-658796		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.0.2c	**Technology:**	Fastwrite
Symptom:	FCIP Open Systems Tape Pipelining (OSTP) Read/Write timeout errors.		
Condition:	During OSTP operations, if the server requests retransmit of read data and status (due to frame loss or FC CRC errors), the ELS-REC and SRR sequences complete, but the server never confirms receipt of the data and the status and the I/O is eventually timed out with an Abort Sequence.		

Defect ID:	FOS-658739		
Technical Severity:	Critical	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS7.4.1d	**Technology:**	Fibre Channel Routing
Symptom:	When a new NPIV device is added to the effective zoning cfg, there can be a short window of frame lost for other NPIV devices on the same physical port running traffic.		
Condition:	When the NPIV is Hard Zoned, adding a new NPIV device on another port can cause a momentary loss of traffic.		
Workaround:	Do not add new NPIV devices into effective HW zoning configuration where other NPIV devices are connected to the same physical port running traffic.		

Defect ID:	FOS-658519		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.0.2b	**Technology:**	Syslog
Symptom:	After upgrade to FOS 8.0.x from v7.x, There is a missing '|' separator between slot and wwn in [MAPS-1003] raslog.		

Condition:	This defect impacts FOS v8.0.x and above only. The missing separator caused customer parser script to fail.

Defect ID:	FOS-658484		
Technical Severity:	Medium	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.1.2	**Technology:**	Management GUI
Symptom:	Webtools allows non-admin "user" role to set E-Port credits instead of greyed it out.		
Condition:	It happens only with Webtools.		

Defect ID:	FOS-657234		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.1.1	**Technology:**	MAPS - Monitoring and Alerting Policy Suite
Symptom:	On G610, MAPS alerts may not be triggered in case of temperature exceeds threshold.		
Condition:	Happens only with G610 on a high temperature environment.		

Defect ID:	FOS-657173		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.0	**Technology:**	Configuration Fundamentals
Symptom:	A Peer zone containing empty alias member(s) as the only principal members of the peerzone will not be displayed properly for: 'zoneshow', 'zoneshow --verbose', 'zoneshow --peerzone [user | target | all]' Also, REST GET operations performed on this type of peerzone will not be populated with the correct format in the response.		
Condition:	If a WWN without colon is given as principal peer zone member, then the given WWN is consider as an alias. Also we might not have an		

	entry for that alias. If a Non-existing alias is given as only principal member of the peer zone, then due to zoning logic failure, property members will be displayed without the verbose option.
Workaround:	Provide colons at appropriate places for WWN zone members.
Recovery:	Provide colons at appropriate places for WWN zone members.

Defect ID:	FOS-657018		
Technical Severity:	Medium	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.1.2	**Technology:**	Management GUI
Symptom:	When use Web Tools to configure E port credit, F port Buffers value is changed as a side effect,		
Condition:	F port buffers value not inline with CLI value		

Defect ID:	FOS-656866		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.0	**Technology:**	Configuration Fundamentals
Symptom:	Switch may hit out of memory due to multiple instances of dhclient running when DHCPV6 is turned on and no DHCP service running on the network.		
Condition:	It happens when DHCPV6 is enabled and DHCP server is not running on the network.		
Workaround:	Avoid using DHCPV6 wherever possible.		

Defect ID:	FOS-656635		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.0	**Technology:**	Configuration Fundamentals

Symptom:	Zone merge can take a long time to complete and the zoned process consumes high CPU usage.
Condition:	During a fabric merge, if the zone configuration has many TI zones (15 to 25 TI zones), then the zone merge will take more time to complete.
Workaround:	Remove unwanted TI zones from the configuration.
Recovery:	Stop the zone merge by disabling the fabric link.

Defect ID:	FOS-656579		
Technical Severity:	Medium	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.1.1a	**Technology:**	MAPS - Monitoring and Alerting Policy Suite
Symptom:	Output of MAPS summary report in mapsdb displays port 0 differently from other ports		
Condition:	The inconsistency in the MAPS summary output is only seen with port 0.		

Defect ID:	FOS-656353		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.0	**Technology:**	Configuration Fundamentals
Symptom:	Switch panic during platform boot up		
Condition:	During multiple switch reboot or hareboots may hit this issue.		

Defect ID:	FOS-656092		
Technical Severity:	Medium	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.1.1a	**Technology:**	Hardware Monitoring
Symptom:	System LED of G610 remains green even after hitting high		

	temperature threshold.
Condition:	It would happen only on G610

Defect ID:	FOS-655881		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.0	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	Snmpwalk and connecting to switch MIB browser and Net-snmp are TIMEDOUT		
Condition:	It happens after clearing snmpstatistics using command "snmpstatistics --clear snmp", the Throttling config was removed accidentally.		

Defect ID:	FOS-655837		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS7.4.1e	**Technology:**	High Availability
Symptom:	Sensor voltage not in range during hafailover leads to a cold recovery.		
Condition:	This may result from a voltage not in range reading from the voltage sensor logged via the raslog message HIL-5010.		

Defect ID:	FOS-655611		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.0	**Technology:**	Configuration Fundamentals
Symptom:	May notice an FSPF event on ports 44-47 after enabling encryption on G620.		

Condition:	May notice an FSPF event on ports 44-47 if ports 44-47 was enabled while enabling encryption on G620.
Workaround:	Disable ports 44-47 first before enabling encryption.
Recovery:	As a precaution, I rebooted the G620 Wedge switches just to re-stabilize the fabric.

Defect ID:	FOS-655404		
Technical Severity:	High	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS8.2.0	**Technology:**	Fibre Channel Routing
Symptom:	I/O disruptions (Interface Control Checks for active FICON devices) during Extension HCL operations		
Condition:	When the FCIP tunnel that is going through HCL is in a switch that is configured to use Exchange Based Routing.		
Workaround:	Unsure of a workaround; possible root cause analysis may help in determining a workaround.		
Recovery:	Recovery entails resetting the channels and restarting traffic.		

Defect ID:	FOS-654621		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.0	**Technology:**	CLI - Command Line Interface
Symptom:	Clihistory displays the user incorrectly when first login fails.		
Condition:	only when first login attempt fails.		
Recovery:	no functionality gets broken.		

Defect ID:	FOS-654503		
Technical Severity:	High	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Monitoring

Reported In Release:	FOS8.2.0	**Technology:**	D-Port - Diagnostic Port
Symptom:	D-Port Link traffic test will fail when user move ports to newly created logical switch.		
Condition:	If both the switches have the same domain ID, then D-port test will fail in link traffic test.		
Workaround:	Resolve the domain ID conflict by doing switchdisable and switchenable.		
Recovery:	Resolve the domain ID conflict by doing switchdisable and switchenable.		

Defect ID:	FOS-654403		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.2.0	**Technology:**	FCIP Tunnel Management
Symptom:	IP address modification for an IP that is attached to one or more SLA configured circuits will either fail with a message to re-enable the circuit or the circuit will get stuck in a 'test' state.		
Condition:	If a customer has a circuit configured with an SLA and an IP address modify request is attempted, the following events will occur: 1) At the start the circuit will be in an 'online' state (not in 'test' state), during the IP address modification the remote side will go down causing the circuit to change states. 2) Finally when the IP address modification finishes (with error or success), the circuit will most likely be stuck in a 'test' state.		

Defect ID:	FOS-653675		
Technical Severity:	Medium	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.1.1	**Technology:**	MAPS - Monitoring and Alerting Policy Suite
Symptom:	Violated rules for intermediate dates get deleted from DashBoard "Rules Affecting Health" section.		
Condition:	This would happen for rules that has NONE timebase.		

Defect ID:	FOS-653625		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS8.2.0	**Technology:**	ISL - Inter-Switch Linking
Symptom:	Configuring static link cost on trunk slave port(s) different than the cost of the trunk master causes 'Port Decom Without Disable" feature to not work correctly on the slave port(s) with the higher link cost.		
Condition:	This issue would only happen as a result of a incorrect static link cost configuration but we do not prevent the user from configuring different link costs on trunk ports.		
Workaround:	Do not configuring trunked ports with different link costs. The user should not do this regardless of this issue.		
Recovery:	Configure all ports in a trunk group with the same link cost		

Defect ID:	FOS-653466		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.0.2a	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	If a swDeviceStatus trap is generated from a port on the default switch, the swDeviceStatusTrap OID 'tail number' is inconsistent.		
Condition:	This may occur when a port on the default switch generates a swDeviceStatus trap.		

Defect ID:	FOS-652136		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS8.2.0	**Technology:**	Fibre Channel Routing

Symptom:	On a FCR backbone to edge setup, after fastboot on a backbone switch, online devices are missing from GE_PT response from a translate domain.
Condition:	This results from a timing issue when device is coming online and an RSCN is sent out before GE_PT is exchanged.

Defect ID:	FOS-651564		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.0	**Technology:**	Management GUI
Symptom:	Port 44-47 will be in the disabled state when any other port in the chassis is enabled with the Encryption mode.		
Condition:	User try to enable the Encryption functionality on any of the port apart from port 44-47 on G620 platform.		

Defect ID:	FOS-651554		
Technical Severity:	Medium	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS7.4.1e	**Technology:**	Hardware Monitoring
Symptom:	snmpconfig command returns "Failed to get snmp config info". As a result BNA is unable to monitor the switch.		
Condition:	This may occur as a result of prior configuration updates such as snmpconfig --set auditInterval 0.		

Defect ID:	FOS-650701		
Technical Severity:	Medium	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS7.4.1d	**Technology:**	CLI - Command Line Interface
Symptom:	Director class switches limit chassis name to 15 characters while fixed port switches can support 31 characters.		

Condition:	CLI command "chassisname" cannot change switch name to greater than 15 characters on directors.

Defect ID:	FOS-650268		
Technical Severity:	Medium	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.1.1	**Technology:**	MAPS - Monitoring and Alerting Policy Suite
Symptom:	Mapsrule create RoR (Rule on Rule) "-value" parameter accepts negative values.		
Condition:	For example, Run: mapsrule --createRoR test_ror_CRC_3 -monitor test_CRC -timebase hour -op g -value -100 -action raslog is accepted.		

Defect ID:	FOS-648052		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.2.0	**Technology:**	RAS - Reliability, Availability, and Serviceability
Symptom:	SupportSave ftp and sftp options will upload the files to user specified remote directory. If the remote directory is not pre-set as writeable, there is case that supportsave may proceed completely, not knowing the upload files are not uploaded properly if the remote server does not return an error for the upload operation.		
Condition:	Customer does not make supportsave upload directory as writable.		

Defect ID:	FOS-645904		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS7.4.2	**Technology:**	High Availability
Symptom:	After HA (hafailover/hareboot), the ports are online in switchshow, but internal states still have these ports marked offline. Consequently		

	routes are not programmed on these ports.
Condition:	This happens when there is a single port failed HArecover with RASLOG, [SWCH-1031], , SLOT 7 | FID 128, WARNING,, Port 0 recovery failed.

Defect ID:	FOS-645782		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.1.1	**Technology:**	Management GUI
Symptom:	E_Port Credits column does not exist on Web Tools.		
Condition:	Problem observed when using Web Tools.		
Workaround:	Use CLI "portCfgEPortCredits".		

Defect ID:	FOS-644950		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.0	**Technology:**	Inband Management
Symptom:	IPv6 Gateway address is not populated when IPv6 Autoconfiguration is enabled		
Condition:	issues show after ipaddress --clear		
Workaround:	remove IPv4, set IPv6, then add IPv4 back		

Defect ID:	FOS-643566		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS7.4.1a	**Technology:**	Management GUI
Symptom:	In webtools after the user has enables an active zone configuration and successfully saves it to the switch, zone config tab may indicate: effective zone config: none		

Condition:	This is a cosmetic issue in webtools zone config tab display, with no functional impact.

Defect ID:	FOS-643020		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS7.4.1e	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	During firmware upgrade, snmpd terminates, resulting in disruptive upgrade.		
Condition:	This is a corner case situation encountered when system goes for a reboot from upgrade and there is already a request in queue to be processed.		

Defect ID:	FOS-642118		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Security
Reported In Release:	FOS7.3.1c	**Technology:**	LDAP - Lightweight Directory Access Protocol
Symptom:	Fabric discovery fails through BNA when using user-name@domain.com format and weblinker.fcg encounters a panic.		
Condition:	This is encountered when fabric discovery is done through BNA using user-name@domain.com format.		
Workaround:	Use UPN only for username in BNA discovery.		

Defect ID:	FOS-640731		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS7.3.1b	**Technology:**	Fibre Channel Routing

Symptom:	Off-chip shared area routes are missing and cause connectivity issue for devices on shared area port after CP failures.
Condition:	Rare condition when there was a loss of heartbeat between Standby and Active CP which caused the Active CP to go down abruptly, both the primary and secondary IFIDs are not mapped to the shared area IFID. Also added debug trace to catch this condition.

Defect ID:	FOS-636695		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS7.4.1d	**Technology:**	Fibre Channel Routing
Symptom:	No traffic is traversing on two shared area ports.		
Condition:	Very rare and very difficult to reproduce.		
Recovery:	Disable both ports. Then enable both ports.		

Defect ID:	FOS-632433		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Security
Reported In Release:	FOS7.4.1e	**Technology:**	LDAP - Lightweight Directory Access Protocol
Symptom:	LDAP user role mapped to user created switch defined role results in failed access in shell.		
Condition:	This may be seen following an upgrade to FOS7.4.1d or higher.		

Defect ID:	FOS-630177		
Technical Severity:	Low	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.0.2	**Technology:**	MAPS - Monitoring and Alerting Policy Suite

Symptom:	MAPs may permit creation of upper limits that are larger than permitted values for certain fields.
Condition:	This may be encountered on Gen 6 platforms.

Defect ID:	FOS-624549		
Technical Severity:	Low	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.0.1b	**Technology:**	CLI - Command Line Interface
Symptom:	supportsave does not include the output form CLI command "seccertutil show -all"		
Condition:	This command encounters permissions issue and consequently this operation output is not reflected in supportsave		

Defect ID:	FOS-619351		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS7.4.1d	**Technology:**	CLI - Command Line Interface
Symptom:	Password distribute command is no longer functional.		
Condition:	This issue is seen in FOS v7.4.1d with CLI" distribute -p "PWD" -d "*""		

Defect ID:	FOS-614228		
Technical Severity:	Medium	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.0.1	**Technology:**	MAPS - Monitoring and Alerting Policy Suite
Symptom:	MAPS TRAP severity level is shown as Informational when the user has configured 'Trap recipient Severity level' to WARNING(3)		
Condition:	This is seen after the user runs snmpconfig command to set 'Trap recipient Severity level' to WARNING(3)		

Defect ID:	FOS-608997		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS7.3.1d	**Technology:**	CLI - Command Line Interface
Symptom:	CP panic may be encountered with some daemons (fcoed, raslogd, vsd etc) termination, followed by a warm recovery.		
Condition:	This occurs after executing setdbg CLI command such as 'setdbg SNMP 3' command.		

10.3 Closed without Code Changes in FOS 8.2.1

Defect ID:	FOS-803778	**Technical Severity:**	High
Reason Code:	Implemented	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS7.4.2	**Technology:**	Hardware Monitoring
Symptom:	Switch may experience hareboot or hafailover after high amount of memory is withheld by Weblinker process.		
Condition:	When external application repeatedly polls on maps rule information.		
Workaround:	Stop external application poll.		
Recovery:	Use hareboot or hafailover to recover memory.		

Defect ID:	FOS-803014	**Technical Severity:**	Medium
Reason Code:	Implemented	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.2.1	**Technology:**	Flow Vision
Symptom:	After issuing "statsclear", flow mirrored frame counts are invalid.		
Condition:	Symptom seen after a user issues "statclear".		

Defect ID:	FOS-802986	**Technical Severity:**	Medium
Reason Code:	Implemented	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.1.2a	**Technology:**	Web Tools
Symptom:	In Web Tools FC Port Configuration Wizard, after checking the box for "enable port after configuration", port is NOT enabled after configuration change.		
Condition:	It occurs when using BNA 14.4.1 to launch Web Tools.		
Workaround:	Launch Web Tools using IP address, then perform port disable and desired configuration change, port is then enabled after the change.		

Defect ID:	FOS-660211	**Technical Severity:**	Medium
Reason Code:	Accepted	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Other
Reported In Release:	FOS8.0.2c	**Technology:**	Other
Symptom:	ethif CLI command cannot be executed on standby CP		
Condition:	User encounters the below error when invoking ethif command on standby CP: ethif --show eth0 rbash: ethif: command not found		

Defect ID:	FOS-660208	**Technical Severity:**	High
Reason Code:	Not Reproducible	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.2.0a	**Technology:**	Extended Fabrics
Symptom:	Credit losses seen on a back-end port on extension platforms.		
Condition:	This is seen on 8G and 16G IP extension platforms, when the FID of default switch is not 128.		
Workaround:	Keep default switch FID as 128 on extension platforms.		

Defect ID:	FOS-660142	**Technical Severity:**	Medium

Reason Code:	Accepted	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.0.2c	**Technology:**	FCIP - Fibre Channel over IP
Symptom:	2018/02/16-11:04:32:068503, [XTUN-3101], 89/48, CHASSIS, ERROR, Brocade_7840, TCP:Slot=0 DP=0:New TCP connections dropped:16806, Max supported TCP connections:512 reached., lsm_cms.c, line: 4635, comp:, ltime:2018/02/16-11:04:32:068396		
Condition:	TCP sessions may fail to close and stay at INVALID state. Example of INVALID connection seen in the supportsave data: 0x50144bd80 0x0 INVALID 005 INV/001 TCP-L 0001 172.18.72.4/36579 <-> 172.27.72.10/350 0 0 66282164 0x5015e6800 0x0 INVALID 005 INV/001 TCP-L 0001 172.18.72.6/36334 <-> 172.27.72.12/350 0 0 66532588 These invalid connections continue to get accounted against the supported number of TCP connections and new TCP connection requests may get dropped if the max limit of number of supported TCP connections is reached.		

Defect ID:	FOS-659881	**Technical Severity:**	Medium
Reason Code:	Implemented	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS7.4.2a	**Technology:**	D-Port - Diagnostic Port
Symptom:	D-Port fails as protocol error for "HDA3" series 16G LWL 10km SFPs during the electric and optical loopback portion of the test.		
Condition:	D-port test reports failure when ran on 16G LWL SFP, Part Number 57-0000089-01, with serial number starting with 'HDA3' (sfpshow). This failure has no impact on production FC traffic itself.		
Workaround:	Avoid running D-port test on 16G LWL 10KM "HDA3" SFP. If D-port test fails then exit by: portdisable <port>; portcfgdport --disable <port>; portenable <port> to resume production traffic without any impact.		
Recovery:	Upgrade to a FOS release version with this defect fix which bypasses electric and optical loopback test to avoid D-port test reporting failure.		

Defect ID:	FOS-659181	**Technical Severity:**	Medium
Reason Code:	Implemented	**Probability:**	Low

Product:	Fabric OS	**Technology Group:**	Other
Reported In Release:	FOS8.0.2c	**Technology:**	Other
Symptom:	One case where running CLI command switchbeacon resulted in a CP panic and hafailover		
Condition:	This only happened once on a customer switch when running switchbeacon on the active CP.		

Defect ID:	FOS-658454	**Technical Severity:**	Medium
Reason Code:	Accepted	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.1.2a	**Technology:**	MAPS - Monitoring and Alerting Policy Suite
Symptom:	RoR in MAPS accepts invalid threshold by allowing values greater than 999999999		
Condition:	Its applicable only for RoR rules in MAPS.		

Defect ID:	FOS-657964	**Technical Severity:**	High
Reason Code:	Accepted	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS7.4.1d	**Technology:**	High Availability
Symptom:	Brocade 7840 may reboot unexpectedly with "Detected termination of process fcpd:####"		
Condition:	This is a rare occurrence resulting from the use of a shared memory segment that was deleted.		

Defect ID:	FOS-657908	**Technical Severity:**	High
Reason Code:	Will Not Fix	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Other
Reported In	FOS8.1.0_LNX	**Technology:**	Other

Release:			
Symptom:	Target is lost when one of the N-ports is disabled between Access Gateway and uplink switch.		
Condition:	Disable trunk member between Access Gateway and uplink switch.		

Defect ID:	FOS-655814	**Technical Severity:**	High
Reason Code:	Information Provided	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.0	**Technology:**	Virtual Fabrics
Symptom:	User may see a panic when attempting to power off any blade while POST is running on a core blade.		
Condition:	POST running on a X6-8 or X6-4 core blade makes frequent access of ASICs on all other blades in the system. Powering off one of these other blades during an ASIC access will cause a panic.		
Workaround:	Do not do anything that would cause a slot to power off if POST is running on a core blade.		

Defect ID:	FOS-655634	**Technical Severity:**	High
Reason Code:	Already Fixed in Release	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.0	**Technology:**	Configuration Fundamentals
Symptom:	Security transaction in a non-primary FCS switch get deadlocked when another non-primary FCS switch in fabric has DCC policies not present in the FCS switch.		
Condition:	Happens when non-primary FCS switch in fabric has DCC policies not present in the FCS switch and fabwide DCC is in tolerant mode.		
Workaround:	Make the switch with additional policies as FCS primary using "secpolicyfcsmove" and remove the unwanted policies. Do hafailover on the affected switch.		
Recovery:	Make the switch with additional policies as FCS primary using "secpolicyfcsmove" and remove the unwanted policies. Do hafailover on the affected switch.		

Defect ID:	FOS-655223	**Technical Severity:**	Medium
Reason Code:	Implemented	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.2.0	**Technology:**	RAS - Reliability, Availability, and Serviceability
Symptom:	incorrect RASLOG message regarding firmware version in below example. Fabric OS should be changed to AMP OS. "2 13:33:25, [SULB-1036], 49, CHASSIS, INFO, BrocadeAMP, The new Version: Fabric OS v2.2.0_bld44"		
Condition:	none		

Defect ID:	FOS-655190	**Technical Severity:**	Medium
Reason Code:	Already Fixed in Release	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Security
Reported In Release:	FOS8.2.0	**Technology:**	Encryption
Symptom:	Firmware download to FOS8.0.x is allowed with inflight encryption configured. FOS8.0.x doesn't support inflight encryption and hence ports configured with encryption will be disabled		
Condition:	Firmwaredownload to FOS8.0.x with inflight encryption configured.		
Workaround:	Disable inflight encryption before firmwaredownload to FOS8.0.x		
Recovery:	Disable inflight encryption and enable the port		

Defect ID:	FOS-653651	**Technical Severity:**	Medium
Reason Code:	Implemented	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.1.0b	**Technology:**	SNMP - Simple Network Management Protocol

Symptom:	User may encounter a very slow response to the CLI command snmpbulkwalk.
Condition:	This may occur when attempting snmpbulkwalk of ifdec table.

Defect ID:	FOS-653188	**Technical Severity:**	High
Reason Code:	In Progress	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.2.0	**Technology:**	Flow Vision
Symptom:	SCSI frametypes SCSI, SCSIGoodStatus, SCSITur and SCSXferrdy inadvertently works on NVMe traffic.		
Condition:	The issue is because NVMe over FC standard reused the FC-4 type 0x08 used by FCP -SCSI.		

Defect ID:	FOS-650414	**Technical Severity:**	Medium
Reason Code:	Not Reproducible	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.0	**Technology:**	Fibre Channel Services
Symptom:	In a backbone-to-edge routed fabric configuration, FC ping from a backbone switch to a device in the edge fabric fails.		
Condition:	In a backbone-to-edge routed fabric configuration, if there is a VE-VE or VEX-VE tunnel along the path to the edge fabric, FC ping from a backbone switch to a device in the Edge fabric will fail.		

Defect ID:	FOS-644047	**Technical Severity:**	Medium
Reason Code:	Implemented	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.0	**Technology:**	Access Gateway
Symptom:	An F-Port on an AG is logging to the FC fabric and has requested FAPWWN. If the current N-Port of the F-Port is disabled during this process, the F-Port might not come up.		

Condition:	N-Port toggled during the F-Port login process which was requesting FAPWWN
Workaround:	Do not toggle the current N-Port of the F-Port which is logging in to the fabric
Recovery:	Toggle the F-Port which is stuck

Defect ID:	FOS-643776	**Technical Severity:**	Medium
Reason Code:	Implemented	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Security
Reported In Release:	FOS7.4.1d	**Technology:**	Security Policies
Symptom:	Switch running FOS v8.x panics when distributing password in a fabric with a mix of FOS versions FOS7.1 or lower and FOS v8.x		
Condition:	Run "distribute -p PWD fid<switch" command on a switch running FOS v7.1 or earlier to distribute password database to a switch running FOS v8.x. The switch running FOS v8.x will panic while processing data received from earlier revision FOS. Mixed fabric releases with FOS v7.2/7.3 and 8.0.1 or later are not impacted.		
Workaround:	Run the command from switches with the highest revision FOS, or upgrade the target/receiving switches to FOS v8.1.1a or later versions which has the fix.		

Defect ID:	FOS-537487	**Technical Severity:**	Low
Reason Code:	Accepted	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS7.4.0	**Technology:**	Management GUI
Symptom:	When the IP address is provided for specific logical switch context, the default switch context will be launched.		
Condition:	Launching WebTools for logical switch context which has IPFC and subnet mask address configured.		
Workaround:	Launch WebTools for the default switch context and navigate to specific logical switch context.		

10.4 Open Defects in FOS 8.2.1

Defect ID:	FOS-804745		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1	**Technology:**	Configuration Fundamentals
Symptom:	Ras Log [C3-1021]"Encryption Compression Block error" and IFL link will not come online when enabling ISL_RDY mode and Encryption on IFL links		
Condition:	An Ex-Port to E-Port link (IFL) will flap continuously, when both Encryption and ISL_RDY mode are enabled on the Ex-Port. The port will not come online.		
Workaround:	Use either ISL RDY mode or Encryption on a Ex-Port, but not both on the same port.		

Defect ID:	FOS-804694		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1	**Technology:**	Firmware upload/download
Symptom:	The standby CP firmware doesn't sync with the active CP firmware version when CPs have different firmware versions.		
Condition:	If Auto firmwaresync is set from active and firmwaredownload is performed on the standby CP, and when reboot/hafailover is issued, the firmwaresync will not be triggered.		
Workaround:	Issue the firmwaresync command manually if firmware sync is required.		
Recovery:	Issuing the firmwaresync manually will cause the firmware to be in sync with the active CP.		

Defect ID:	FOS-804650		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management

Reported In Release:	FOS8.2.1	**Technology:**	Virtual Fabrics
Symptom:	Software verify will be seen for each port that is attempted to be moved between partitions.		
Condition:	Issue observed when moving FC32-64 blades between Logical partitions.		
Recovery:	Software verify messages observed on console is harmless. The movement operation will complete without any side effects.		

Defect ID:	FOS-804616		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1	**Technology:**	CLI
Symptom:	Software VERIFY error when WWN based Persistent PID is configured		
Condition:	When there is a WWN based Persistent PID feature is configured on the switch,software VERIFY error maybe seen in the following cases: a. With no WWN entries bound with the PID and if a reboot/hareboot is issued on the switch b. Last bounded entry is attempted for removal using "wwnaddress --unbind"		
Workaround:	At least one WWN based Persistent PID entry could be bound to avoid the VERIFY		
Recovery:	The switch does not reboot. No recovery needed.		

Defect ID:	FOS-804296		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1	**Technology:**	Configuration Fundamentals
Symptom:	CLI command configdefault on a X6-8 and X6-4 chassis base switch, that has encrypted links, pass without warning the user to remove the encrypted links before the operation.		
Condition:	CLI command configdefault should be blocked when encrypted port is configured on FC32-48 blade, otherwise results in resource		

	unallocated error.
Workaround:	Remove the encryption configuration from the FC32-48 port before attempting the configdefault operation

Defect ID:	FOS-804224		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.2.1	**Technology:**	FCIP
Symptom:	Observed ESM-1101 during a SX6 blade slotpower off with one of the following: esm_cfg_sys.c:1586 esm_portcfg_clear() failed rc:176 esm_slot.c:1603 failed to release GE:10/ge2 rc:176 .		
Condition:	ESM-1101 event can occur during a slotpoweroff of an SX6 blade.		
Recovery:	These are warning messages and are self-recovering		

Defect ID:	FOS-804203		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Virtualization
Reported In Release:	FOS8.2.1	**Technology:**	Virtual Fabrics
Symptom:	System panic may occur, although rarely, while collecting supportsave on a GEN6 chassis systems		
Condition:	Supportsave collection operation may trigger the system panic		
Recovery:	System will reboot after panic to recover. Due to hafailover, the standby CP will take over as active CP and assist in the smooth operation of the system		

Defect ID:	FOS-804173		
Technical Severity:	Medium	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1	**Technology:**	SNMPv2, SNMPv3 & MIBs

Symptom:	SNMP trap, swDeviceStatusTrap, is generated with "Logout" reason code instead of “Login”.
Condition:	The issue is observed when the QSFP port connected to a device is enabled.

Defect ID:	FOS-804155		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.2.1	**Technology:**	Flow Vision
Symptom:	Non disruptive upgrade to 8.2.1 may fail on a chassis with sys_mon_all_vms monitoring flow.		
Condition:	Observed when non disruptive upgrade is issued on a chassis where sys_mon_all_vms monitoring flow is active.		
Workaround:	Deactivate sys_mon_all_vms before upgrade using "flow --deact sys_mon_all_vms" CLI and activate the predefined flow (flow --act sys_mon_all_vms) after upgrade is complete.		

Defect ID:	FOS-804131		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.2.1	**Technology:**	WAN Performance Analysis Tools
Symptom:	portcmd --wtool stop-all error message isn't clear that its only intended for Automated WAN Tool sessions.		
Condition:	When attempting to stop User WAN Tool sessions with portcmd --wtool stop -all command		
Workaround:	Use "portcmd --wtool <wt-id> stop" command to stop User WAN Tool sessions		

Defect ID:	FOS-804126		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management

Reported In Release:	FOS8.2.1	**Technology:**	CLI - Command Line Interface
Symptom:	GE speed mismatch between 'switchshow' output and 'portcfgge --show' output. Also unable to change port speed to 1G or issue 'portcfgdefault'. Configuration replay errors seen during switch bootup and if the port is configured as a LAN 10G port, it may come up as a WAN port after a reboot		
Condition:	On 7810, if GE port speed is set to 10G on any GE port and reboot is performed after a time based license has expired		
Workaround:	Install a valid license prior to rebooting the switch.		
Recovery:	Install a new valid license, which is not expired, and reboot the switch. Alternatively the port can be recovered by disabling / enabling autonegotiation using 'portcfgge <ge-port> --disable -autoneg' followed by 'portcfgge <ge-port> --enable -autoneg'.		

Defect ID:	FOS-804124		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.2.1	**Technology:**	WAN Performance Analysis Tools
Symptom:	Unable to enable a WAN Tool session		
Condition:	When configured WAN Tool sessions exceed the supported limits, while all sessions are in a disabled state, results in the inability to enable WAN Tool session in this state.		
Workaround:	Keep the number of configured WAN Tool sessions for a DP within the supported limit.		
Recovery:	Delete WAN Tool sessions on a DP to within the supported amount. Then attempt to enable the session in question.		

Defect ID:	FOS-804103		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.2.1	**Technology:**	Flow Vision
Symptom:	Failure to remove SIM port blocks attempt to remove expired flow		

	vision license.
Condition:	This symptom is observed only when flow generator flow is active.
Workaround:	Remove SIM port using "flow --ctrlcfg simport -disable".
Recovery:	Remove SIM port using "flow --ctrlcfg simport -disable".

Defect ID:	FOS-804072		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1	**Technology:**	Management GUI
Symptom:	WebTools displays incorrect property members for peerzones		
Condition:	When peerzone is empty after removing peerzone alias using WebTools		
Workaround:	Ensure that the peerzone is not empty after removing the alias. The issue does not occur if member exist in the peer zone after alias removal.		

Defect ID:	FOS-804069		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1	**Technology:**	Software Installation & Upgrade
Symptom:	System-description attribute of "lldp --show" command incorrectly displays FOS 8.2.1 version.		
Condition:	Issue may be observed after non-disruptive downgrade from FOS v8.2.1 to v8.2.0 firmware version.		
Workaround:	Before firmware downgrade, system-description attribute can be modified to display correct firmware version using "lldp --config -sysdesc <string>" command.		
Recovery:	After firmware downgrade, system-description attribute can be modified to display correct firmware version using "lldp --config -sysdesc <string>" command		

Defect ID:	FOS-803937		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1	**Technology:**	Virtual Fabrics
Symptom:	fosexec issued with "lscfg --show" command for all switches in the fabric may not return output for for some domains.		
Condition:	Remote domain may return NULL response in somecases, which can go undetected at the sender's end, resulting in no output for remote fosexec.		
Recovery:	Login in to each of the domains and issue "lscfg --show" command to collect the data.		

Defect ID:	FOS-803919		
Technical Severity:	High	**Probability:**	null
Product:	Fabric OS	**Technology Group:**	Other
Reported In Release:	FOS8.2.1	**Technology:**	Other
Symptom:	Invalid SFP when a 16G or 32G SFP is inserted into a FC-32-48 blade		
Condition:	When a FC32-48 blade is inserted in a slot the previously held a FC32-64 blade and Ethernet ports were configured.		
Recovery:	Disable the port, change the port configuration from Ethernet to FC type and reenable the port.		

Defect ID:	FOS-803902		
Technical Severity:	High	**Probability:**	null
Product:	Fabric OS	**Technology Group:**	Other
Reported In Release:	FOS8.2.1	**Technology:**	Other
Symptom:	Active CP panic on an X6 chassis, with SX6 extension blade, that is an FCR core switch		
Condition:	In extremely rare cases, the CP panic may be seen due to a race condition in the switch		

Defect ID:	FOS-803885		
Technical Severity:	Medium	**Probability:**	null
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.2.1	**Technology:**	Extended Fabrics
Symptom:	Removing the IP from a circuit that has SLA returns error for the wtool and can leave the circuit in a out-of-sync state, which may cause future modifications to fail.		
Condition:	Removing a local-ip address or remote-ip address from a circuit that also has an SLA configured.		
Workaround:	Remove the SLA from the circuit first, then remove the IP address.		

Defect ID:	FOS-803879		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	System
Reported In Release:	FOS8.2.1	**Technology:**	CLI
Symptom:	Firmwareshow and SupportSave commands may take a long time to complete. Firmwaredownload may abort from timeout		
Condition:	The issue is observed when invalid DNS servers are configured on the switch.		
Workaround:	Update DNS configuration with proper entries.		
Recovery:	Update DNS configuration with proper entries.		

Defect ID:	FOS-803873		
Technical Severity:	High	**Probability:**	null
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1	**Technology:**	Firmware upload/download
Symptom:	On 7840 observed "BCM_CHIP_ATTACH failed" and FSS error during non-disruptive migration		

Condition:	Issue is seen when ambient temperature is greater than or equal to 50C, which is outside of the operating temperature specification (0-40C).
Workaround:	Keep the 7840 extension switch in ambient temperature range of 0-40C.

Defect ID:	FOS-803805		
Technical Severity:	High	**Probability:**	null
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1	**Technology:**	Configuration Fundamentals
Symptom:	REST GET on /brocade-interface/fibrechannel/name/{name}/max-speed reports incorrect value for 10G FC ports.		
Condition:	The corresponding CLI operation "ptstasshow" is not correct and doesn't match the REST operation, which is correct.		

Defect ID:	FOS-803717		
Technical Severity:	Medium	**Probability:**	null
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1	**Technology:**	Web Tools
Symptom:	"FC Routing service is in the process of being disabled" on 7810 for a long period of time after FCR-mode is disabled from Webtools.		
Condition:	When attempting to disable FCR on 7810 extension switch using WebTools		
Recovery:	Re-initiate Webtools session to the 7810 switch		

Defect ID:	FOS-803705		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS8.1.0	**Technology:**	Port Bring-up

Symptom:	For the New CLI Command PortcfgCleanAddress (that can configure on a port-by-port basis to enable Clean Address Bit) Configuration is disabled by default.
Condition:	If the Clean Address Bit configuration is enabled for the port, then the FLOGI response on this port shall always have the "Clean Address Bit" set.
Workaround:	Do not use the new CLI without vendor guidance. Please contact Technical Support first when the setting is desired.
Recovery:	Do not use the new CLI without vendor guidance. Please contact Technical Support first when the setting is desired.

Defect ID:	FOS-803556		
Technical Severity:	High	**Probability:**	null
Product:	Fabric OS	**Technology Group:**	Other
Reported In Release:	FOS8.2.1	**Technology:**	Other
Symptom:	fcRouting configs such as fcRoute.Xlate and PersistXD configs are not be restored to the Base FID of the X6-8 chassis using the config-file via Brocade Network Advisor		
Condition:	The fcRouting entries of logical switch base FID 127 are not backed-up by the BNA Configuration File utility		
Workaround:	Use BNA "configupload -all" type of function to upload Base switch fcRouting entries		

Defect ID:	FOS-803259		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.2.1	**Technology:**	FCIP - Fibre Channel over IP
Symptom:	During the config replay portion of hafailover / HCL indicating that an error has occurred displays [ESM-1101], ERROR, esm_ha.c:8289 esm_ipaddr_add() failed (rc:25)		
Condition:	When a switch is in the middle of a warm recovery (such as a ha reboot) and a slot is power cycled, the configuration may not be replayed or pushed to the slot. This will leave the slot in a state where it may have an incomplete or no configuration.		

Workaround:	Do not attempt to power cycle a blade during any kind of CP boot operation. This includes removing and reinstalling the blade.
Recovery:	An additional power cycle of the slot in question will recover the configs.

Defect ID:	FOS-803194		
Technical Severity:	Medium	**Probability:**	null
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.2.1	**Technology:**	MAPS - Monitoring and Alerting Policy Suite
Symptom:	100GE (25x4) QSFP in the FC32-64 blade does not report correct Tx Power and leads to violations reported by MAPS		
Condition:	When Ethernet QSFPs are present in the FC32-64 blade		
Workaround:	Turn off SFP monitoring in MAPS for QSFPs		

Defect ID:	FOS-803118		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.2.1	**Technology:**	Flow Vision
Symptom:	Learning flow to monitor all the egress traffic on an AG F port does not report stats. Static flow creation to monitor egress traffic on AG F port fails.		
Condition:	Issue is seen when flow monitor is defined on AG F port to discover all egress traffic.		
Workaround:	Monitoring of egress traffic on an AG F port is not supported. User can monitor the ingress traffic on the AG F port (e.g. flow --create flow_name --srcdev "*" -ingr F port).		

Defect ID:	FOS-802934		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management

Reported In Release:	FOS8.1.1a	**Technology:**	Ethernet Interface
Symptom:	Switch becomes inaccessible when the broadcast IP address is configured as gateway address.		
Condition:	Occurs only when brodcast IP is configured as Gateway address.		
Recovery:	1. Log in via console as root and execute "route add default gw x.x.x.x" command to temporarily set the default gateway to the correct address. This will temporarily allow for remote access to the switch via IP address. 2. If the current IP address and subnet mask need to be changed, use command "ifconfig eth0 x.x.x.x netmask x.x.x.x" 3. Contact Technical support to clear the incorrect gateway in WWN card 4. After the incorrect gateway address in WWN card is fixed, then reboot the switch to bring back ipadm		

Defect ID:	FOS-802896		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.2.1	**Technology:**	Flow Vision
Symptom:	Non disruptive firmware upgrade to FOS v8.2.1 may fail on a chassis with sys_mon_all_vms monitoring flow.		
Condition:	When non disruptive upgrade is issued on a chassis where sys_mon_all_vms monitoring flow is active.		
Workaround:	Deactivate sys_mon_all_vms before upgrade using "flow --deact sys_mon_all_vms" CLI and activate the predefined flow "flow --act sys_mon_all_vms" after upgrade is complete.		

Defect ID:	FOS-802447		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.2.1	**Technology:**	Flow Vision
Symptom:	Flow monitored on a VE port does not report stats after the destination device transitions to online state.		
Condition:	Issue is observed when flow monitoring is enforced on the VE port using the WWN of the destination device.		

Workaround:	Deactivate and activate the flow that is monitored on VE port. E.G: flow --deactivate <flow_name>;flow --activate <flow_name>

Defect ID:	FOS-802299		
Technical Severity:	Medium	**Probability:**	null
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1	**Technology:**	Web Tools
Symptom:	WebTools slow performance in sub-tabs of FC Router GUI		
Condition:	When there are 1000 or more LSAN devices connected and there are a large number of LSAN Zones and LSAN fabrics		

Defect ID:	FOS-801447		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Other
Reported In Release:	FOS8.2.1	**Technology:**	Other
Symptom:	Error message "esm_cfg_ipsec.c:7889 IPSec: mkdir /mnt/etc/fabos/certs/extn/ rc=-1 errno=2" may be displayed on console.		
Condition:	The message may be observed during non-disruptive firmwaredownload operation on 7840.		

Defect ID:	FOS-801392		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.1.2a	**Technology:**	CLI - Command Line Interface
Symptom:	The aaaconfig command used to be non-interactive in FOS versions prior to FOS v8.x.x		
Condition:	Running CLI aaaconfig with -e option, it still prompts user with “Encryption type is currently set to none. Do you want to set encryption type to aes256? (y/n)”.		

Defect ID:	FOS-801128		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.2.1	**Technology:**	APM - Advanced Performance Monitoring
Symptom:	Portperfshow command may display throughput greater than the port speed.		
Condition:	The issue is observed when the port is running at almost full bandwidth.		
Recovery:	Corrected values will be updated during the next portpershow display cycle.		

Defect ID:	FOS-800557		
Technical Severity:	Medium	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1	**Technology:**	IPv6 Addressing
Symptom:	User authentication may fail with RADIUS configured as primary AAA server.		
Condition:	The symptom is observed when DHCPv6 is enabled and stateless IPv6 autoconfiguration is disabled on the switch.		

Defect ID:	FOS-800512		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1	**Technology:**	Management GUI
Symptom:	In BNA / Spectre, standby CP's firmware version details are shown as 'NULL'.		
Condition:	After firmware upgrade and reboot		

Defect ID:	FOS-800300		
Technical Severity:	High	**Probability:**	null
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1	**Technology:**	CLI - Command Line Interface
Symptom:	spinfab fails on G630 E-ports		
Condition:	After running offline diag tests on G630, spinfab tests may fail or frames may drop.		
Workaround:	Reboot the G630 after running offline Diag test (Plb, turboramtest , portledtest and systemverification).		
Recovery:	Reboot the switch.		

Defect ID:	FOS-660483		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.1.2a	**Technology:**	High Availability
Symptom:	Customer may experience that a port bounce results in loss of sync		
Condition:	This may be encountered on a switch with FMS mode enabled and there is device performing PLOGIN with invalid SID.		

Defect ID:	FOS-658940		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS7.2.1_HIL3	**Technology:**	Fibre Channel Services
Symptom:	Devices connected to an Access Gateway can be inadvertently logged out and not function normally.		
Condition:	This occurs when a misbehaving device tries to abort an exchange that is already closed.		
Recovery:	Try to bounce the port; This may not always work.		

Defect ID:	FOS-656244		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.0	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	For a configured F-port trunk, snmpwalk query for 'swFCPortName' 'swFCPortSpecifier' SNMP objects number of entries returned will be one extra compared to number of physical ports present in that logical context. Similarly when the XISL is enabled and snmpwalk query for 'swFCPortSpecifier' object returns an extra entry.		
Condition:	F-Port trunk or XISL feature configured and enabled on the switch.		

Defect ID:	FOS-655807		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.0.2a	**Technology:**	Hardware Monitoring
Symptom:	"LED" from the "portflagsshow" output is gone when the port is disabled then re-enabled.		
Condition:	This would happen only for offline ports.		

Defect ID:	FOS-655799		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.2.0	**Technology:**	Flow Vision
Symptom:	If 'flow --reset' isn't performed on a logical switch, before deleting the logical switch (FID), the old flows (belonging to the deleted logical switch) will not be reset.		
Condition:	A logical switch (FID) is deleted, but 'flow --reset' operation isn't performed before deleting the logical switch.		
Workaround:	Reset the flows before deleting a logical switch		

Defect ID:	FOS-654083		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Security
Reported In Release:	FOS8.2.0	**Technology:**	Security Policies
Symptom:	When multiple back to back password distribution is performed on a fabric with large number of Access Gateway switches connected, the transaction doesn't complete in an Access Gateway switch and further transactions are not allowed for the Access Gateway switch.		
Condition:	Multiple back to back password distribution on a fabric with large number of Access Gateway switches.		

Defect ID:	FOS-646323		
Technical Severity:	Medium	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.1.0b	**Technology:**	CLI - Command Line Interface
Symptom:	CLI command "portshow 0" reflect "FAA" as inactive, even when FAA is enabled for the port.		
Condition:	This is a cosmetic discrepancy, that appears in the output of only "portshow 0", with no functional impact.		

Defect ID:	FOS-644856		
Technical Severity:	Medium	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.1.0b	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	The parameters like mul, AvgPT, maxPT set with the snmpstatistics command are lost when rebooting.		
Condition:	Applicable for all FOS products		
Recovery:	Re-configure the values after reboot.		

Revision History

FOS-821a-RN101; October 29, 2018

- Updated **What's New in FOS 8.2.1a** section on Brocade G620 with new memory chip support.
- Added list of CVEs addressed in FOS 8.2.1 to **What's New in FOS 8.2.1** section.
- Style edits.
- Added FOS-803782 to the Closed with Code in Fabric OS 8.2.1 defect table.

FOS-821a-RN100; October 17, 2018

Initial document version.


BROCADE
A Broadcom Inc. Company