Fabric OS® v9.2.1

Fabric OS v9.2.1 Release Notes Digest

Version 4.0

Table of Contents

Chapter 1: Preface

1.1 Contacting Technical Support for your Brocade® Product

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

Online	Telephone
For nonurgent issues, the preferred method is to log on to the Support portal at support.broadcom.com. (You must initially register to gain access to the Support portal.) Once registered, log on and then select **Brocade Products**. You can now navigate to the following sites: ▪ **Case Management** ▪ **Software Downloads** ▪ **Licensing** ▪ **SAN Reports** ▪ **Brocade Support Link** ▪ **Training & Education**	For Severity 1 (critical) issues, call Brocade Fibre Channel Networking Global Support at one of the phone numbers listed at www.broadcom.com/support/fibre-channel-networking/contact-brocade-support.

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

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

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

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

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 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.

- 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 G630, G620, G610, G720, and G730 – On the switch ID pull-out tab located on the bottom of the port side of the switch.
  - Brocade 7810 and 7850 – 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 as well as on the left side underneath (looking from the front).
  - Brocade X6-8, X6-4, X7-8, and X7-4 – Lower portion of the chassis on the non-port side beneath the fan assemblies.

- 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.

- License Identifier (License ID).

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

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

1.2 Related Documentation

White papers, data sheets are available at www.broadcom.com. Product documentation for all supported releases is available on the support portal to registered users. Registered users can also find release notes on the support portal.

Chapter 2: Locating Product Manuals and Release Notes

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

2.1 Locating Product Manuals and Release Notes

2.1.1 Locating Product Manuals on Broadcom

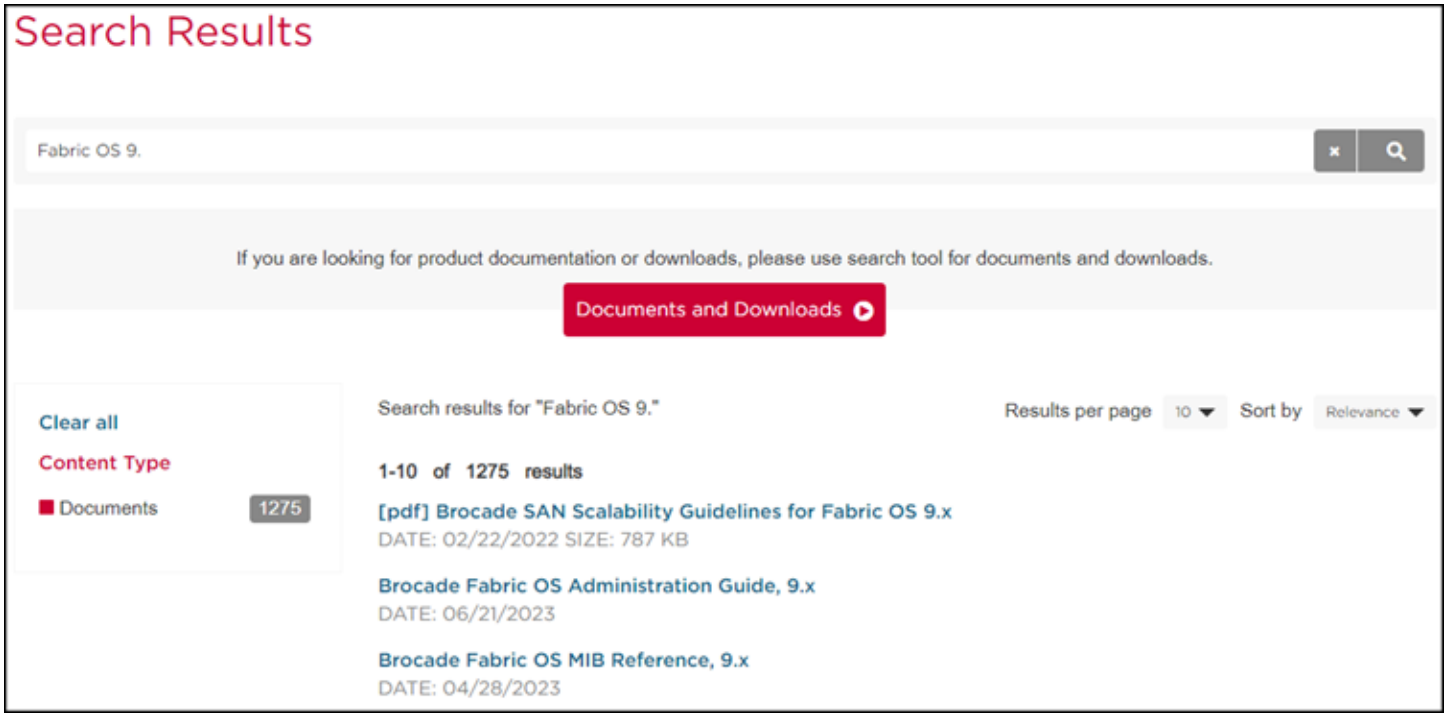
Complete the following steps to locate your product manuals on Broadcom.com.

1. Go to www.broadcom.com.
2. Enter the product name or the software version number in the **Search** box.

   For example, the following search is for software and documentation files for software version 9.

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

   The list of documents available for the release displays.



2.1.2 Locating Product Manuals and Release Notes on the Support Portal

Complete the following steps to locate your product manuals on the support portal.

1. Go to support.broadcom.com, click **Login**, and enter your username and password.

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

2. Select **Brocade Storage Networking** in the support portal.

2.2 Document Feedback

Quality is our first concern and we have made every effort to ensure the accuracy and completeness of this document. If you find an error, omission or 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

The Fabric OS v9.2.1 is a maintenance release based on FOS v9.2.0a.

This release supports all hardware platforms and features in FOS v9.2.0a.

Fabric OS v9.2.1 includes software enhancements and defect fixes for FOS v9.2.0 and FOS v9.2.0a.

Fabric OS v9.2.1 is the initial release supporting Unified Storage Fabric (USF) on the X7-4/8, which includes support for AnyIO ports on the FC64-48 port blade as well as universal properties for the existing 64G SFP (XBR-000462).

Chapter 4: What's New in FOS 9.2.1

The Fabric OS v9.2.1 release includes new software features and enhancements of existing, with the main areas listed below and covered in more detail in the respective sections and chapters.

4.1 Hardware

Fabric OS v9.2.1 does not include new hardware.

The following new capabilities are added to the existing hardware with FOS v9.2.1:

- Brocade X7-4/8 supports USF.
- Brocade FC64-48 port blade supports 24 AnyIO ports. AnyIO ports can be configured as either FC or Ethernet ports.
- Brocade 64G SWL SFP support universal properties (64G SWL SFP support either FC or Ethernet per the configured port).

4.1.1 Platforms

In addition to the new hardware capabilities, FOS v9.2.1 also supports the same Brocade Gen 6 and Gen 7 Fibre Channel platforms supported in FOS v9.2.0x.

4.2 New and Modified Software Features

- System Security
  - Federated Authentication (FA)
- MAPS and Fabric Performance Impact
  - MAPS Groups
  - SFP Monitoring
  - IP Storage Ethernet ports monitoring
  - FPI monitoring for IP Storage
  - Certificate monitoring
  - Switch memory monitoring
- Traffic Optimizer (TO)
  - IP Storage support
- Unified Storage Fabric (USF)
  - IP Storage logical switch and logical fabric
  - IP Storage diagnostics
  - SNMP MIBS for IP Storage
  - sFlow
- Fabric Infrastructure
  - ipsPacketDump (Firmware patch)

- Miscellaneous
  - Flow Vision Scale
  - D-Port on EX-Port
  - Link Latency Determination (LLD)
  - Time Zone configuration
- Web Tools
  - Display of USF components
  - Port investigation
  - Zoning enhancement
- REST API
  - RDP-polling-cycle

4.2.1 System Security Enhancements

Fabric OS System Security provides functionalities such as User Management, Cryptography Management, Certificate Management, Firewall (IP Filter) and other miscellaneous features. Role Based Access Control (RBAC), Authenticated access to the switch, Fabric, and management interface (Ethernet) modules ensure that the integrity of the switch is upheld in terms of access, authentication, and handling vulnerabilities.

4.2.1.1 Federated Authentication

FOS supports password-based and password-less authentication mechanisms. In password-based authentication, the FOS switch accepts the credential in plaintext and parses before they are validated (locally with switch local user database or on an external AAA server such as LDAP, RADIUS, TACACS+ or RSA authentication servers).

With FOS v9.2.1 Federated Authentication (FA) support is added.

In Federated Authentication, authentication is performed by an Identity Provider (IDP) that manages identities of users, including the user's multiple configured factors for multi factor authentication (MFA).

With Federated Authentication mode set in FOS the access is permitted when the user or application attempts login to the FOS switch using a valid access token issued by the IDP configured (and trusted) by the FOS switch.

The authentication flow is different for interactive users and applications.

Users successfully authenticate themselves with the IDP using a redirect URL and code provided by switch (CLI interactive logins via SSH only).

Applications that login to FOS (automation scripts using REST API, SANnav and ASC-G), require the client applications to setup PKI certificates (public key) with the IDP as part of application registration before attempting logins to the FOS switch. This enables applications to login to FOS without interactively providing credentials to the IDP during the login process.

The ID/Access tokens used by FOS are JWT format tokens. FOS can either fetch IDP public keys or these can be imported by the customer to perform token validations. All clients that connect to the IDP for federated authentication, must be registered with IDP.

NOTE In FOS v9.2.1 Microsoft Entra ID (previously called MS Azure AD) is the only supported IDP.

For new and updated commands and more details on how to configure Federated Authentication, refer to the *Fabric OS Administration Guide 9.2x.*

4.2.1.1.1 Fabric OS Compatibility

All FA configurations must be removed prior to downgrade below FOS v9.2.1.

4.2.2 MAPS and Fabric Performance Impact (FPI) Enhancements

In FOS v9.2.1 MAPS is enhanced to support USF. The logical port groups in the IPS logical switch are enhanced to allow users to use the existing MAPS features and apply them on Ethernet ports.

In addition, new groups are provided to provide the flexibility to monitor FC and Ethernet specific features independently.

FOS v9.2.1 supports the following MAPS and FPI enhancements:

- MAPS Groups
- SFP Monitoring
- IP Storage Ethernet ports monitoring
- FPI monitoring for IP Storage
- Certificate monitoring
- Switch memory monitoring

4.2.2.1 MAPS Groups

The following MAPS groups changes are applied in FOS v9.2.1.

4.2.2.1.1 ALL_PORTS

To simplify the MAPS configuration and management the MAPS logical group ALL_PORTS is enhanced to contain both FC and Ethernet ports from IPS LS (in older FOS versions, ALL_PORTS group contains only FC ports). In addition, the user-defined groups can be created using both FC and Ethernet ports. This allows the users to create common rules to monitor FC and Ethernet ports.

Example:

```
Switch101:FID1:admin> switchshow
LS Attributes: [FID: 1, Switch Type: IP Storage Switch, Address Mode 0]
Index Slot Port Address Media Speed State Proto
==================================================
8 3 8 2d0800 -- N64 Online FC E-Port 10:00:00:27:f8:f1:4b:a0 "Switch201"
(downstream)(Trunk master)
9 3 9 2d0900 -- 10G Online ETH

Switch101:FID1:admin> logicalgroup --show ALL_PORTS
Group Name     |Predefined |Type |Member Count |Members
ALL_PORTS      |Yes        |Port |2            |3/8-9
```

4.2.2.1.2 SFP_STATE Monitoring

This enhancement to the ALL_PORTS logical group has the following impacts on the existing FCoE ports (Ethernet) monitoring.

Prior to FOS v9.2.1, SFP_STATE is being monitored using ALL_ETH_PORTS group. The group contains the Ethernet ports and primarily is being used to monitor the SFP state.

From FOS v9.2.1 the existing rules that monitor SFP_STATE using ALL_PORTS are sufficient to monitor both Ethernet and FC.

- ALL_PORTS(SFP_STATE/NONE == FAULTY)
- ALL_PORTS(SFP_STATE/NONE == OUT)
- ALL_PORTS(SFP_STATE/NONE == IN)

Consequently, the following rules are deprecated and removed from the active policy:

- ALL_ETH_PORTS(SFP_STATE/NONE == FAULTY)
- ALL_ETH_PORTS(SFP_STATE/NONE == OUT)
- ALL_ETH_PORTS(SFP_STATE/NONE == IN)

The above rules are present in the rules database in FOS v9.2.1 to support backward compatibility.

Since these rules are no longer associated with any of the default policies in FOS, these rules will be obsoleted in a future release.

4.2.2.1.3 ALL_FC_PORTS

A new logical group called ALL_FC_PORTS is introduced to include only FC ports (both online and offline ports).

The new group is present in all LSs and it is a subset of ALL_PORTS.

Example:

```
Switch101:FID1:admin> switchshow
LS Attributes: [FID: 1, Switch Type: IP Storage Switch, Address Mode 0]
Index Slot Port Address Media Speed State Proto
==================================================
8 3 8 2d0800 -- N64 Online FC E-Port 10:00:00:27:f8:f1:4b:a0 "Switch201"
(downstream)(Trunk master)
9 3 9 2d0900 -- 10G Online ETH

Switch101:FID1:FID1:admin> logicalgroup --show ALL_FC_PORTS
|Predefined    |Type |Member Count |Members
|Yes           |Port |1            |3/8
```

NOTE It is not supported to manually add/remove ports from the MAPS groups ALL_FC_PORTS and ALL_ETH_PORTS.

4.2.2.1.4 ALL_ETH_PORTS

The logical group ALL_ETH_PORTS include only Ethernet ports (both online and offline ports). The group is present in all LSs and it is a subset of ALL_PORTS.

Example:

```
Switch101:FID1:admin> switchshow
LS Attributes: [FID: 1, Switch Type: IP Storage Switch, Address Mode 0]
Index Slot Port Address Media Speed State Proto
==================================================
8 3 8 2d0800 -- N64 Online FC E-Port 10:00:00:27:f8:f1:4b:a0 "Switch201"
(downstream)(Trunk master) 9 3 9 2d0900 -- 10G Online ETH

Switch101:FID1:admin> logicalgroup --show ALL_ETH_PORTS
Group Name     |Predefined |Type |Member Count |Members
ALL_ETH_PORTS  |Yes        |Port |1            |3/9
```

4.2.2.1.5 ALL_LAGS

A new logical group called ALL_LAGS is introduced to include online LAGS. The new group is present in IPS LS.

NOTE Manual addition/removal of ports from the ALL_LAGS group is not supported.

4.2.2.2 IP Storage Ethernet Ports Monitoring

Monitoring of IPS LS Ethernet ports includes error and performance stats for the ports. The following metrics are monitored on Ethernet ports:

- Cyclic redundancy check errors (CRC)
- Invalid transmission words (ITW)
- Loss of signal (LOSS_SIGNAL)
- State change (STATE_CHG)
- Port bandwidth of Incoming traffic (RX)
- Port bandwidth of outgoing traffic (TX)
- Port bandwidth utilization (UTIL)

The above monitoring systems are already supported for FC ports and are used to monitor the Ethernet ports.

Each of the above monitoring systems supports basic elements of the MAPS timebase, actions (such as FENCE, RASLOG, EMAIL and SNMP), ROR, etc. and rules can be defined.

Example:

```
defALL_ETH_PORTSCRC_0 ALL_ETH_PORTS(CRC/MIN>0) RASLOG
```

The above default rule monitors number of CRC errors per minute and sends a RASLOG alert if any port exceeds the threshold.

Alert example:

```
[MAPS-1003], WARNING, x7-8,ETH-Port 1, Condition=ALL_ETH_PORTS(CRC/min>0), Current
Value:[CRC, 10 CRCs], RuleName=defALL_E_PORTSCRC_0, Dashboard Category=Port Health
```

In FOS v9.2.1 the following metrics are monitored LAG ports (ALL_LAGS):

- Port bandwidth of Incoming traffic (RX)
- Port bandwidth of outgoing traffic (TX)
- Port bandwidth utilization (UTIL)

NOTE MAPS monitors the LAG throughput through the ALL_LAGS group only.

4.2.2.3 Fabric Performance Impact (FPI) Monitoring for IP Storage

MAPS is enhanced to monitor port oversubscription (OS) for Ethernet ports by leveraging the existing basic elements of monitoring:

- ALL_PORTS group - contains Ethernet and FC ports
- PORT_BANDWIDTH monitoring system - monitoring system to monitor OS
- Default rules and actions

  Example of the default rule:

  ```
  defALL_PORTS_OVERSUBSCRIBED ALL_PORTS(PORT_BANDWIDTH/NONE==OVERSUBSCRIBED)
  ```

When the above default rule gets triggered an alert for oversubscription is generated.

Example:

```
[MAPS-1003], 167452, FID 128, WARNING, G19_Wed23_Cong_Init, Eth-Port 11/2,
Condition=ALL_PORTS(PORT_BANDWIDTH==OVERSUBSCRIBED), Current Value:[PORT_BANDWIDTH,
OVERSUBSCRIBED,(TX=99.9%) ], RuleName=defALL_PORTS_OVERSUBSCRIBED, Dashboard
Category=Fabric Performance Impact.
```

NOTE On LAGs the OS feature is monitored at individual ports and not at LAG level.

4.2.2.3.1 New/Modified/Deprecated Commands

The following commands and/or command output is modified in FOS v9.2.1

mapsSam

FOS CLI command `mapssam` is extended to include ETH ports as well.

Example:

```
Switch101:FID128:admin> mapssam --show

Port     Type  Total Up Time     Total Down Time   Down Occurrence   Total Offline Time
(Percent)            (Percent)         (Times)           (Percent)
=============================================================================================
0        U     0.00              0.00              0                 100.00
1        F     100.00            0.00              0                 0.00
2        E     100.00            0.00              0                 0.00
3        ETH   100.00            0.00              0                 0.00
```

portShow

The FOS CLI command `portShow` is enhanced to support Ethernet ports and display `portHealth`.

Example:

```
Switch101:FID128:admin> portshow 3
portIndex: 3
portName: port3
portHealth: HEALTHY
Authentication: None
portDisableReason: None
portCFlags: 0x1
```

mapsConfig

The FOS command `mapsConfig` pause/restart is enhanced to support pause/restart monitoring ETH ports.

Example:

```
Switch101:FID128:admin> switchshow
Index Port Address Media Speed State Proto
==================================================
33 33 022100 id N64 Online FC E-Port (Trunk port, master is Port 32 )
35 35 022300 id 10G Online ETH

Switch101:FID128:admin> mapsconfig --config pause -type port -members 35
2023/04/24-06:39:43 (GMT), [MAPS-1131], 6183, FID 128, INFO, switch_123, Monitoring on
members 35 of type PORT is paused.
```

NOTE In IPS LS, only actions which apply to E and ETH ports are valid. These are RASLOG, EMAIL, SNMP, FENCE and DECOM.

4.2.2.4 MAPS Certificate Monitoring

In FOS v9.2.1 MAPS is enhanced to monitor IDP server Certificates for validity and alert prior to expiry.

Once FA (IDP) server CA certificates are imported, MAPS starts monitoring the imported FA certificates.

This can be verified by executing the command `logicalgroup --show`

Example:

```
Switch101:FID128:admin> logicalgroup --show ALL_CERTS
Group Name     |Predefined |Type             |Member Count |Members
ALL_CERTS      |Yes        |Certificate      |4            |HTTPS SW Certificate, LDAP
Server CA Certificate,RADIUS Server CA Certificate,IDP Server CA Certificate
```

MAPS monitors days for expiry for each imported certificate (DAYS_TO_EXPIRE monitoring system) and the number of certificates which have already expired (EXPIRED_CERTS monitoring system).

In FOS v9.2.1 MAPS monitors these attributes for the imported IDP server CA certificates. MAPS supports monitoring of IDP chain certificates as well.

Existing rules for DAYS_TO_EXPIRE and EXPIRED_CERTS will monitor IDP server CA certificates. No new MAPS rules are added.

Example, MAPS RASLOG for IDP certificate Expiry:

```
2023/07/30-05:33:58 (GMT), [MAPS-1003], 180, FID 128, WARNING, sw0, IDP Server CA
Certificate,[Name:fa.pem SN:50CDE204A99CB018E3D978D58A1EE596DADB659A],
Condition=ALL_CERTS(DAYS_TO_EXPIRE/NONE<=90), Current Value:[DAYS_TO_EXPIRE, 30 days],
RuleName=days_rule, Dashboard Category=Security Violations, Quiet Time=None.
```

Below is the list of CERTS monitored by MAPS.

- HTTPS
- SYSLOG
- LDAP
- RADIUS
- FCAP
- ASC
- KAFKA
- EXTN SW
- EXTN CA
- RSA CA
- IDP CA

4.2.2.5 MAPS Switch Memory Monitoring

In FOS v9.2.0 MAPS was enhanced to monitor the physical as well as virtual memory using new default rules to monitor the memory.

In FOS v9.2.1 MAPS is enhanced to perform HA recover action automatically, when critically low free memory is detected on the switch. The HA failover operation for the chassis system and HA reboot for the fixed-form-factor switches, is performed when MAPS detects the system is running with critically low free memory available. The HA failover is performed to avoid the system otherwise going through a cold reboot.

NOTE When MAPS triggers HA recover due to critical low switch memory; the available memory on the switch is at a threshold where the switch would otherwise go through a cold reboot or become non-responsive.

Automatic HA action protects critical system functionality and acts with an explicit notification. MAPS ensures the system has enough resources to complete the operation gracefully.

Automatic HA recover action protects the system functionality without user intervention. Failure to act on time will result in a cold reboot or failover and could potentially impact traffic.

MAPS already monitors system memory usage continuously (since FOS v9.2.0). With FOS v9.2.1 a new MAPS Action `HA_RECOVER` is added to provide this functionality.

Example:

```
CHASSIS(MEMORY_USAGE_STATE/NONE==CRITICAL) HA_RECOVER, RASLOG
```

MAPS takes the HA action as soon as memory usage exceeds critical high thresholds, and the system is running below the low free memory threshold - in this case, the above rule triggers and results in HA failover/reboot preceded by a critical notification for the operational team: raslog, SNMP, email, and so on.

In case the MAPS's `HA_RECOVER` action fails, then MAPS generates a critical raslog and aborts the action. MAPS does not retry to do HA failover or reboot again.

Example of RASLOG:

```
[MAPS-1221], CRITICAL, sw0, HA_RECOVER action has failed
```

The MAPS `HA_RECOVER` action is configured and active by default after upgrade to FOS v9.2.1 and cannot be disabled.

Example:

```
Switch101:FID128:admin> mapsconfig --show
Configured Notifications:SW_CRITICAL,SW_MARGINAL,SFP_MARGINAL,FPIN,HA_RECOVER
admin> mapsconfig --actions none
```

MAPS uses the existing system rules, which cannot be deleted by the user.

- `CHASSIS(MEMORY_USAGE_STATE/NONE==CRITICAL) HA_RECOVER, RASLOG`
- `CHASSIS(MEMORY_USAGE_STATE/NONE==WARNING) RASLOG`

The customer can create custom rules to monitor the memory. If the customer has a rule to monitor critical memory usage, `HA_RECOVER` action will be taken regardless of whether the rule has the `HA_RECOVER` action. For example, the below custom rule (R1) will take the action even if the user does not configure the action.

Example:

```
mapsrule --create R1-mon MEMORY_USAGE_STATE -group CHASSIS -value CRITICAL -act raslog -
op eq -timebase none
```

In this case, the `HA_RECOVER` action will be configured by MAPS while being created by the user as follows:

R1: `CHASSIS(MEMORY_USAGE_STATE/NONE==CRITICAL) HA_RECOVER,RASLOG`

In case the custom rule (in this case, for example, R3) already exists prior to upgrading to FOS v9.2.1, then the

`HA_RECOVER` action will be enabled when the user upgrades the firmware:

R3: `CHASSIS(MEMORY_USAGE_STATE/NONE==CRITICAL) RASLOG,HA_RECOVER`

As soon as R3 triggers in FOS v9.2.1, the `HA_RECOVER` action will be taken.

Consecutive `HA_RECOVER` actions can only be performed every 60 minutes to avoid toggling the CPs. This means MAPS waits one hour and make sure system is up and running for an hour before taking second `HA_RECOVER` action.

1. ROR is not support in `MEMORY_USAGE_STATE` monitoring.
2. The existing default rule to monitor IN_RANGE (defCHASSISMEMORY_USAGE_STATE_IN_RANGE) is obsolete. If a custom rule is present prior to upgrade of FOS, the custom rule will be unmonitored.

4.2.3 Traffic Optimizer

In FOS v9.2.1 the active profile for IP storage traffic places all traffic in the default PG named PG_SYSTCDEFAULT. The IP profile configuration cannot be modified.

4.2.4 Unified Storage Fabric (USF)

Unified Storage Fabric (USF) is a new capability in FOS v9.2.1, enabling IP Storage (IPS) in parallel with FC on the fabric.

With Brocade USF the fabric is a dedicated network with integrated storage services for all types of storage, including Fibre Channel, FICON, iSCSI, NVMe/TCP, and NAS. Leveraging the performance, reliability and security of the SAN fabric while consolidating and simplifying management within the storage team. Providing investment protection for existing IP and FC networks and enhances the performance and reliability of IP storage.

4.2.4.1 Overview

USF isolates FC and IP Storage traffic on the same physical fabric through the provisioning of logical fabrics consisting of IPS logical switches, and AnyIO ports within a Brocade X7 Director. The Brocade X7 with the FC64-48 port blade (and 64G optics) enables AnyIO ports for either FC or IP connections, the universal SFP (PN: 57-1000495-01) automatically changes mode based on the port configuration for either FC or Ethernet.

Servers connecting to IP storage can be attached directly to the USF IP fabric, though more commonly the servers will be connected via a Top of Rack (ToR) data center network switch. With this architecture, the IP storage traffic is separated out of the data center network at the ToR switch connected to the USF IP fabric with redundant IP connections. The IP storage arrays are connected either directly or through a ToR to the USF IP fabric. With this solution design, IP storage leverages all the Brocade fabric services, centralized management, and the inherent dual fabric deployment of the Brocade SAN, providing redundancy and resiliency for IP storage services. It also enables unified provisioning and management for IP and FC storage from the storage team with minimal dependencies on the network team.

The USF IP storage fabric supports both block-based (iSCSI, NVMe/TCP etc.) storage and file-based (NFS, SMB, S3, Ceph, and so on) storage.

NOTE USF facilitates both FC and IP storage traffic in parallel while fully separated and isolation between the two protocols, there is no storage protocol translation between IP and FC.

4.2.4.2 USF Components

USF does not require a license and is available on FOS v9.2.1.

The IP Storage support consists of the following components:

Physical

- Switch types – X7-4 and X7-8
- Port blades – FC64-48
  - Ports – 16 to 23 and 32 to 47 are AnyIO ports
- SFP – 64G FC □ 25/10G Eth (PN: 57-1000495-01)
- Dedicated ISLs – Any ports available on the X7 directors connecting IP Logical Switches (ports are in FC mode)

Logical

- IPS LS – One IP Logical Switch can be provisioned per X7 director.
- VRF – Default VRF (id 0) is automatically created with the IPS (additional VRFs can be defined)
- VLAN – 3600 VLAN IDs are available for configuration.
- LAG – Link Aggregation is supported across interfaces in an IPS LS (max. 16 ports)
- MLAG – MLAGs are not supported on the FOS switches in this release.
  Connecting to MLAG TORs is supported.

4.2.4.3 USF-Supported Configurations and Scalability

The following supported configurations and scalability apply to Fabric OS v9.2.1.

In all cases these limitations are not enforced.

4.2.4.3.1 Supported Configurations

In FOS v9.2.1, the following deployment models are supported:

1. Host and Storage directly connected to the IPS Fabric in USF.
2. Host and Storage connected to ToR which is connected at layer 3 (L3 ToR) to the IPS fabric in USF.
3. Any combination of 1 and 2.

Consequently, it is not supported in FOS v9.2.1 to connect ToR at layer 2 (L2 ToR) to the IPS Fabric in USF

NOTE FOS v9.2.1 supports only lossy IP storage traffic.

4.2.4.3.2 Scalability Limits

In FOS v9.2.1, the following scalability is supported:

- One IPS LS per chassis
- 800 devices per IPS fabric in USF
- MTU size of 2k
- 48 LAGs per IPS LS
- 8 domains per IPS Logical Fabric
- 4 VRFs
- 256 VLANs
  - 16 VLANs per Interface
- 512 Static routes

4.2.4.4 IPS Provisioning

With FOS v9.2.1 IPS LS can be provisioned with the following steps (no license is required for USF):

- Create IPS LS on the director(s)
- Move ports to the IPS LS
- Configure AnyIO ports for Ethernet

NOTE In case the SFP firmware is not already updated to the universal SFP driver this must be done in a subsequent step with the command `sfpupgrade`.

- Add the (FC) ports for ISL (DISL) connections between the IPS LSs across the X7 directors (ICLs are also supported).

4.2.4.5 IP Storage Logical Switch

The IP Storage Logical Switch (IPS LS) is a (new) logical switch with IP Storage properties. In FOS v9.2.1 one IPS LS can be provisioned per chassis and the IPS LS domain id is persistent and must be unique across the fabric. The default LS cannot be configured as an IPS LS.

Only FC E-ports and IP storage ports (Ethernet ports connecting to host, target or a TOR) are allowed in the IPS LS. F-ports and Ex-ports ports are not allowed, and the IPS LS cannot utilize XISL ports.

The IPS LS is only supported on (native) X7 (not X6+) and can have ports from port-blades FC64-48, FC64-64 and CR blades (core routing blades). Ethernet ports are only supported on the FC64-48 port blade, while E-Ports ports are supported across all three blade types. No other port blades are supported.

On the FC64-48 port blade only ports ranging from 16 to 23 and 32 to 47 have AnyIO (flexport) capability. Only the 64G SFP has universal capability and is supported for Ethernet ports.

NOTE Ethernet ports in the IPS LS will need to be converted back to FC port type before transitioning out of the LS, in the case it is decided to remove ports from an IPS LS.

FCoE and FCR are not supported in IPS LS.

4.2.4.6 Universal SFP

The 64G SFP in the FC64-48 port-blade is universal SFP capable and changes protocol from FC (64G) to Ethernet (25/10G) when the port is configured to Ethernet. In case the SFP driver is down level the SFP driver must be upgraded with the command `sfpupgrade`.

Example:

```
IPS1:FID101:admin> sfpupgrade 4/47
[04/47  | SFP  |***]:Current MCU version     : 0x19           (latest: 0x1f)
[04/47  | SFP  |***]:Current DSP version     : 0xda0718       (latest: 0xda0c00)
[04/47  | SFP  |***]:MCU version             : Out-dated, needs upgrade
[04/47  | SFP  |***]:LUT marker              : Up-to-date
[04/47  | SFP  |***]:DSP version             : Out-dated,needs upgrade
[**/*** | SFP  | PHASE1]:Image Integrity Check : Passed
[**/*** | SFP  | PHASE1]:Image Integrity Check : Passed
[**/*** | SFP  | PHASE1]:Image Integrity Check : Passed
[**/*** | SFP  | PHASE1]:Image Integrity Check : Passed
[**/*** | SFP  | PHASE2]:Image Integrity Check : Passed
[**/*** | SFP  | PHASE2]:Image Integrity Check : Passed

[**/*** | ***** | ***]: Number of sfps queued for upgrade: 1 (SFP: 1, SFPDD 0)

**************************************************
SFP upgrade validations done. Attempting SFP upgrade on
incompatible SFPs may lead to the SFP being non-operational. This operation needs to run
till completion, if interrupted, the SFPs may become inoperable.
**************************************************
Are you sure to continue upgrade [y/n]: y
[**/*** | ***** | ***]:upgrade sessions active:1 (requested: 1)
[04/47 | SFP    | PHASE1]:Upgrade started
[04/47 | SFP    | PHASE1]:complete 36%
[04/47 | SFP    | PHASE1]:complete 73%
[04/47 | SFP    | PHASE1]:Upgrade completed
[04/47 | SFP    | PHASE1]:wait for module refresh
[04/47 | SFP    | PHASE1]:Upgrade successful
[04/47 | SFP    | PHASE2]:Upgrade started
[04/47 | SFP    | PHASE2]:complete 6%
[04/47 | SFP    | PHASE2]:complete 21%
-----Truncated------
[04/47 | SFP    | PHASE2]:complete 93%
[04/47 | SFP    | PHASE2]:Upgrade completed
[04/47 | SFP    | PHASE2]:wait for module refresh
[04/47 | SFP    | PHASE2]:Upgrade successful
[04/47 | SFP    | ***]:Start SFP Power-cycle
[04/47 | SFP    | ***]:SFP Power-cycle completed
**************************************************
*  SFP Upgrade Report      *
**************************************************
No. of SFPs queued for upgrade   : 1
No. of SFPs upgrade complete     : 1

No. of SFPs upgrade failed : 0
**************************************************
```

The SFP upgrade duration is 15 minutes.

The universal SFP now supports Ethernet and the ports are now configured to port type ETH:

```
IPS1:FID101:admin> portcfgflexport --proto eth 4/47
Success: Port(s) 4/47 are configured as port type ETH
```

4.2.4.7 IP Storage Commands

The following commands are available to configure the IP Storage logical components:

- VRF – Virtual Routing and Forwarding
  - `ipsVrf`
- VLAN – Virtual LAN
  - `ipsVlan`
- Interface – IP Storage interface configuration
  - `ipsInterface`
- IP Static Route – IP Static Route configuration
  - `ipsStaticRoute`
- Routing Table – Routing table information
  - `ipsRouteTable`
- Static ARP – Static ARP configuration
  - `ipsStaticArp`
- ARP Table – ARP table information
  - `ipsArpTable`
- LAG – Link Aggregation Group
  - `ipsLag`

For full details and description of command usage refer to the *Fabric OS Administration Guide 9.2x* and *Fabric OS Command Reference Manual 9.2x*.

4.2.4.8 IPS Diagnostics

IP Storage diagnostics is available in every IPS LS and can be used to validate the paths from an IP Storage LS to network devices - such as hosts, targets, switches and routers connected to the IP Storage Fabric.

IPS diagnostics includes the following commands and functions:

- `ipsPing`
- `ipsTraceRoute`
- `ipsNeighborInfo`
- `ipsPathVerify`
- `ipsReachable`

For full details and description of command usage see the *Fabric OS Administration Guide 9.2x* and *Fabric OS Command Reference Manual 9.2x*.

4.2.4.9 SNMP MIBs for IPS

The list of SNMP MIBs supported for IPS are summarized below.

New MIBs:

- LLDP-MIB
- LLDP-EXT-DOT1-MIB
- LLDP-EXT-DOT3-MIB
- IEEE8023-LAG-MIB
- BROCADE-IP-STORAGE-MIB

NOTE In the above list, the BROCADE-IP-STORAGE-MIB is a proprietary MIB which fetch fabric-wide data, and the other MIBs are all standard MIBs which fetch local (switch) data.

There are no new SNMP traps supported in this release. All the new MIBs have Read Only access.

Existing MIBs Which Are Relevant to IPS:

- IF-MIB

The legacy MIBs listed below are already supported in Fabric OS and the functionality remains the same.

- IP-MIB
- TCP-MIB
- UDP-MIB

4.2.4.10 IPS sFlow Monitoring

sFlow is a multi-vendor sampling technology embedded in network devices such as switches, routers and servers. Providing an ability to continuously monitor traffic at line rate across multiple interfaces. The sFlow protocol created by InMon and standardized in RFC 3176, version 5 is currently the latest supported version. sFlow agents and collectors are the building blocks of the monitoring solution.

The sFlow Agent is the monitoring component that samples packets and interfaces. Packet samples are one out of a specified number of packets on a configured interface. Interface samples are counter statistics at periodic intervals on the Ethernet interfaces.

FOS provides an embedded sFlow agent for IPS interface samples and statistics. The sFlow Agent is then configured to exports sampled data in UDP datagram to the sFlow collector(s).

The collector is a software application on an external server that collects the exported data from different agents to provide a cohesive view. Using sFlow collector software, the information collected from sFlow agents can be analyzed and presented to network administrators in a variety of ways, such as charts, dashboards, and thresholds. sFlow monitoring helps in the identification, diagnosis, and correction of traffic issues.

The following summarizes the default support of sFlow agent introduced in FOS v9.2.1.

- sFlow agent sampling scope is limited to Ethernet interfaces only (at physical port level not at LAG level).
- sFlow can be enabled only on the ingress traffic.
- sFlow agent shares 256 frames per second FC mirroring limit per ASIC.
- sFlow agent cannot be configured or managed through SNMP by the collectors
- Data from sFlow-enabled interfaces' can be uploaded to a single collector.
- Out-of-band data upload to the collector with management VRF support
- The ASIC sampling algorithm decides the sampled packet across all the flows on the interface.
- sFlow Agent cannot sample at a particular flow level
- Sampled packets follow a random selection algorithm and not determined by a fixed periodic packet count
- Sample rate is pre-configured to 1 in 1048576 packets. It is not configurable in FOS v9.2.1.
- Interface counter statistics collected at a pre-configured 20-second polling interval.
- The sample is taken by extracting the packet header.
- sFlow sample truncation size is 128 bytes.
- UDP datagram size is 1500 bytes and not configurable.
- The sample metadata has software derived values, and the formula is tabulated in respective sections.

For full details and description of sFLOW configuration and command usage see the *Fabric OS Administration Guide 9.2x* and *Fabric OS Command Reference Manual 9.2x*.

4.2.5 Firmware Patch

In FOS v9.2.0 the firmware management feature firmwarepatch was introduced. Firmwarepatch is implemented to provide a more efficient method to support customers that need a patch release. Firmwarepatch provides the ability to install the patch on the current FOS version of the switch instead of a full firmware download process with a CVR release build which replaces the FOS image on the switch.

4.2.5.1 IPS PacketDump

With FOS v9.2.1 the firmwarepatch IPSpacketDump is available (by contacting support) for IPS troubleshooting in USF.

The command `ipsPktDump` is a maintenance account level command which is designed to capture in-band IPS packets and display the header contents. The command provides various options to customize the display of captured packets along with writing the captured packers to pcap files. The functionality is like `tcpdump` but only available on (inband) IPS interfaces capturing a maximum of the first 48 bytes from each captured packet.

4.2.6 Miscellaneous

This section includes miscellaneous enhancements and changes in FOS v9.2.1.

4.2.6.1 Flow Vision Scale

From FOS v9.2.0x to FOS v9.2.1 the distribution of IT and ITL/ITN scale and stats granularity are changed. For details see Flow Vision.

4.2.6.2 D-Port on EX-Port

With FOS v9.2.1, D-Port test can be performed without disabling the EX-Port configuration. The EX-Port can be configured on a VF disabled or VF enabled switch. In case of a VF enabled switch, the EX-Port is supported only on base switch.

The EX-Port is also a configurable parameter configured using `portcfgexport`. To run the D-Port test, the EX-Port config is removed internally and its parameters like RA_TOV and fabricID are stored on the config file. The D-Port on EX-Port configurations are committed and stored in the port config using PDM_OPT_NO_COMMIT.

On reboot or hafailover the D-Port configuration will be persistent. After D-Port config removal, FCR fabric will be restored automatically. The D-Port test can be run either in static or dynamic or on-demand D-Port mode.

Static to Static: Configure D-Port on both sides of the link as follows:

```
Switch:FID128:admin> Portdisable <port no>
Switch:FID128:admin> Portcfgdport –enable <port no>
Switch:FID128:admin> Portenable <port no>
```

Before configuring the port as D-Port, all the EX-Port parameters like fabric ID, RA_TOV, ED_TOV, etc., will be saved in a config file (for future use). A new flag, dportBackupExport, will be defined in the port config bitmap for D-Port over EX-Port. The EX-Port configuration will be removed internally, and D-Port mode will be enabled.

On successful reversion of D-Port test i.e. on D-Port configuration removal, this new flag will be used to restore the EX-Port parameters, so that FCR switch will not get merged with edge fabric.

Static to Dynamic or Vice Versa: Configure static D-Port on E-Port and bring the EX-Port as dynamic. When D-Port is configured, the ELP will be sent to the FCR switch with D-Port mode. FCR on receiving this ELP will check the D-Port mode and reject the ELP. On receiving the D-Port mode, the EX-Port parameters/configuration will be disabled internally. A new flag, dportBackupExport will be set for D-Port over EX-Port and the port will be toggled. Since EX-Port parameters are disabled, the port will transition from EX-Port to E-Port and normal ELP will be sent so that the FCR switch will come up in the dynamic mode and the D-Port tests will be performed.

On successful reversion of static D-Port (E-Port), the switch will initiate ELP on port online. The FCR switch on receiving the ELP will check the port config bitmap. If the new flag is set, the EX-Port parameters will be restored, and the port will be toggled. After port toggle, E to EX-Port protocol kicks in.

4.2.6.3 Time Zone Configuration

Prior to FOS v9.2.1, a time zone configuration change in FOS required a reboot of the switch.

In FOS v9.2.1 it is no longer required to reboot the switch for time zone changes to take effect.

NOTE In a director both CPs must be running FOS v9.2.1 to support changing the time zone without requiring switch reboot.

There are no new commands added for this enhancement.

4.2.6.4 Link Latency Determination

In FOS v9.2.1, a new Link Latency Determination (LLD) feature is supported between N-Port and F-Port to reliably determine the link latency of the connection during the link bring up stage itself. This is supported only on Gen 7 platforms.

LLD is enabled by default and controlled with the command `portCfgLld`.

```
Usage:     portCfgLld {--enable | --disable | --show } [<slot>/]<port>
           portCfgLld --help
Operands :
           --enable - Enable the Link Latency Determination feature
           --disable - Disable the Link Latency Determination feature
           --show - Show LLD configuration for the port
           --help - Help command to see Usage
```

The latency value is computed by exchanging the MARK primitives between Switch and HBA. Newer Gen7 HBAs support the MARK primitives exchange. This feature is applicable between N-Port and F-Port, other port types are not applicable. When D-Port mode is enabled for F-Port, the latency value will be computed.

There is no user alert displayed for latency value either via raslog or audit message. Previously the link latency value was measured during the D-Port test. Now this functionality is enhanced to be computed during the link initialization phase itself. When the latency value can't be determined, or it is invalid 0 will be displayed.

Example output displaying the latency value is highlighted below:

```
Switch101:FID128:admin> sfpshow 14 -link
Identifier: 3  SFP
Connector:     7     LC
Transceiver: 0204406000000000 16,32,64_Gbps M5 sw Inter,Short_dist
State transitions: 1
Roundtrip Link Latency: 420nSec
Port Speed Capabilities Not Available
```

4.2.6.4.1 Access Gateway (AG Mode) Considerations

The behavior is similar for AG Mode enabled switches. In the AG switch, the N-Port will mimic the HBA behavior. The N-Port after sending FLOGI will transmit Device Mark. The transmitted MARK primitive will be looped back and the latency is calculated.

4.2.6.4.2 Trunking Considerations

In case of trunk ports, the latency will be calculated separately for principle and subordinate ports. The mark primitives will be exchanged regardless of dummy or real FLOGI whichever is sent or received first.

This feature is applicable for all F-Port trunk scenarios:

- AG to Switch
- HBA to Switch in trunk mode.

NOTE There is no impact when the principal port or subordinate port goes offline. The latency value is calculated only once when the port comes online, and the value is valid till the port goes offline.

4.2.6.4.3 NPIV Considerations

In case of NPIV ports, the LLD feature is supported for the base login FLOGI frame. The MARK primitives exchange will not be honored for FDICSs from NPIV devices.

4.2.6.4.4 D-Port Considerations

When D-Port mode (either static or dynamic) is enabled for the F-Port, the MARK primitives will be sent regardless of real or D-Port FLOGI whichever precedes first.

4.2.7 Web Tools

4.2.7.1 Display of USF Components

With FOS v9.2.1 Web Tools (WT) is enhanced to display IPS logical switches and ETH-Port interfaces. WT does not provide configuration of IPS components in USF.

4.2.7.2 Port Investigation

With FOS v9.2.1 WT does not support port investigation for all the ports (FC-Ports, ICL-Ports, ETh-Ports and GigE-Ports) from the Switch port list view.

Accordingly, Tunnel and Circuit investigation is removed for VE ports.

4.2.7.3 Zoning

With FOS v9.2.1 WT is enhanced to reflect the workflow and user experience in SANnav Management Portal.

The enhancements include:

- Display Principal and Peer tooltip label.
- The tooltip label (Peer / Principal) is displayed on the peer zone icons on hovering the mouse to represent the member as peer or principal.
- Provision to create new Zone from Zone Configuration Add Zone dialog.
- Users can create new zones within Zone configuration without navigating to the zone tab.
- Add Status (Active and Inactive) column in Zone list page.
- Zone status column shows the current status of the zone in zone list page (Active / Inactive).
- Add Members and Zone Column in Zone Alias List page.
- Members and Zone columns are added in the zone alias list page. Members column displays the list of members for the alias and Zone column displays the zones in which the alias is present.
- Moved activate Zone configuration to Page Action menu.
- The Activate Zone option is moved to the page action menu from the bottom of the page.
- Display Defined (Modified) status in the Zone Configuration List page.

  If the defined configuration is modified, then the label (modified) will be appended in the status column in the zone configuration list view.

4.2.8 REST

FOS v9.2.1 includes REST enhancements listed below in addition to equivalent REST support for all new or modified CLI commands in FOS v9.2.1.

4.2.8.1 rdp-polling-cycle

A new leaf rdp-polling-cycle has been added to the brocade-fibrechannel-configuration to configure the polling cycle. If the value of the leaf is configured to be 0, the polling cycle is disabled. The value can be set in between 1 to 24 to specify the polling cycle in hours.

4.3 Deprecated and Obsoleted Software Features

This section describes deprecated and obsoleted features.

4.3.1 Deprecated Software Features

FOS v9.2.1 deprecate support for the following features: TACACS+ authentication

TACACS+ functionality is kept intact while the end user is notified with the message (displayed below) in following cases:

- During the firmware update, only if a TACACS+ server is configured.
- When a new TACACS+ server is added.

```
TACACS+ is deprecated and will be obsoleted in a future FOS version.
In this FOS version, TACACS+ functionality is unchanged.

Please plan accordingly.
```

4.3.2 Obsoleted Software Features

FOS v9.2.1 obsoletes support for the following features: Fabric Assigned PWWN.

FA PWWN was deprecated in FOS v9.2.0 and is now obsoleted. All FA PWWN pertinent CLI operations are blocked (both switch port and AG assisted CLI commands) and configuration is not allowed to be imported, configured or otherwise created. Firmwareupgrade is not permitted to 9.2.1 when FA PWWN configuration exists on the switch.

The following error message will be displayed when attempting to upgrade to FOS v9.2.1 with FA PWWN present on the switch:

```
ERROR: fapwwn is deprecated. Please remove all fapwwn configurations in all the logical
switches by using the "fapwwn --delete" command. After removing the config, please
disable the fapwwn configuration on the HBA ports and make sure the physical PWWN is
used.

Firmwaredownload failed.
```

Listing the FA PWWN defined on the switch

```
Switch:FID128:admin>fapwwn --show all
-------------------------------------------------------------------------------------
Port     Device Port WWN           Virtual Port WWN          PID    Enable   MapType
-------------------------------------------------------------------------------------
0        --:--:--:--:--:--:--:--   52:00:10:00:00:0f:50:30   10101   Yes     Port/Auto
```

4.3.3 Deprecated CLI Comands

FOS v9.2.1 deprecate support for the following FOS diagnostics commands:

- `porttest`
- `porttestshow`
- `stopporttest show`

Instead, customers can use the command `spinfab`.

Chapter 5: Software License Support

5.1 Optionally Licensed Software

Fabric OS v9.2.x includes all basic switch and fabric support software, as well as optionally licensed software that is enabled via license keys or license files.

Optionally licensed features include:

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

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

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

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

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

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

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

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

Integrated Routing – This license allows any Fibre Channel port in a Brocade X7-4, X7-8, G720, G730 and G620 to be configured as an EX_Port supporting Fibre Channel Routing (FCR).

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

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

On the Brocade X6-8:

The first ICL POD license enables 8 UltraScale ICL QSFP ports on each core blade of the X6-8 director, which are QSFP port numbers 0-3 and 8-11. The second ICL POD license enables all UltraScale ICL QSFP ports on each core blade of the director.

On the Brocade X6-4:

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

On the Brocade X7-8:

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

On the Brocade X7-4:

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

On the Brocade 7810:

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

5.2 Temporary License Support

The following licenses are available in Fabric OS v9.2.x as either universal temporary or regular temporary licenses:

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

NOTE

- Temporary licenses for features available on a per-slot basis enables the feature for all slots in the chassis.
- There are no temporary licenses for the Brocade 7850 platform.

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

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

Chapter 6: Hardware Support

6.1 Supported Devices

The following devices are supported in this release:

- Brocade X7-8 Director
- Brocade X7-4 Director
- Brocade X6-8 Director
- Brocade X6-4 Director
- Brocade G730 Switch
- Brocade G720 Switch
- Brocade G630 Switch
- Brocade G620 Switch
- Brocade G610 Switch
- Brocade G648 Blade Server SAN I/O Module
- Brocade 7850 Extension Switch
- Brocade 7810 Extension Switch

6.2 Supported Blades

6.2.1 X6-8 and X6-4 Blade Support

Fabric OS v9.2.x software is fully qualified and supports the blades for the X6-8 and X6-4 as noted in the following table.

Blades	FOS v9.2.x Support
FC32-48 32G FC Blade	Supported.
SX6 Gen 6 Extension Blade	Supported. Up to a maximum of four blades of this type.
FC32-64 32G FC/FCoE Blade	Supported.

6.2.2 X7-8 and X7-4 Blade Support

Fabric OS v9.2.x software is fully qualified and supports the blades for the X7-8 and X7-4 as noted in the following table.

Blades	FOS v9.2.x Support
FC64-64 64G FC Blade	Supported
FC64-48 64G FC Blade	Supported.
FC32-X7-48 32G X7 FC Blade	Supported.
FC32-48 32G FC Blade	Supported.
SX6 Gen 6 Extension Blade	Supported. Up to a maximum of four blades of this type.
FC32-64 32G FC/FCoE Blade	Supported.

6.3 Supported Power Supplies

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

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

6.4 Supported Optics

FOS v9.2.0 is the first release supporting the Gen 7FC QSFP+, PN:57-1000481-01 (XBR-000420) with serial number BAB1yywwxxxxxxs.

When this optic is present and downgrade from FOS v9.2.0 is performed, the `firmwaredownload` will fail with the following error:

```
Downgrade is not allowed as some of the ICL ports are connected with GEN7 100M QSFPs.
Please remove the QSFP(s) flagged and retry firmwaredowngrade.
```

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

Chapter 7: Software Upgrades and Downgrades

7.1 Platform Specific Downloads

This release of FOS is available for entitled equipment download in Platform Specific Download (PSD) form. FOS PSD releases provide a smaller version of the FOS image that can only be loaded on a single hardware platform, consisting of a single switch model or group of switch models. These FOS PSD images enable much faster download and file transfer times since they are between 65-90% smaller in size than traditional full FOS images.

Unlike traditional FOS release images that can be installed on any supported Brocade switch and director, FOS PSD images must be downloaded separately for each platform that the FOS release will be used on. The full list of unique FOS PSD images available for this release and the models that each PSD image supports is noted in FOS Image Filenames.

7.1.1 Using FOS PSDs

FOS PSD images are generally used in the same manner as traditional full FOS release images.

Once loaded onto a switch, the FOS image running is identical to what would be in use if a traditional full image was used for the installation. Issuing a `firmwareshow` command on a switch will display only the FOS version level, with no indication of whether the code was loaded from a FOS PSD image or a full FOS image.

7.1.1.1 Loading FOS PSDs via Web Tools or FOS Command Line

Installing a FOS PSD image on a switch is performed in the same manner as using a traditional full FOS image. If a FOS PSD image is loaded on an incorrect switch model (for example, attempting to load a FOS PSD image for a Gen 6 entry level switch on a Gen 6 Director), the following error message displays:

```
Cannot download the requested firmware because the firmware doesn't support this
platform. Please enter another firmware.
```

7.1.1.2 Loading FOS PSDs via Brocade SANnav Management Portal

Brocade SANnav Management Portal v2.1.1 or earlier does not support FOS PSD images. However, FOS PSD images are supported with SANnav v2.1.1.3 and later releases. SANnav v2.1.1.3 and later can both host and install FOS PSD images onto Brocade switches.

7.2 FOS Image Filenames

Fabric OS v9.2.1

Image Filename	Description
v9.2.1.md5	Fabric OS v9.2.1 MD5 Checksums
v9.2.1_all_mibs.tar.gz	Fabric OS v9.2.1 SNMP MIBs
v9.2.1_EXT.tar.gz	Fabric OS v9.2.1 for Linux to install on 7810 and 7850 platforms
v9.2.1_EXT.zip	Fabric OS v9.2.1 for Windows to install on 7810 and 7850 platform
v9.2.1_EMB.tar.gz	Fabric OS v9.2.1 for Linux to install on G648 platform
v9.2.1_EMB.zip	Fabric OS v9.2.1 for Windows to install on G648 platform
v9.2.1_G6_ENTRY.zip	Fabric OS v9.2.1 for Windows to install on G610 platform

v9.2.1_G6_ENTRY.tar.gz	Fabric OS v9.2.1 for Linux to install on G610 platform
v9.2.1_G6_MID.tar.gz	Fabric OS v9.2.1 for Linux to install on G620 platform
v9.2.1_G6_MID.zip	Fabric OS v9.2.1 for Windows to install on G620 platform
v9.2.1_G6_ENTP.tar.gz	Fabric OS v9.2.1 for Linux to install on G630 platform
v9.2.1_G6_ENTP.zip	Fabric OS v9.2.1 for Windows to install on G630 platform
v9.2.1_G7_MID.tar.gz	Fabric OS v9.2.1 for Linux to install on G720 platform
v9.2.1_G7_MID.zip	Fabric OS v9.2.1 for Windows to install on G720 platform
v9.2.1_G7_ENTP.tar.gz	Fabric OS v9.2.1 for Linux to install on G730 platform
v9.2.1_G7_ENTP.zip	Fabric OS v9.2.1 for Windows to install on G730 platform
v9.2.1_G6G7_DIR.tar.gz	Fabric OS v9.2.1 for Linux to install on X6-8, X6-4, X7-8 and X7-4 platforms
v9.2.1_G6G7_DIR.zip	Fabric OS v9.2.1 for Windows to install on X6-8, X6-4, X7-8 and X7-4 platforms
v9.2.1.releasenotes_v2.pdf	Fabric OS v9.2.1 Release Notes

The image files for each respective platform can be downloaded from your switch vendor's website and support.broadcom.com, except for YANG files which are available on www.broadcom.com/products/fibre-channel-networking/software/fabric-operating-system.

7.3 Migration Path

This section contains important details to consider before migrating to or from this FOS release. Refer to the *Brocade Fabric OS Software Upgrade User Guide* for detailed instructions on non-disruptive and disruptive upgrade procedures.

7.3.1 Migrating to FOS v9.2.1

The supported upgrade paths to Fabric OS v9.2.1 are as follows:

Current Version	Upgrade Path
FOS v9.2.0x	Nondisruptive upgrade
FOS v9.1.x	Disruptive upgrade: Upgrade directly from FOS v9.1.x to v9.2.1 Nondisruptive upgrade: First upgrade from FOS v9.1.x to FOS v9.2.0x. (Install TruFOS certificate prior to upgrade to v9.2.0x if not already present on the switch)
FOS v9.0.x	Disruptive upgrade: Upgrade directly from FOS v9.0.x to v9.2.1 Nondisruptive upgrade: First upgrade from FOS v9.0.x to FOS v9.1.x. (Install TruFOS certificate prior to upgrade to v9.2.0x if not already present on the switch)
FOS v8.2.x	First upgrade from FOS v8.2.x to FOS v9.x. Then install TruFOS Certificate and proceed according to above.

7.3.2 Migrating from FOS v9.2.x

The following table lists the currently supported Fabric OS downgrade versions and platforms.

Gen 6 and Gen 7 Platforms and Supported Firmware Downgrade Versions from Fabric OS v9.2.x

Platforms	Fabric OS v9.2.x	Fabric OS v9.1.x	Fabric OS v9.0.x	Fabric OS v8.2.x
Brocade Gen 7 (64G) Fixed-Port Switches				
Brocade G720 (Switch Type 181.0)	Supported	Supported	Supported	Not Supported
Brocade G720 (Switch Type 181.5)	Supported	Supported (Fabric OS v9.1.1 and later)	Not Supported	Not Supported
Brocade G730 (Switch Type 189.8)	Supported	Supported	Not Supported	Not Supported
Brocade Gen 7 (64G) Directors				
Brocade X7-4 Director	Supported	Supported	Supported	Not Supported
Brocade X7-8 Director	Supported	Supported	Supported	Not Supported
Brocade G610 (Switch Type 170.0 to 170.3)	Supported	Supported	Supported	Supported
Brocade G610 (Switch Type 170.4 or higher)	Supported	Supported	Supported (Fabric OS v9.0.1b and later)	Not Supported
Brocade G620 (Switch Type 162)	Supported	Supported	Supported	Supported
Brocade G620 (Switch Type 183.0)	Supported	Supported	Supported	Not Supported
Brocade G620 (Switch Type 183.5)	Supported	Supported (Fabric OS v9.1.1 and later)	Not Supported	Not Supported
Brocade G630 (Switch Type 173)	Supported	Supported	Supported	Supported
Brocade G630 (Switch Type 184)	Supported	Supported	Supported	Not Supported
Brocade 7810 Extension Switch	Supported	Supported	Supported	Supported (Fabric OS v8.2.1 and later)
Brocade G648 Blade Server SAN I/O Module	Supported	Supported	Supported	Supported
Brocade MXG610 Blade Server SAN I/O Module	Not Supported	Supported	Supported	Supported
Brocade X6-4	Supported	Supported	Supported	Supported
Brocade X6-8	Supported	Supported	Supported	Supported
Brocade X6-4 (Switch Type 165.5)	Supported	Supported (Fabric OS v9.1.0b and later)	Not Supported	Not Supported
Brocade X6-8 (Switch Type 166.5)	Supported	Supported (Fabric OS v9.1.0b and later)	Not Supported	Not Supported

7.4 Brocade Trusted FOS (TruFOS) Certificate

Brocade TruFOS Certificates are factory installed on applicable platforms shipping with FOS v9.x.
When upgrading to FOS v9.2x a valid TruFOS certificate is required for all platforms (except embedded switches).

FOS v9.2.0 is the first FOS version where TruFOS applies to the following platforms:

- G720
- G620
- G610
- 7850
- 7810

TruFOS certificate installation can be performed using SANnav or using the CLI command license as shown in the example below:

```
Switch:admin> license –install -h 10.10.10.10 -t ftp -u UserName -p Password -f
/20211013171159568_10_00_c4_f5_7c_64_5b_60.xml
License Installed [FOS-87-0-04-11209683]
```

NOTE When downgrading from FOS v9.2.0 MAPS TruFOS rules become unmonitored for the platforms listed above.

7.5 Upgrade/Downgrade Considerations

Firmware upgrade and downgrade support for FOS v9.2.1 is displayed in the table below.

NOTE Disruptive firmware download with FOS levels two versions apart is allowed only for upgrades not for downgrades.

From	To	Behavior
v9.2.1	v9.2.0x	Non-Disruptive
v9.2.0x	**v9.2.1**	Non-Disruptive
v9.2.1	v9.1.x	Disruptive
v9.1.x	**v9.2.1**	Disruptive
v9.0.1x	**v9.2.1**	Disruptive
v9.2.1	v9.0.1x	**Not supported**

When upgrading a Gen 7 director or switch (X7-4, X7-8, G730, G720) to FOS v9.2.x, it is recommended to upgrade to FOS v9.2.0a or later. For additional information see TSB 2023-289-A.

In FOS v9.1.x (and later) when performing `firmwaredownload`, the HA reboot triggers the broadcast message:
`The system is going down for reboot NOW!`
This is a standard Linux message when a system is doing a graceful shutdown.

This is non-disruptive to I/O traffic during this process.

Example below:

```
Do you want to continue (Y/N) [Y]:
Firmware download in progress, please wait.
Broadcast message from root@Switch (Fri Aug 26 10:59:01 2022):
The system is going down for reboot NOW!
```

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

Chapter 8: Limitations and Restrictions

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

8.1 Scalability

All scalability limits are subject to change. Limits may be increased once further testing has been completed, even after the release of this version of the Fabric OS software. For current scalability limits for Fabric OS software, refer to the *Brocade SAN Scalability Guidelines for Brocade Fabric OS v9.X* document.

8.1.1 Flow Vision

In FOS v9.2.1 the distribution of IT and ITL/ITN scale and stats granularity are changed as shown in the table below:

Property	FOS v9.2.0	FOS v9.2.1
Total flows	72k	72k
IT	8k	32k
IT stats granularity	5 min	5 min
ITL/ITN	64k	56k
ITL/ITN stats granularity	6h	30 min
VITL/VITN	64k*	56k*
VITL/VITN stats granularity	6h	30 min

*ITL/ITN and VITL/VITN share the same resource allocation and is provided on the principle of first come/first serve.

Flow Vision is not supported the Brocade 7850 Extension platform.

8.2 Compatibility/Interoperability

This section describes important compatibility and interoperability across Brocade products.

8.2.1 Brocade SANnav Management Portal Compatibility

When managing SAN switches with SANnav Management Portal it is required to first upgrade SANnav Management Portal to v2.3.1 (or later) prior to upgrading SAN switches to FOS v9.2.1.

For details, review the latest *SANnav Management Portal Release Notes*.

8.2.2 Web Tools Compatibility

Web Tools supports firmware migration to v9.2.x from FOS v9.1.x.

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

If a DSA algorithm is used for the HTTPS certificate, then Web Tools cannot discover the switch because all the supported ciphers for this algorithm are no longer supported.

8.2.3 Fabric OS Compatibility

- The following table lists the earliest versions of Brocade software supported in this release, that is, the earliest supported software versions that interoperate. Use the latest software versions to get the greatest benefit from the SAN.
- To ensure that a configuration is fully supported, always check the appropriate SAN, storage, or blade server product support page to verify support of specific code levels on specific switch platforms before installing on your switch. Use only Fabric OS versions that are supported by the provider.
- For a list of the effective End-of-Availability dates for all versions of Fabric OS software, refer to the *Brocade Software End-of-Availability Notice* published to the Brocade Product End-of-Life web page https://www.broadcom.com/support/fibre-channel-networking/eol.
- For the latest support and posting status of all release of Brocade Fabric OS, refer to the *Brocade Software: Software Release Support and Posting Matrices* published to the Brocade Product End-of-Life web page https://www.broadcom.com/support/fibre-channel-networking/eol.

Supported Products	Fabric OS Interoperability
Brocade 5424, 5431, 5432, 5480, NC-5480	FOS v7.4.2 or later (Not compatible in the same fabric. Must use FCR or connect as AG)
Brocade 300	FOS v7.4.2 or later (Not compatible in the same fabric. Must use FCR or connect as AG)
Brocade 7800	FOS v7.4.2 or later (Not compatible in the same fabric. Must use FCR) Note: There is no interoperability on VE interface(s) with another VE interface on a device running FOS v9.1.x (Brocade 7810 or Director with SX6 blade)
Brocade 7840	FOS v8.2.0 or later Note: When running FOS v8.2.1 or later there is interoperability on VE interface(s) with another VE interface on a device running FOS v9.1.x (Brocade 7810 or Director with SX6 blade)
Brocade DCX 8510-8/DCX 8510-4	FOS v8.2.x[1]
Brocade DCX 8510-8/DCX 8510-4 with FC16-64 blade	FOS v8.2.x[1]
Brocade 6505, 6510, 6520, 7840	FOS v8.2.x[1]
Brocade 6542	FOS v8.2.x[1]
Brocade 6543	FOS v8.2.x[1]
Brocade 6547, 6548, M6505, 6545, 6546	FOS v8.2.x[1]
Brocade 6558	FOS v8.2.x[1]
Brocade G610 (switchType 170.0 to 170.3)	FOS v9.0.0 or later[2]

[1] Only qualified with FOS v9.0.0 or later.
[2] While this platform is supported with FOS v8.x it is only qualified with FOS v9.0.0 or later.

Brocade G610 (switchType 170.4 or higher)	FOS v9.0.1b or later
Brocade G620 (switchType 162)	FOS v9.0.0 or later
Brocade G620 (switchType 183.0)	FOS v9.0.0 or later
Brocade G620 (switchType 183.5)	FOS v9.1.1 or later
Brocade G630 (switchType 173)	FOS v9.0.0 or later[Error! Bookmark not defined.]
Brocade G630 (switchType 184)	FOS v9.0.0 or later
Brocade 7810	FOS v9.0.0 or later[Error! Bookmark not defined.]
Brocade X6-8/X6-4	FOS v9.0.0 or later[Error! Bookmark not defined.]
Brocade X6-8/X6-4 (switchType 166.5 and 165.5)	FOS v9.1.0b or later
Brocade G720 (switchType 181.0)	FOS v9.0.0 or later
Brocade G720 (switchType 181.5)	FOS v9.1.1 or later
Brocade G730 (switchType 189.8)	FOS v9.1.0 or later
Brocade X7-8/X7-4	FOS v9.0.0 or later
Brocade G648[3]	FOS v9.0.0 or later
Brocade MXG610[4]	FOS v9.0.1a or later
Brocade 7850	FOS v9.2.0 or later

8.2.4 SNMP Support

Fabric OS v9.2.x 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 v9.2.x*.

8.2.5 Obtaining MIBs

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

1. Go to support.broadcom.com, click **Login**, and enter your username and password.

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

2. Select **Brocade Storage Networking** in the support portal.

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

8.2.6 Flow Vision, IO Insight and VM Insight

- In FOS v9.2.x the VMID+ feature is supported with extended ISL (XISL) usage on logical switches.
- The VMID+ feature is not supported with Fibre Channel Router (FCR).
- Configuring an EX_Port and F_Port with the application header on the same chassis is not supported in VF and non-VF mode. However, the configuration is not blocked.
- The VMID+ feature is not supported on FICON logical switch ports.
- Enabling the VMID+ configuration on F_Ports connected to encryption-supported third-party devices is not supported.

[3] Brocade G648 is also supported with FOS v8.2.0_gft release.
[4] Brocade MXG610 is also supported with FOS v8.1.0_lnx2, v9.0.1a, and v9.1.0b.

8.2.7 REST API Support

Fabric OS v9.2.x documents the supported REST API functions in the *Brocade Fabric OS REST API Reference Manual*.

8.2.7.1 Obtaining YANG Files

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

1. Go to www.broadcom.com/products/fibre-channel-networking/software/fabric-operating-system.
2. Select **Downloads**.
3. The YANG files can be located under the Yang Modules.
4. Unzip or untar the Fabric OS package file; the `yang.tar.gz` file contains the collection of YANG module files that this FOS release version supports. Untar the `yang.tar.gz` file to obtain individual YANG module files.

   Alternatively, the YANG modules for a specific FOS version can be downloaded from github.com/brocade/yang.

8.3 Important Notes

Brocade recommends to always review Important Notes for each release.

8.3.1 4G Support on Gen 6 Switches

The Brocade G620 with switchType 183, G630 with switchType 184, and FC32-X7-48 blades do not support 4G EX-Port.

Brocade G620 with switchType 183, G630 with switchType 184, and FC32-X7-48 blades support 4G E-Port connected between those three only (switchType 183, 184 and FC32-X7-48).

8.3.2 Access Gateway

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

8.3.3 Brocade Analytics Monitoring Platform

FOS v9.2.x supports vTap on Brocade legacy Gen 6 platforms to be monitored by the Brocade Analytics Monitoring Platform. The supported Brocade platforms include: G610, G620, G630, X6-4, and X6-8.

8.3.4 ClearLink Diagnostics (D_Port)

Fabric OS v9.2.x supports D_Port tests between two Brocade switches and between Brocade switches and Gen 5 (16Gb/s), Gen 6 (32Gb/s), and Gen 7 (64Gb/s) Fibre Channel adapters from QLogic and Emulex.

NOTE From FOS v9.2.0, Electrical and Optical loopback tests are deprecated from D-Port test functionality and CLI output. Link distance is only provided for distances over 1000 meters.

The following are specific adapter models and driver versions supported by Brocade with Fabric OS v9.2.x for ClearLink Diagnostics. Adapter firmware or driver versions that are later than the ones listed in the table may not work.

	Emulex 16G Adapter	Emulex 32G Adapter	Emulex Gen 7 Adapter	QLogic 16G Adapter	QLogic 32G Adapter
Adapter Model	LPe16002B-M6	LPe32002-M2	LPe35002 LPe35004 LPe36000	QLE2672	QLE2742
Adapter Firmware	12.8.542.25	12.8.542.26	12.8.542.xx	v8.08.231	V9.0.6.02
Adapter Driver	12.6.165.0	12.6.165.0	12.6.165.0 12.8.351.x	STOR Miniport 9.4.4.20	STOR Miniport 9.4.5.20

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

8.3.5 DDNS

Enabling and disabling the DDNS for IPv6 are disruptive operations which leads to DHCPv4 management IP change. Enabling this operand without caution will lead to losing all active SSH sessions due to IP address change. The users can login back to the switch only after finding the newly leased DHCPv4 address using the serial console.

NOTE When using MS Windows DHCP server, DNS should be configured on the switch (static or dynamic) for IPv6 DDNS feature to work with the Windows DHCP server.

8.3.6 Diagnostic POST

If Diagnostic POST is enabled, `supportSave` should not be started until the POST tests are completed after a switch or director boots up. Starting `supportSave` collection when POST tests are still running can result in unpredictable behavior.

8.3.7 DWDM

- For best performance and resiliency when deploying native FC ISLs over DWDM, best practice is to deploy distinct ISLs over DWDM with in-order delivery (iodset) configured on the switches.
- Trunking over DWDM is not recommended or supported by Brocade due to the risk of out-of-order frame delivery. Trunking relies on deterministic deskew values across all trunked links to provide in-order delivery as well as FC primitives for trunk formation. These deskew values cannot be guaranteed with DWDM equipment in the path.
- Use of trunking over DWDM links should only be done when validated and supported by the DWDM vendor.
- With Gen 7 switches, the permitted deskew (variance in latency due to difference in cable length) is less at 64G compared to lower interface speeds.

8.3.8 Ethernet Management Interface

- The recommended interface speed configuration for a Brocade Gen 6 or Gen 7 switch or director chassis is 1G auto-negotiate.
- If a Brocade switch management interface is running at 10Mb/s, certain FOS operations such as firmwaredownload may fail.
- The 10Gb/s management interface on CPX6 blades is not supported.
- Half-duplex mode is not supported in FOS v9.x and is blocked.

- The `ethif --reseterror` command option is supported in FOS v9.1.x and later.

8.3.9 Extension

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

Site1 Switch/Blade	Site1 Firmware	Site2 Switch/Blade	Site2 Firmware
7840	8.2.1 or later	7840	8.2.1 or later
SX6	9.0.0 to 9.1.x	7840	8.2.1 or later
7810	9.0.0 to 9.1.x	7840	8.2.1 or later

NOTE Extension between a Brocade 7810 or SX6 running FOS v9.2x and a Brocade 7840 is not supported.

Extension between a Brocade 7850 and Brocade 7810 or SX6 is supported only if the 7810 or SX6 is running FOS 9.2.0 or later. The following table documents the combinations.

Site1 Switch/Blade	Site1 Firmware	Site2 Switch/Blade	Site2 Firmware
7850	9.2.0 or later	7810	9.2.0 or later
7850	9.2.0 or later	SX6	9.2.0 or later

NOTE Extension between a Brocade 7850 and a Brocade 7840 is not supported.

8.3.10 FCoE

The following topologies for FCoE on the FC32-64 are not supported with FOS v9.2.x:

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

8.3.11 FC-NVMe

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

8.3.12 Firmware Migration

When doing staged firmware download migration from FOS v9.0.x to FOS v9.2.0 using `firmwaredownload -r` option if there is any explicit expected or unexpected switch reboot before the firmware is activated it can result in the switch or chassis being in an unrecoverable state. Consequently, the system will end up in an erroneous state and will not be able to boot up correctly.

NOTE

- This only applies when starting from FOS v9.0.x. When performing staged `firmwaredownload` migration starting from FOS v9.1.x to FOS v9.2.0 this does not apply.
- When upgrading deployments with FCoE (UCS FI connected with Ethernet Uplinks) from FOS v9.1.0x the following order must be followed to ensure non-disruptive upgrades:

- FOS v9.1.0x -> v9.1.1x -> v9.2.0x in order to retain FCoE logins and traffic during the upgrade process.
- An SNMP FFDC file may result as part of firmware migration to or from FOS v9.2.1 when the switch or director chassis is managed by SANnav v2.3.1. The conditions necessary to encounter the FFDC are the FOS level on the standby CP or secondary partition lack SHA512 authentication support. There is no functional impact however FFDC generation message appears repeatedly.

8.3.13 Forward Error Correction

- FEC is mandatory with Gen 6 and Gen 7 Fibre Channel operating at 32Gb/s or higher bandwidth. This means that the portcfgfec command applies only to ports that are running at 16Gb/s or 10Gb/s.
- FEC capability is not supported with all DWDM links. This means that FEC may need to be disabled on 16Gb/s or 10Gb/s ports when using DWDM links with some vendors. This is done using the portcfgfec command. Failure to disable FEC on these DWDM links may result in link failure during port bring-up. Refer to the *Brocade Fabric OS v9.x Compatibility Matrix* for supported DWDM equipment and restrictions on FEC use.

8.3.14 FPGA Upgrade

In general FPGA upgrades should only be performed when directed by your support provider.

When deploying the Gen 7 Fibre Channel 2KM QSFP (XBR-00476) for ICLs on Brocade X7, the Field Programmable Gate Array (FPGA) on each Core Routing blade (CR64) must be upgraded. If a Gen 7 Fibre Channel 2KM optic is plugged into CR64 blade with a down level FPGA version the RAS-LOG BL-1087 is displayed.

Example: `[BL-1087], 2973/525, SLOT 1 | CHASSIS, CRITICAL, X7-4, FPGA in slot 5 should be upgraded to support the Gen7 ICL QSFP for blade ID 214.`

From FOS v9.1.1 (and later), the FPGA upgrade can be performed non-disruptively by upgrading the CR64 blades one by one.

The upgrade process can take up to 20 minutes per CR64 blade.

NOTE If for any reason the FPGA upgrade fails it is recommended to reissue the upgrade steps, do NOT power-cycle the director or the affected slot.

8.3.14.1 FPGA Upgrade (for FOS v9.1.1 and Later)

To upgrade the FPGA on the CR64 blades perform the following steps:

1. Perform the following command to verify current FPGA code level `fpgaupgrade --latest`
2. Verify the *current* FPGA code level is lower than 0x01.0a for the CR64 blade slots
   - Slot 7 and 8 on X7-8
   - Slot 5 and 6 on X7-4

   After verification proceed to the next step.
3. Verify both CR64 blades are online with the command `slotshow`.
4. Prepare for upgrade of the FPGA on the first CR64 blade with the command `portdecom <ICL port> -qsfp` perform this for all connected E-ports (ICL ports) on the CR64 blade.
5. Disable the first CR64 blade on which the ICL ports were decommissioned in the previous step `portdisable -s <core blade slot #>`.
6. Upgrade the FPGA on the first CR64 blade with the command `fpgaupgrade -s <core blade slot #>`
   a. Respond `Yes` to automatically power-off and power-on the blade.
      (i) `Do you want to power-off and power-on the slot # automatically, after FPGA and/or CPLD upgrade (y/[n])?:`

b. In case you respond `No` to automatically power-off and power-on the blade perform these steps manually.

(i) `slotpoweroff <core blade slot #>`

(ii) `slotpoweron <core blade slot #>`

7. Verify the FPGA on the first CR64 blade is upgraded with the command `fpgaupgrade –latest.`
   a. Verify the FPGA code level is 0x01.0a
8. Enable the first CR64 blade with the command `portenable -s <core blade slot #>` (as needed).
9. Persistently enable all ICL ports on the CR64 blade (which were disabled in step 5 prior to the upgrade) `portcfgpersistentenable <ICL port>.`

   Repeat this step for all connected E-ports (ICL ports) on the CR64 blade.
10. Verify the ICL ports are online with the command `switchshow.`
11. Repeat steps 4 through 11 on the second CR64 blade.

The FPGA upgrade is now complete.

8.3.15 Security

In this section important security notes relevant to FOS v9.2.x are listed.

Default Secure

Platforms shipping with FOS v9.2.x from factory have Default Secure enabled. This means that unsecure protocols are blocked, and stronger cryptographic settings are applied. For more details refer to the *Brocade Fabric OS Administration Guide for Fabric OS v9.2.x*.

Default Session Limit

Default session limit is increased to 12 for local admin and maintenance accounts. The session limit is shared between the two accounts.

OU Field in FOS Switch CSRs No Longer Available

Effective August 24, 2022, the OU field will no longer appear in order forms for digital certificates, will be ignored in API requests, and will not be included in all new, renewed, and reissued public TLS/SSL certificates. This is due to a change by the CA/Browser forum, who dictates and issues guidelines to all Certificate Authority vendors. Accordingly, FOS v9.2.x is enhanced to adhere to the change imposed by CA/Browser forum.

This applies to certificates but excludes CA certificates. The OU field is removed in CSRs, Self-signed certificates, and a warning will be displayed on imports if the OU field is present.

Example of the Warning message:

```
FID128:admin> seccertmgmt import -cert https
Select protocol [ftp or scp]: scp
Enter IP address: 10.10.10.10
Enter remote directory: <certificate path>
Enter certificate name (must have ".crt" or ".cer" or ".pem" suffix):10.10.10.10-web.pem
Enter Login Name: <server username>
<user>@192.0.2.1's password:
```

Enter certificate name (must have `.crt` or `.cer` or `.pem` suffix):`10.10.10.10-web.pem`

WARNING Imported certificate contains OU field, which is deprecated starting with Fabric OS v9.2.0 based on the recommendations form CA/Browser forum.

Excerpt of certificate with OU field:

```
openssl x509 -in signed.10.10.10.10-web.pem -text -noout
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number: 1 (0x1)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, ST = California, L = San Jose, O = Brocade, OU = test, CN =
192.0.2.1, emailAddress = name@domain
        Validity
            Not Before: Jul 27 14:16:38 2016 GMT
            Not After : Jul 27 14:16:38 2017 GMT
        Subject: C = US, ST = California, L = San Jose, O = Brocade, OU = Demo, CN =
CA@demo
```

Excerpt of certificate without OU field:

```
openssl x509 -in 10.10.10.10-web.pem -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4098 (0x1002)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, ST = California, L = San Jose, O = Brocade, CN = 10.10.10.10,
emailAddress = name&domain
        Validity
            Not Before: Apr 14 13:41:43 2023 GMT
            Not After : Apr 11 13:41:43 2033 GMT
        Subject: C = US, ST = California, O = Brocade, CN = 10.10.10.10, emailAddress =
name@domain
```

The Following Security Enhancements All Apply to FOS v9.x

- FOS v9.x requires passwords for admin and user accounts to be changed from the default password string “password”. In the following scenarios, default password may still be present in FOS v9.0.x and v9.1.x. It is recommended to change the password in this scenario or at the next login prompt:
  - A default password is used in an earlier FOS version (prior to v9.0.0). FOS is upgraded from the earlier FOS version to FOS v9.x.
  - A default password is used in an earlier FOS version on active CP. The standby CP runs FOS v9.x and becomes active due to HA failover.
  - A default password is used in an earlier FOS version. Password is distributed from the earlier FOS version to FOS v9.x.
- It is recommended to reconfigure shared secrets for F_Port authentication between Access Gateway and switch before firmware upgrade to FOS v9.x. The shared secrets should be configured as given in the following table.

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

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

FOS Version	Shared Secret Configuration

Pre-v9.0.0	Device local secret = Switch local secret Device peer secret = Switch peer secret
9.0.0 or later	Device local secret = Switch peer secret Device peer secret = Switch local secret

- FOS v9.x does not support F_Port authentication to Marvell QLogic BR series (Former Brocade Product Line) HBAs as these HBAs only support legacy Brocade F_Port authentication. For these devices to connect to FOS v9.x, F_Port authentication must be disabled.
- FOS v9.x does not support F_Port trunking when F_Port authentication is enabled.
- Prior to upgrading to FOS v9.x:
  - First, ensure the secrets on both the switches (E-port authentication) are not the same. Otherwise, the E-port will segment after the upgrade to v9.x
  - Secondly, reconfigure shared secrets to be in compliance with FC-SP 2 standard.

    If users configure any duplicated Virtual Fabric (VF) list with `ldapcfg –mapattr <ldaprole>` command, only the first mapping from the list will be used during LDAP authentication and authorization.
- FOS v9.x requires role mapping or VSA attributes to be configured for LDAP user authentication in a VF-enabled switch. In a non-VF switch, `ldapcfg --maprole` is mandatory. It should be configured before upgrading to FOS v9.x to avoid login failure for LDAP users.
- Users must specify the domain of an LDAP server when adding the LDAP server to the remote AAA configuration of a switch.
- Optional certificate extensions, such as BasicConstraints, KeyUsage, and ExtendedKeyUsage are ignored when a certificate containing these is imported in basic mode. During session establishment, the extensions are validated. Hence, invalid extensions will be rejected and result in session failure.
- Login of LDAP users using Distinguished Name (DN) will be supported only for the users created in container “Users” of the domain configured in the switch, even though the switch is configured with Global Catalog (GC) port of the server. Login using User Principal Name (UPN) and sAMAccountName will be supported irrespective of the domain and OU on which the user is created.

8.3.15.1 Syslog

When using non secure syslog server configuration in FOS 9.1x and upgrading to FOS v9.2x the `cfgload.secure` configuration setting should be verified prior to upgrade. When this setting is set to `1` non secure syslog is no longer permitted after upgrade to 9.2x.

Example, verifying `cfgload.secure` setting:

```
Switch:FID128:admin> configure --show -mod CHS
Key Name                                                                  Value
Add Suffix to the uploaded file name(cfgload.cfgfile_suffix)                  0
Do you want to enable auto firmwaresync(cfgload.firmware_sync)                1
Enable secure switch mode(cfgload.secure)                                     1
```

When the `cfgload.secure` setting is set to `1` the end user must make the following decision:

- Move to using a secure syslog server (this is the recommended best practice)

Or

- Change the `cfgload.secure` setting to `0`, prior to upgrade to FOS v9.2x

  To change the `cfgload.secure` setting to `0` use the command

  ```
  configure --set -mod CHS -key cfgload.secure -value 0
  ```

Example, configuring `cfgload.secure` setting to `0` and verifying:

```
Switch:FID128:admin> configure --set -mod CHS -key cfgload.secure -value 0
```

```
Switch:FID128:admin> configure --show -mod CHS
Key Name                                                                    Value
Add Suffix to the uploaded file name(cfgload.cfgfile_suffix)                    0
Do you want to enable auto firmwaresync(cfgload.firmware_sync)                  1
Enable secure switch mode(cfgload.secure)                                       0
```

NOTE Setting `cfgload.secure` to `0`, also implies that FTP and HTTP protocols are permitted in FOS. These protocols can be blocked using IPFilter policy

8.3.16 Zoning

When performing `configdownload` with a file that contains unsorted zone membership, any unsorted members will be automatically sorted in the system when `configdownload` completes. As a result, when a switch is later re-enabled, port segmentation may occur due to adjacent switches having the same zones with unsorted membership lists. Users can recover from segmentation by executing `cfgDisable`, `cfgClear`, and `cfgSave` operations in order to clear the zoning database from the switch that just performed `configdownload`. After segmented ISL ports are re-enabled, zone merge can proceed.

NOTE These steps should ONLY be performed if the zone database is the same on the configdownload switch as it is on the rest of the fabric.

8.3.17 Brocade X6 Field Migration

- Field migration of a Brocade X6 switch to an upgraded X6 with Gen 7 support is not supported in FOS v9.2.x. In case a Brocade X6 switch is running FOS v9.2.x and it is desired to migrate to an upgrade X6 with Gen 7 support it is required to first downgrade to FOS v9.1.x and then perform the migration.
- FOS v9.1.x is the last release which supports a field migration of a Brocade X6 switch Type 165.5 and 166.5 to an upgraded X6 with Gen 7 support.
- Field migration of a Brocade X6 (switch Type 165 and 166) to an upgraded X6 with Gen 7 support is available with FOS v9.0.0x, FOS v9.0.1x and FOS v9.1.x.
  Refer to the *Brocade X6 Field Migration Guide* for step-by-step instructions.
- During field migration of Brocade X6 to a field upgraded X6 with Gen 7 support, the `portcfgupload` file will contain `portcfgtrunkport` commands for ICLs. A warning message is displayed to indicate that the command is not valid for ICL ports because trunking cannot be disabled on ICLs. This warning will not affect the ICLs and is harmless.

8.3.18 Miscellaneous

- After a power supply unit is removed from a Brocade G620, the `historyshow` command may miss the entries for this FRU removal or insertion event. In addition, the RASLog error message EM-1028 may be logged when the power supply is removed. This condition can be corrected by power-cycling the switch.
- After running offline diagnostics mode 1 on QSFP ports, a Brocade G620 must be rebooted before operational use.
- After running offline diagnostics with `portledtest`, `portloopbacktest`, or `turboramtest` commands on FOS v9.x, Brocade G630 with swtichType 184 must be rebooted before operational use.
- All links in an ICL QSFP connection on a Brocade X6 Director must be configured to the same speed using the `portcfgspeed` command from one of the following supported speeds: 16Gb/s, 32Gb/s, or ASN. To connect an ICL from an X6 with a 4x32GFC breakout optic (P/N 57-1000351-01) or a 4x16G FC optic to a 4x16G FC optic in a DCX 8510, the X6 port's speed must be set to 16Gb/s.
- Brocade G630 LEDs illuminate amber and green during power-up.
- The CLI command option `snmpconfig -set accesscontrol` is planned to be deprecated in the next major release.
- When replacing a FC32-64 blade with a FC32-48 blade, flexport and FCoE configurations should be removed before the FC32-64 blade is removed.

- Enhanced checks are performed on optics during firmware upgrade to FOS v9.0.0 or later. Firmware download is blocked if unsupported optics are discovered. The scanning of the optics takes a few minutes to complete. The amount of time it takes is dependent on the number of ports on a switch. On a fully loaded eight slot director, it can take up to five minutes to complete. In addition, ports with optics that fail the enhanced checks in FOS v9.x will not be able to come online due to the optics as invalid module.
- Brocade G620 with switchType 183 and G630 with switchType 184 do not support the following legacy optical modules:
  - 16G SWL (HAA1, HAA2 serial number)
  - 16G LWL (HDA1, HDA2, HDA3 serial number)
  - 32G QSFP SWL (ZTA serial number)

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

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

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

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

- All user ports in a Gen 7 ICL QSFP port must be assigned to the same logical switch when Virtual Fabric is configured. Port 0 of the ICL QSFP must be enabled first before port 1, port 2, and port 3 within the same QSFP to be enabled. If port 0 of the Gen 7 ICL QSFP becomes offline, port 1, port 2, and port 3 of the QSFP will become offline as a result.
- All user ports in a Gen 7, 2KM ICL QSFP port must be assigned to the same logical switch when Virtual Fabric is configured. Port 3 of the ICL QSFP must be enabled first before port 0, port 1, and port 2 within the same QSFP to be enabled. If port 3 of the Gen 7, 2KM ICL QSFP becomes offline, port 0, port 1, and port 2 of the QSFP will become offline as a result.
- The output of CLI command `sfpShow` or any other interfaces to retrieve information from Gen 7 SWL QSFP (part number 57-1000490) and LWL QSFP (part number 57-1000491) does not match the part numbers on the media sticker labels. The output shows Gen 6 part number (57-1000351 for SWL or 57-1000480 for LWL). This does not affect operation of the optics.
- When a fabric with FOS v9.x is connected to a fabric with pre-FOS v9.0.0, RASLOG message FABR-1001 is generated as shown in the following example. This is an expected message. There is no impact on the ISL functionality.

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

- FOS v9.x has disabled directory listing in CLI shell. As a result, entering <tab><tab> key does not list all CLIs available. Users can enter help command to list the commands. The shell tab completion by entering the first letter followed by <tab> key is supported.
- The FCR support of Long Distance Fabric mode conflict cannot coexist with long distance port configuration. If long distance mode (LD, LS, or LE) is enabled on the EX_Port and the EX_Port detected Backbone Fabric's Long Distance Fabric configuration is different from the connected Edge Fabric's Long Distance Fabric configuration, then the EX_Port will be disabled.
- If Long Distance Fabric is enabled on a switch via the configure command, it is recommended to upgrade the switch from FOS v8.2.x directly to FOS v9.0.0a or later. If the Long Distance Fabric configuration is enabled on an E_Port or EX_Port, firmware upgrade or downgrade to FOS v9.0.0 will effectively cause the Long Distance Fabric configuration to be disabled.
- If an HTTPS certificate is installed on a switch in FOS v9.x, HTTP access is blocked by default as HTTPS access is supported.

- When portloopbacktest mode1 test runs on multiple Gen 7 ICL ports with multiple iterations, the test may fail. The workaround is to run the test on one ICL port at a time with a reduced number of iterations.
- Running long distance LE mode between any blades or switches among FC32-X7-48, FC64-48, or G720 with port QoS mode enabled and vc_translation_link_init mode enabled may result in frame timeouts. The workaround for this problem is to use LS or LD mode for long distance.
- If downloading firmware on an unsupported platform, a write post to /rest/operations/show-status/message-id/20000 occurs and will incorrectly concatenate firmware download error messages. No recovery is needed, and this behavior will not cause any functional impact.
- Brocade G620 with switchType 183, G630 with switchType 184, and FC32-X7-48 blades do not support 4G EX-Port.
- Brocade G620 with switchType 183, G630 with switchType 184, and FC32-X7-48 blades support 4G E-Port connected between any of the three listed only.
- When Connecting Brocade G730 with X7, G720, G620 switchType 183 or G630 switchType 184 these switches should run FOS v9.0.1c or later.
- When performing a configdownload operation this will not overwrite the existing MAPS Custom RASLog mode feature configuration on the switch. For example, if custom raslog mode is disabled in the switch but it is enabled in downloaded configuration, then the feature will remain disabled in switch and must be manually configured after the configdownload operation is complete.
- In FOS v9.1.1, CPX blades in X6 Switch Type 165.5 and 166.5 and X7 are displayed as CPX7 in slotshow command output.
- When upgrading from FOS v9.0.x to FOS v9.1.x, the AG ports will be moved from ALL_HOST_PORTS group to ALL_OTHER_F_PORTS group. Consequently, the MAPS thresholds for ALL_OTHER_F_PORTS will apply to these ports in FOS v9.1.x. The default thresholds for the groups ALL_HOST_PORTS and ALL_OTHER_F_PORTS are the same and if these are not changed there is no impact. In case custom thresholds are used and these are configured differently for the groups ALL_HOST_PORTS and ALL_OTHER_F_PORTS the thresholds (monitoring) for AG ports are impacted accordingly.
- When performing factory reset on an X6/X7, the cipher.syslog key is not reset to factory value.

  Consequently, TLS handshake failure messages are displayed ongoing on standby CP:

  ```
  Message: [SEC-3077], 123, SLOT 1 | CHASSIS, INFO, sw0, Event: TLS SESSION, TLS handshake failed, Info: certificate verify failed. Host=x.x.x.x
  ```

  To work around this, perform `factoryreset` in the following way:

  1. `Factoryreset`
  2. When the `TLS handshake failure` message is displayed `-reboot` the standby CP.
     - In FOS v9.1.x (or later), to conform to RFC3315 and RFC5942, the default value of prefix length for IPv6 DHCP address changed from 64 to 128. The prefix and gateway information are provided by the Router Advertisement (RA) and it is expected that RA is enabled in the network. If IPv6 RA is not enabled in the network, IPv6 connectivity issues will occur.

  The resolution is to enable RA to resolve IPv6 network connectivity issues.
- In case an NPIV flow is identified as SDDQ or Over Subscribed (and moved by Traffic Optimizer to an OS PG), the flow movement may cause some frames to be delivered Out of Order (OOO). In general, open systems devices have no issues when this happens.
- When performing `supportSave` with `SCP` as the selected transfer protocol, the command defaults to using SFTP internally. In environments where SFTP ports are blocked the `supportSave` upload will fail.
- When displaying the content of an attached USB with the command `usbstorage --list` the directory structure is displayed using "/" (slash) in previous versions of FOS this was "\" (back slash).
- GigE ports on SX6 and 7850 platforms can only be moved to a logical switch when the port has only speed and autonegotiation configuration. This is a change in behavior from earlier releases.
- The command `firmwarecleaninstall` is available only for install of FOS v9.2.0a (upgrade or downgrade is not supported.
- When upgrading a Gen 7 director or switch (X7-4, X7-8, G730, G720) to FOS v9.2.x, it is recommended to upgrade to FOS v9.2.0a or later. For additional information refer to *TSB 2023-289-A*.
- When doing repeated failovers on NetApp A400 and FAS9000 storage arrays, the switch can register very high counts of uncorrectable errors on the ports connected to the storage arrays. These errors do not have any impact on storage data transport.

- In FOS v9.2.1 the MAPS chassis_memory -InRange rule is unmonitored and obsoleted.
- In the FC port external schema (available through NB streaming from SANnav Management portal) the user_port_index has been replaced with port_number for ease of use for end users:

  Previous schema (pre FOS v9.2.1):

  { "name" : "user_port_index", "type" : "int", "doc": "The user port index of the front-end port." }

  New schema (FOS v9.2.1):

  { "name" : "port_number", "type" : "string", "doc": "The slot/port number of the port", "default": ""},
- An SNMP FFDC file may result as part of firmware migration to or from FOS v9.2.1 when the switch or director chassis is managed by SANnav v2.3.1. The conditions necessary to encounter the FFDC are the FOS level on the standby CP or secondary partition lack SHA512 authentication support. There is no functional impact however FFDC generation message appears repeatedly.

Chapter 9: Security Vulnerability Fixes

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

FOS v9.2.1:

CVE-2024-29954

CVE-2024-29953

CVE-2022-25236

CVE-2022-25235

CVE-2023-26553

CVE-2023-26551

CVE-2019-6109

CVE-2023-3817

CVE-2023-3446

CVE-2023-2975

CVE-2023-2650

CVE-2023-0466

CVE-2023-0465

CVE-2023-0464

Chapter 10: Defects

10.1 Closed with Code Changes in FOS v9.2.1

Defect ID	Description
FOS-822366	cald terminated and kernel paniced during supportsave collections.
FOS-842564	The 7850 console is flooded with messages with string "cmicx_sbusdma_curr_op_details" affecting LAG and Ethernet port stats functionality.
FOS-846574	REST GET on /brocade-security/dh-chap-authentication-secret does not match CLI output.
FOS-847080	Switch supportsave collection from SANnav would fail
FOS-848121	On an X7 chassis with SX6 blades that have HA capable VE ports, the VE ports might occasionally toggle.
FOS-848228	Improper error message are displayed for invalid inputs to "framelog" command.
FOS-848422	HA Out of Sync due to SNMPd terminated in FOS upgrade HA window.
FOS-848703	If RSC is enabled on the switch, changing authspec fails
FOS-849473	Rest returns blank and/or error while switch has a large weblinker process.!
FOS-849642	Switch reported a flood of hardware errors, followed by daemons watchdog timeout and switch reboot. Sometimes these hardware errors also triggered port fault and/or blade fault. A raslog similar to this one should also be observed: [TO-1006], 1011618/1002267, FID 128, INFO, Switch_100, Flows destined to b1a02 device have been moved to PG_OVER_SUBSCRIPTION_4G_16G PG., cfs_ctrlr.c, line: 1470, comp:cfsd, ltime:2023/05/17-06:15:33:923058
FOS-849829	FICN-1056 (ERROR) RASLOG reported, but traffic not interrupted
FOS-849852	G610 fails to boot after power outage with reason "ERROR: can't get kernel image!"
FOS-849929	Weblinker dies with a large corefile and switch keeps going to "SNMP credentials invalid" state in SANnav.
FOS-851141	SNMP termination during swBootPromLastUpdated query and stuck rpm would be seen with ps exfcl output, such as: 0 0 29270 2413 20 0 0 0 exit Z ? 0:00 _ snmpd <defunct> 0 0 23760 1 20 0 5144 3304 - R ? 5531:10 rpm
FOS-851223	Switch run out of kernel memory and triggered deamon panic, cpu busy or port/blade fault.
FOS-851559	8Gb device slow to connect to 32G SFP on chassis.
FOS-852926	MAPS (module mdd) could go into a defunct state, and the state prevents MAPS from restarting, resulting in HA out of SYNC.
FOS-852945	Following FOS Upgrade from v9.1.01e to v9.1.1c X6 director SX-6 Blade showing still in progress
FOS-853249	cald process aborted due to memory resource not available.
FOS-853452	The memory corruption will result in mdd panic.
FOS-854143	Kernel panic when 64G oversubscription is introduced in the fabric with many neighbors on the same chip.

10.2 Open in FOS v9.2.1

Defect ID	Description
FOS-810530	Zone merge slow performance and failure on that switch that has defzone all access defined. Along with this behavior IPC drops RASLOGs events and/or termination of process nsd maybe seen.
FOS-845543	During HCL, observe RASlog ESS-2001 message followed by RASlog ESS-2002.
FOS-850500	User observes Fan kick starts and stays at a very high speed.
FOS-851800	Ipfilter rule getting added with start port number value when port range was configured with space between port range separator(eg: start_port - end_port instead of start_port-end_port).
FOS-852616	The IPS fabric does not process the fragmented frames and it will discard them. All ICMP requests discarded due to fragmentation are not counted in "portStatsShow" command output.
FOS-853425	IpsArpTable --show output is not in sync across the fabric for unresolved devices. The unresolved ARP device is only displayed on the domain where it's being learned.
FOS-854060	Syslogadmin: IPv6 Syslog server IP is logging even after IPv6 addresses are removed from the switch.
FOS-854348	"tsclockserver --set/tsclockserver" with FQDN succeeds even if configured DNS is unable to resolve the configured NTP Server FQDN to an IP address
FOS-854359	Tsclockserver: RAS TS-1002 is flooded on non-principal switches when an active NTP server goes offline.
FOS-854609	Adding default static route is throwing error. "There are max number of nexthop gateways for a given route already."

Revision History

Version	Summary of changes	Publication date
1.0	Initial version of document	12/20/2023
2.0	Updated section Brocade SANnav Management Portal Compatibility Added Syslog section under Security in Important Notes	02/21/2024
3.0	Editorial and stylistic changes.	03/05/2024
4.0	Updated disclosed CVEs for FOS v9.2.1 in Security Vulnerability Fixes. Correction in the table listing supported upgrade paths to Fabric OS v9.2.1 in Migrating to FOS v9.2.1.	04/19/2024


BROADCOM®