Brocade Fabric OS v7.4.0a Release Notes v3.0

August 26, 2015

Document History

Document Title	Summary of Changes	Publication Date
Brocade Fabric OS v7.4.0a Release Notes v1.0	Initial Release	May 29, 2015
Brocade Fabric OS v7.4.0a Release Notes v2.0	Add Appendix for FICON Environments, add defect 000554782 to the Closed With Code Change table, and add additional instructions for removing APM monitors under Obsoleted FOS Features section	July 17, 2015
Brocade Fabric OS v7.4.0a Release Notes v3.0	Add an item under Extension section of the Important Notes Add base defect tables from FOS7.4.0 release notes	August 26, 2015

Contents

Overview

FOS v7.4.0a is a patch release based on FOS v7.4.0. All hardware platforms and features supported in FOS v7.4.0 are also supported in FOS v7.4.0a. Besides defect fixes, FOS v7.4.0a adds support for following existing hardware and enhancement.

- Brocade Encryption Switch (BES) and FS8-18 blade
- E-port connections between two FC16-64 blades

New Hardware Support

Brocade Fabric OS v7.4 does not introduce support for any new hardware platforms. FOS v7.4 adds support for the following new hardware:

- Brocade-branded 4GB external USB flash drive

Summary of New Software Features

FOS v7.4 includes support for many new software features and enhancements including:

- IP Extension features for Brocade 7840
- FCIP enhancements for Brocade 7840
- MAPS (Monitoring and Alerting Policy Suite) enhancements
- Flow Vision enhancements
- ClearLink Diagnostics (D_Port) enhancements
- Peer Zoning support
- Target Driven Zoning support
- Lossless DLS enhancement
- FCR enhancements
- Security enhancements
- Time Server enhancements
- SNMP enhancements
- RDP Enhancements
- Firmware download enhancements
- RAS enhancements
- Zoning enhancements
- FICON enhancements
- Miscellaneous enhancements

Obsoleted FOS Features

The following features supported in FOS v7.3 and earlier releases are obsolete beginning with FOS v7.4:

- Fabric Watch
- Advanced Performance Monitoring (APM)

Users running Fabric Watch for switch monitoring in FOS v7.3 are advised to convert to MAPS monitoring before upgrading to FOS v7.4. Converting Fabric Watch to MAPS before upgrading to FOS v7.4 can preserve Fabric Watch threshold configurations. If users choose to upgrade to FOS v7.4 without converting to MAPS, Fabric Watch will stop functioning after the firmware upgrade and the Fabric Watch thresholds cannot be automatically migrated for use by MAPS. Please refer to the Fabric OS MAPS Administrator's Guide for step-by-step migration instructions.

Users running APM in FOS v7.3 are required to remove all monitors before upgrading to FOS v7.4 by using the following commands:

1. Enter perfdeleemonitor to remove all End-to-end monitors.
2. Enter perfcfgsave to save this change.
3. Enter fmmonitor --delmonitor to remove all filter monitors.
4. Enter fmmonitor --delete *frametype* to remove the specified user-defined frametype.
5. Enter perfttmon --delete to remove all switch level Top Talker monitors.
6. Enter perfttmon --delete fabricmode to remove fabric mode Top Talker monitors.

After upgrading to FOS v7.4, the APM monitors will stop functioning. Users can use the Flow Vision features as part of Fabric Vision for performance monitoring. Please refer to the Fabric OS Flow Vision Administrator's Guide for detailed instructions on removing APM monitors and Flow Vision feature configurations.

Brocade Fabric Vision licenses are required for MAPS and Flow Vision. The combination of Brocade Fabric Watch license and Brocade APM license enables the MAPS and Flow Vision features. For switches with only Fabric Watch licenses or only APM licenses, users can acquire and install the missing license to acquire MAPS and Flow Vision features.

New Feature Descriptions

New Hardware Support

FOS v7.4 adds support for the following new hardware:

- Brocade-branded 4GB external USB flash drive

IP Extension features for Brocade 7840

FOS v7.4 introduces IP Extension support for the Brocade 7840. Users can use this capability to extend IP storage for replication and disaster recovery in much the same way as Fibre Channel storage while taking advantage of the compression, encryption, QoS, and trunking features available in the Brocade 7840.

A Brocade 7840 running FOS v7.4 can support both FCIP Extension and IP Extension at the same time. IP Extension includes the following:

- Support for system configuration for IP Extension
- Support for GbE port configuration for IP Extension
- Tunnel configuration for IP Extension
- Adaptive Rate Limiting
- TCP/IP Features
- Traffic Control List

Support System Configuration for IP Extension

FOS v7.4 supports users configuring Brocade 7840 for both FCIP Extension and IP Extension (hybrid mode). By default, Brocade 7840 supports FCIP Extension only. Changing a Brocade 7840 between FCIP-only and hybrid mode requires a switch reboot.

Support GE Port Configuration for IP Extension

FOS v7.4 supports users configuring the front end 1/10 GbE ports as LAN ports on a Brocade 7840 for hybrid mode. These ports are used to connect to IP storage devices on the LAN side. FOS v7.4 supports static Link Aggregation Group (LAG) configuration so that multiple LAN ports can be assigned to the same LAG group.

Tunnel configuration for IP Extension

FOS v7.4 supports user configuration of IP tunnels on a Brocade 7840 in the same way as FC tunnels are configured. IP tunnels and FC tunnels are all represented under virtual E-port (VE). Each VE is configured as a FC-only tunnel or as both FC and IP tunnels. Trunking, QoS, and compression are supported on IP tunnels as they are for FC tunnels.

Adaptive Rate Limiting (ARL)

FOS v7.4 supports all ARL features available on the FCIP Extension for IP Extension. The static distribution of unused bandwidth is hierarchical.

TCP/IP Features

FOS v7.4 supports the following TCP/IP features for IP Extension.

- LAN side jumbo frames
- IPv4 and IPv6 for LAN side
- Maximum 512 TCP connections per Data Processor (DP)
- Maximum 512 TCP open requests per second per DP
- Maximum 64 UDP flows per DP
- DSCP/VLAN L2CoS marking
- Segment Preservation
- Each LAN TCP window will be 64K by default. If TCP window scaling is requested, the maximum advertised window is 256K. The maximum window per connection is 2M irrespective of the advertised window.

- Untagged and single tagged packets are supported.
- Stacked/double (IEEE 802.1ad) tagged packets from hosts are not supported. Packets will be dropped.

Traffic Control List

FOS v7.4 supports Traffic Control List (TCL) to manage and route IP flows. Each TCL is identified by a unique user configured name. FOS v7.4 supports maximum 128 TCLs. System generated default TCL will drop all the incoming packets.

FCIP Enhancements to Brocade 7840

Base Switch Support for 7840

FOS v7.4 enhances Virtual Fabric support on 7840 switches to include the base switch, i.e., to support XISL. Users can configure E_port (ISL over FC), EX_port (IFL over FC), and VE_port (ISL over GE) in base switch. The maximum number of logical switches supported — including the base switch — remains four.

FCIP Hot Code Load (HCL)

FOS v7.4 enhances FCIP HCL support in the following conditions, which were excluded in FOS v7.3.

- Support concurrent FCIP HCL on all 7840 switches in the configuration
- Support multiple sites for FCIP HCL

Monitoring and Alerting Policy Suite (MAPS) Enhancements

FOS v7.4 has a number of important MAPS feature enhancements. These include:

- Basic monitoring without Fabric Vision license
- Monitor NPIV device login limits
- Monitor backend ports
- Monitor FCIP circuit QoS
- Monitor FCIP circuit RTT and jitter on Brocade 7800 and FX8-24 blade
- Fabric Performance Impact monitoring enhancement
- Slow drain device quarantine action for Fabric Performance Impact monitoring
- Port toggle action
- FICON notification action
- Alert quiet time support
- Usability enhancements

Monitoring without Fabric Vision license

FOS v7.4 introduces a new basic monitoring capability in MAPS. The basic monitoring capability allows end users without Fabric Vision licenses on their switches to use MAPS to monitor overall switch status, FRU health, and switch resource categories under the new pre-defined MAPS policy dflt_base_policy.

Monitor NPIV device login limits

FOS v7.4 introduces MAPS monitoring of NPIV login limits. FOS has limits on the number of NPIV devices that can login to a physical F_port. MAPS monitors the percentage of logged in NPIV devices relative to the maximum number of NPIV logins allowed on the F_port to alert users before the limit is reached.

Monitor backend ports

FOS v7.4 introduces back-end port error monitoring in MAPS. Users can take early recovery actions if any of the monitored back-end errors have crossed specified thresholds. Typical recovery actions include SerDes tuning on a switch or reseating blades. For detailed instructions on these actions, please contact your support provider for additional assistance.

Monitor FCIP circuit QoS

FOS v7.4 enhances FCIP QoS monitoring in MAPS to add monitoring of Fibre Channel QoS parameters at circuit level. The circuit QoS monitoring combined with the tunnel QoS monitoring available since FOS v7.3 provides additional granularity to monitor the FCIP link performance.

Monitor FCIP circuit RTT and jitter on 7800 and FX8-24

MAPS monitors circuit round trip time (RTT) and jitter statistics in FOS v7.3 on Brocade 7840. FOS v7.4 supports these two FCIP circuit monitoring elements on Brocade 7800 and FX8-24 blade so that they are available to 8G FC extension platforms.

Fabric Performance Impact monitoring enhancement

FOS v7.4 enhances Fabric Performance Impact (FPI) monitoring to add a new IO_LATENCY_CLEAR state so that end users can receive notification when latency conditions are cleared. FOS v7.4 enhances FPI monitoring by adding latency counter monitoring on all ports to detect potential transient spikes of latency conditions. In addition, FOS v7.4 moves port TX, RX, and UTIL monitoring systems to the FPI category from the Port Health category in FOS v7.3 and earlier releases so that all potential congestion conditions are reported under the FPI category.

Slow drain device quarantine action for Fabric Performance Impact monitoring

FOS v7.4 introduces a new MAPS action that automatically isolates slow drain devices when they are detected by FPI monitoring. This frees up buffer credits for normal devices that are sharing the same links and mitigates the effect due to presence of slow drain devices in the fabric.

Port toggle action for Fabric Performance Impact monitoring

FOS v7.4 introduces Port Toggle as an action which automatically recovers slow drain device conditions when they are detected by FPI monitoring. A port toggle, (which is a port disable followed by a port enable) can recover the ports from some slow drain device conditions or force traffic failover to an alternate path.

FICON notification action

FOS v7.4 introduces FICON notification as a new action that enables MAPS events to be sent to FMS with detailed event information upon rule violations. FMS CUP can translate these MAPS events into FICON-specific Health Summary Check reports.

Alert quiet time support

FOS v7.4 introduces a quiet time support for RASLOG and EMAIL alert actions. This feature allows end users to configure within a rule a period of time not to receive duplicated alerting actions after the first alert has already been sent.

Usability enhancements

FOS v7.4 has a number of usability enhancements to MAPS. These include:

- Allow *none* to be used as an email address to clear previously configured email addresses in the CLI command *mapsconfig*.
- Enhanced Temperature Sensor monitoring so that actions are triggered on change of Temperature Sensor (TS) states.
- Modified FRU monitoring so that the states being monitored are more accurate and useful for operations.
- An upper limit to the number of rules that can be created in a policy. The maximum number of rules in a policy is dependent on the character length of each rule name.

Flow Vision Enhancements

FOS v7.4 provides the following enhancements to Flow Vision:

All F_Port Flow Monitoring

FOS v7.4 introduces a system predefined learning flow named sys_mon_all_fports to monitor performance on all F_ports in a switch. Flow learning on all F_ports provides a continuous, automatic, and comprehensive view of application traffic patterns for all device connections.

Scalability Improvement

FOS v7.4 increases the scalability limit supported by Flow Vision. In particular, the total number of sub-flows supported by chassis switches is increased to 2048 and by fixed port switches is increased to 512.

Identify All Devices in a Flow

FOS v7.4 supports displaying all zoned devices in a flow by introducing a new option -allzoned to the Flow Vision command. This will identify all zoned devices for a flow defined on an E_Port or F_Port.

Fabric Flow Dashboard

FOS v7.4 introduces support of a Flow Dashboard that provides information for a flow from all the available data points in the fabric through which it can pass. With all relevant data summarized for a flow of interest, users are able to more easily troubleshoot and identify the root cause of various issues that may occur.

ClearLink Diagnostic (D_Port) Enhancements

FOS v7.4 implements the following D_Port feature enhancements.

Link Power (dB) Loss Calculation

FOS v7.4 supports calculating TX and RX power loss of a link with D_Port tests. D_Port tests include the power loss calculation to provide additional details on the health of physical media of links.

Dynamic D_Port and On-demand D_Port with DWDM

FOS v7.4 enhances D_port pre-provision feature to allow administrators to pre-provision certain ports connected to DWDM links. With the pre-provisioned list, dynamic D_port and on-demand D_port tests can start automatically on those ports with the optical loopback test skipped.

CLI Command Hierarchical Help Display

FOS v7.4 enhances the help page for D_port CLI commands so that only the relevant sub-options are displayed when a command action is specified for the portCfgDport and portDportTest commands.

Peer Zoning Support

FOS v7.4 introduces support for Peer Zoning as defined in the FC-SW-6 and FC-GS-7 standard. In a Peer Zone configuration, membership in a zone is differentiated into principal members and non-principal or peer members. Peer Zoning configuration allows communication between a principal member and any peer member but does not allow communication between two peer members or between two principal members. By adopting Peer Zoning, users can simplify zoning configuration and management, improve performance, and increase scalability.

Target Driven Zoning support

FOS v7.4 introduces the Target Driven Zoning feature that allows end devices to create Peer Zone configurations through inband commands. This feature enables zoning to be configured by management software on storage devices and reduces the manual configuration needed on switches.

Lossless DLS enhancement

FOS v7.4 introduces a routing enhancement to support lossless Dynamic Load Sharing (DLS) in a 2-hop topology. This enhancement allows adding links or switches in existing paths that are up to 2 hops between a host and a target, including the new link that is coming online, to ensure lossless and in-order frame delivery.

FCR enhancements

FOS v7.4 has a number of enhancements in FCR. These enhancements include:

Location Embedded LSAN zone

FOS v7.4 introduces the location-embedded LSAN zone feature. A location-embedded LSAN zone specifies in the LSAN zone name the remote fabric ID that shares devices. The corresponding FCR switch will use this information in the LSAN zone names to store only these entries for the locally connected edge fabric. As a result. users are now able to configure more LSAN zones across a backbone fabric.

Increase Number of Imported Proxy Devices

FOS v7.4 increases the maximum number of proxy devices that can be imported into each edge fabric to 4000. This limit applies to the cumulative number of all proxy devices created on all translate domains in the edge fabric. FOS versions prior to v7.4 support 2000 proxy devices as the limit for this number.

Sort WWNs in *lsanzoneshow* CLI

FOS v7.4 supports sorting WWNs in the CLI command lsanzoneshow output. A new -o or -sort option is added to the CLI command to display entries in sorted order by WWNs for each LSAN zone listing.

Support Port Range for *portcfgexport* and *portcfgvexport* CLI

FOS v7.4 supports port range as input parameters for the portcfgexport and portvexport CLI commands so that multiple ports can be configured as EX-port or VEX-port at the same time.

Support Peer Zoning with FCR

FOS v7.4 supports Peer Zoning in LSAN zones if users have configured a peer zone in an edge fabric. Peer zoning rules and RSCN distribution will be enforced by edge fabric switches.

Support New Domain ID Range for Front and Translate Phantom Domains

FOS v7.4 supports assigning for an FCR the front domain ID in the range of 160 through 199 and the translate domain ID in the range of 200 through 239. Users can use the CLI command *fcrConfigure --resetPhantomDomain* to use the new range to avoid conflicting with the real switch domain IDs.

Security Enhancements

FOS v7.4 has a number of important security enhancements:

Obfuscation of RADIUS Shared Secrets

FOS v7.4 supports obfuscation of the RADIUS shared secrets so that they are not stored as plaintext. With this option, stored shared secrets are not visible as plaintext in configUpload files and SupportSave files.

Import/Export Syslog Server Certificates

FOS v7.4 adds the support of importing and exporting a syslog server certificate to support syslog over TLS. A syslog server CA certificate can be imported from a remote host or exported to a remote host.

Password Policy Enhancement for Root Password Change

FOS v7.4 adds a new option in the switch account password policy to allow root password change by root account login sessions without prompting for the existing (old) password.

secCryptoCfg CLI Command

FOS v7.4 supports a new CLI secCryptoCfg command to configure the set of acceptable cryptographic algorithms for the SSH and HTTPS protocols on a switch. Administrators can use this new CLI command to mandate various cryptographic algorithms conform to their policies.

Default Account Password Change

FOS v7.4 modifies the behavior of default switch account password change. Login to admin account would only prompt changes to the default admin and user account passwords. The default root and factory account passwords change would only be prompted when login to the switch as root.

Time Server Enhancements

FOS v7.4 enhances Time Server to support Network Time Protocol (NTP) server configuration distribution to Access Gateway switches. This enhancement allows AGs, including cascaded AG connections, to receive the same NTP server configuration from a connected fabric.

SNMP Enhancements

FOS v7.4 implements the following SNMP enhancements.

Log Messages for SNMPv3 Authentication

FOS v7.4 logs SNMP authentication success and failure as audit log messages to track the authentication results for SNMPv3 requests.

SNMPv3 Individual Inform Tag

FOS v7.4 enhances SNMPv3 configuration to allow SNMP informs to be enabled or disabled at individual receiver host level. With this enhancement, users can configure some receivers to get SNMP informs, while other receivers get SNMP traps.

Disable SNMP Write Access

FOS v7.4 changes the default SNMP configuration to have SNMP write disabled. This affects the default switch configuration loaded with FOS v7.4 on a new switch from factory.

Obsoletes Fabric Watch and Advanced Performence Monitoring MIBs

FOS v7.4 obsoletes the following MIBs associated with Fabric Watch and Advanced Performance Monitoring feature: swFwSystem, swBlmPerfMnt, swTopTalker.

RDP Enhancements

FOS v7.4 enhances the Read Diagnostic Parameter (RDP) support which includes the following:

- Enable polling to refresh RDP data cache at a default 4 hour interval.
- Include signal power loss information in the *sfpShow --link* or *sfpShow --pid* options.
- Include corrected and uncorrected FEC blocks in *portShow --link* or *portShow --pid* options.

Firmware Download Enhancements

FOS v7.4 introduces the following important enhancements for firmware download.

Staged Firmware Download

FOS v7.4 supports staged firmware download so that users can download firmware package to a switch first and choose to install and activate the downloaded firmware at a later time.

Firmware Clean Installation

FOS v7.4 supports firmware clean installation. This installs a firmware package without retaining the existing configuration or maintaining HA. With this feature, customers receiving a new switch from factory can install firmware in a single step to the desired version that their networks are running, without going through multiple steps of non-disruptive firmware download.

Firmware Auto Sync Enhancement

FOS v7.4 enhances the firmware auto sync feature to support automatic synchronization of firmware versions on a standby CP with a version different from the active CP. If an active CP runs FOS v7.4 or higher:

- A standby CP with firmware version as early as FOS v6.4 can be upgraded automatically.
- A standby CP with firmware version later than FOS v7.4 can be downgraded automatically.

Firmware Integrity Check

FOS v7.4 introduces a firmwareCheck CLI command to check the integrity of firmware packages already installed on the switch. If any of the files or packages as part of firmware has been changed, the firmware integrity check will fail and notify users which package has failed the check.

Challenge-Response Authentication

FOS v7.4 introduces support for SSH servers configured with "keyboard-interactive" as defined in IETF RFC 4256 as authentication method to be used with SCP or SFTP for firmware download, support save, and config upload/download commands. With this SSH server configuration, FOS v7.4 only supports account passwords as a form of challenge-response authentication.

RAS Enhancements

FOS v7.4 supports the following RAS enhancements:

WWN Card Replacement Enhancements

FOS v7.4 enhances the procedure for field replacement of WWN cards in chassis based systems. WWN cards are chassis FRUs that contain chassis WWNs and other information. Each chassis has two WWN cards for redundancy. FOS v7.4 enhances WWN card handling so that certain error or data corruptions associated with WWN cards can be recovered in the field.After users replace a single defective WWN card with a new one, some data can be restored from the current/non-defective WWN card to the newly replaced WWN card. In addition, the system periodically checks the integrity of the WWN cards and logs RASLOG error messages if problems are detected.

Show RASLOG Messages within a Timeframe

FOS v7.4 adds options to errdump and errshow CLI command so that only RASLOG messages within the specified beginning and end time will be shown, instead of all RASLOG messages.

Audit Log Enhancements

FOS v7.4 enables audit log by default for all classes of messages. FOS v7.4 increases the maximum number of audit log messages stored on a switch to 1024 from 256.

Clihistory Identify Command Virtual Fabric FID

FOS v7.4 enhances cliHistory so that FID contexts will be shown along with the command line. With this enhancement, clihistory in a support save file includes the FID information for support and debug usage.

Zoning Enhancements

FOS v7.4 adds the following enhancements to standard zoning to simplify zoning configuration:

List Zones with Specific Alias

FOS v7.4 adds support to zoneshow command to display only the zone configurations that match a given alias instead of the entire zone database. Administrators can use this enhancement to quickly locate certain zone configurations that contain a specific alias or alias prefix.

Sort zoneShow Command Output by WWN

FOS v7.4 enhances the *zoneShow --sort* command output in sorted order for both (D,I) and WWN members.

Indicate offline members in zoneShow output

FOS v7.4 provides a new option *--validate* to the zoneshow command to indicate members in the configuration but not online in the fabric. Administrators can use this enhancement to quickly discover the online and offline members in a zone configuration.

Traffic Isolation (TI) Zoning Enforcement enhancement

FOS v7.4 enhances TI zoning rule enforcement so that devices connected to the same local switch are also enforced by the TI zoning rule.

TI Failover Disabled Zone Message

FOS v7.4 adds a RASLOG message ZONE-1060 to warn users if the TI zone dedicated path is the only path available between two domain IDs.

FICON Enhancements

FOS v7.4 adds the following FICON related enhancements :

MAPS notification to FMS CUP

FOS v7.4 supports a new MAPS FICON notification action. With this action, MAPS rule violations can trigger notifications to the FMS host as Health Summary Code reports.

ConfigUpload and ConfigDownload of FMS Mode

FOS v7.4 enhances configUpload and configDownload to ensure that a configDownload can turn ON the FMS mode in a logical switch that had FMS mode OFF.

D_Port Support in Port Descriptor

FOS v7.4 reports the state of an FC port in D_Port mode to the HOST with the Port Information Block (PIB).

Miscellaneous Enhancements

Login to Logical Switch IP

FOS v7.4 enhances Logical Switch IP address support so that logins using the logical switch IP address automatically set the user VF context to the logical switch associated with the IP address.

Dynamic Switch Port Names

FOS v7.4 introduces a dynamic port name feature to automatically assign port names on a switch based on a default standard format and port types. Users can enable and disable the “Dynamic port name feature” with the configure CLI command.

Port Index Support for CLI Command portErrShow and portTestShow

FOS v7.4 enhances the portErrShow and portTestShow command to support port index as inputs, in addition to the existing slot/port as input.

Link Reset on Loss of Sync

FOS v7.4 enhances credit recovery on backend links for 8G platforms by performing link reset (LR) on loss of sync (LOS) events. This enhancements applies to a port where a loss of sync is detected and the peer port of the backend link is on a 8G platform.

Enhance switchShow CLI Output

FOS v7.4 modifies switchshow -portname command output to display the port PWWN of the switch ports along with the port names.

portLoginShow Command with History Option

FOS v7.4 enhances the portLoginShow CLI to display details of the device that last logged out from a port. This enhancement supports the port login types of “fe” for FLOGI devices and “fd” for FDISC devices. Users can use the -history option to show the device logout information.

Port Peer Beacon Support EX-Port

FOS v7.4 enhances port peer beacon (LCB) feature to support links with EX-ports.

BufOpMode for FC Gen5 Blades

FOS v7.4 adds support of Buffer Optimization Mode (BufOpMode) for FC Gen5 core blades and port blades. The BufOpMode enables non-local switching in an edge ASIC chip where both E-port and F-port exist.

portStatsShow Command Display TXQ Latency

FOS v7.4 enhances the portStatsShow CLI command to display the ASIC transmit queue (TXQ) latency information for each virtual channel (VC).

Support De-bouncing of Loss of Signal for Fixed Speed and Auto Negotiate Ports

FOS v7.4 expands loss of signal de-bouncing for both fixed-speed and auto-negotiated ports in any port state. FOS v7.4 adds a “mode 2” option for the portcfglosstov CLI command to enable for both fixed-speed ports and auto-negotiate ports.

Backend Link Failure Blade Fault Option

FOS v7.4 enhances back-end link failure handling. With this enhancement, when back-end link failure is detected, the link is re-initialized first and the blade is faulted only when re-initialization fails. In addition, a blade would not be faulted if there is another online port within the trunk.

DLS Support on Embedded Switches

FOS v7.4 supports DLS on the embedded platforms. Earlier FOS versions do not support dynamic load sharing (DLS) on the FC embedded platforms.

New portChannelShow CLI Command

FOS v7.4 adds a CLI command portChannelShow to display a DPS group for one or all reachable domains.

Support preserving port2area and area2port mappings with configUpload and configDownload

FOS v7.4 supports uploading and downloading the port2area and area2port mapping tables in a configuration file for all logical switches in a chassis through the new -map option with the existing configUpload and configDownload CLI command.

Optionally Licensed Software

Fabric OS v7.4 includes all basic switch and fabric support software, as well as optionally licensed software that is enabled via license keys.

Optionally licensed features include:

Brocade Ports on Demand — Allows customers to instantly scale the fabric by provisioning additional ports via license key upgrade. (Applies to select models of switches).

Brocade Extended Fabrics — Provides greater than 10km of switched fabric connectivity at full bandwidth over long distances (depending on platform this can be up to 3000km).

Note: If a port on 16G FC blades or a 16G switch is configured to operate at 10G speed, Extended fabrics license is not needed to enable long distance connectivity on that port.

Brocade ISL Trunking — Provides the ability to aggregate multiple physical links into one logical link for enhanced network performance and fault tolerance. Also includes Access Gateway ISL Trunking on those products that support Access Gateway deployment.

Brocade Advanced Performance Monitoring — All Advanced Performance Monitoring features are obsolete in FOS v7.4. This license remains to provide end users with Fabric Watch license to upgrade to Fabric Vision capabilities.

Brocade Fabric Watch — All Fabric Watch features are obsolete in FOS v7.4. This license remains to provide end users with Advanced Performance Monitoring license to upgrade to Fabric Vision capabilities.

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

FICON Management Server — Also known as "CUP" (Control Unit Port), enables host-control of switches in Mainframe environments.

Enhanced Group Management — This license enables full management of devices in a data center fabric with deeper element management functionality and greater management task aggregation throughout the environment. This license is used in conjunction with Brocade Network Advisor application software and is applicable to all FC platforms supported by FOS v7.0 or later.

Note: This capability is enabled by default on all Gen 5 65XX model switches and DCX 8510 platforms, and on DCX and DCX-4S platforms that are running Fabric OS v7.0.0 or later. Gen 5 embedded switches receive this capability by default with FOS v7.2.1 and later. Individual upgrade is required when upgrading directly to FOS v7.2.1 on Gen 5 embedded switches. Subsequent group operations on Gen 5 embedded switches including group upgrade are supported.

Adaptive Networking with QoS — This license was deprecated beginning with FOS v7.2. All functionality enabled by the license is now part of base FOS firmware capabilities.

Server Application Optimization — This license was deprecated beginning with FOS v7.2. All functionality enabled by the license is now part of base FOS firmware capabilities.

Integrated Routing — This license allows any port in a DCX 8510-8, DCX 8510-4, Brocade 6510, Brocade 6520, DCX-4S, DCX, 5300, 5100, 7800, 7840, or Brocade Encryption Switch to be configured as an Ex_port or VEx_port (on some platforms) supporting Fibre Channel Routing.

Encryption Performance Upgrade — This license provides additional encryption processing power. For the Brocade Encryption Switch or a DCX/DCX-4S/DCX 8510-8/DCX 8510-4, the Encryption Performance License can be installed to enable full encryption processing power on the BES or on all FS8-18 blades installed in a DCX/DCX-4S/DCX 8510-8/DCX 8510-4 chassis.

DataFort Compatibility — This license is required on the Brocade Encryption Switch or DCX/DCX-4S/DCX 8510-8/DCX 8510-4 with FS8-18 blade(s) to read and decrypt NetApp DataFort-encrypted disk and tape LUNs. DataFort Compatibility License is also required on the Brocade Encryption Switch or DCX/DCX-4S/DCX 8510-8/DCX 8510-4 Backbone with FS8-18 Encryption Blade(s) installed to write and encrypt the disk and tape LUNs in NetApp DataFort Mode (Metadata and Encryption Algorithm) so that DataFort can read and decrypt

these LUNs. DataFort Mode tape encryption and compression is supported beginning with the FOS v6.2.0 release on DCX platforms. Availability of the DataFort Compatibility license is limited; contact your vendor for details.

Advanced Extension — This license enables two advanced extension features: FCIP Trunking and Adaptive Rate Limiting. The FCIP Trunking feature allows multiple IP source and destination address pairs (defined as FCIP Circuits) via multiple 1GbE or 10GbE interfaces to provide a high bandwidth FCIP tunnel and failover resiliency. In addition, each FCIP circuit supports four QoS classes (Class-F, High, Medium and Low Priority), each as a TCP connection. The Adaptive Rate Limiting feature provides a minimum bandwidth guarantee for each tunnel with full utilization of the available network bandwidth without impacting throughput performance under high traffic load. This license is available on the 7800, 7840, and the DCX/DCX-4S/DCX 8510-8/DCX 8510-4 for the FX8-24 on an individual slot basis.

10GbE FCIP/10G Fibre Channel — This license enables the two 10GbE ports on the FX8-24 and/or the 10G FC capability on FC16-xx blade ports supported on DCX 8510 platforms except for the FC16-64 blade. On the Brocade 6510, Brocade 6520 this license enables 10G FC ports. This license is not applicable to Brocade 7840 or Brocade 6505.

On FX8-24:

With this license installed and assigned to a slot with an FX8-24 blade, two additional operating modes (in addition to 10 1GbE ports mode) can be selected:

- 10 1GbE ports and 1 10GbE port, or
- 2 10GbE ports

On FC16-xx:

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

On Brocade 6510, Brocade 6520:

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

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

Advanced FICON Acceleration — This licensed feature uses specialized data management techniques and automated intelligence to accelerate FICON tape read and write and IBM Global Mirror data replication operations over distance, while maintaining the integrity of command and acknowledgement sequences. This license is available on the 7800, 7840, and the DCX/DCX-4S/DCX 8510-8/DCX 8510-4 for the FX8-24 on an individual slot basis.

7800 Port Upgrade — This license allows a Brocade 7800 to enable 16 FC ports (instead of the base four ports) and six GbE ports (instead of the base two ports). This license is also required to enable additional FCIP tunnels and also for advanced capabilities like tape read/write pipelining.

ICL 16-link, or Inter Chassis Links — This license provides dedicated high-bandwidth links between two Brocade DCX chassis, without consuming valuable front-end 8Gb ports. Each chassis must have the 16-link ICL license installed in order to enable the full 16-link ICL connections. (Available on the DCX only.)

ICL 8-Link — This license activates all eight links on ICL ports on a DCX-4S chassis or half of the ICL bandwidth for each ICL port on the DCX platform by enabling only eight links out of the sixteen links available. This allows users to purchase half the bandwidth of DCX ICL ports initially and upgrade with an additional 8-link license to utilize the full ICL bandwidth at a later time. This license is also useful for environments that wish to create ICL connections between a DCX and a DCX-4S, the latter of which cannot support more than 8 links on an ICL port. Available on the DCX-4S and DCX platforms only.

ICL POD License — This license activates ICL ports on core blades of DCX 8510 platforms. An ICL 1st POD license only enables half of the ICL ports on CR16-8 core blades of DCX 8510-8 or all of the ICL ports on CR16-4 core blades on DCX 8510-4. An ICL 2nd POD license enables all ICL ports on CR16-8 core blades on a DCX 8510-8 platform. (The ICL 2nd POD license does not apply to the DCX 8510-4.)

Enterprise ICL (EICL) License — The EICL license is required on a Brocade DCX 8510 chassis when that chassis is connected to four or more Brocade DCX 8510 chassis via ICLs either as ISLs or IFLs.

This license requirement does not depend upon the total number of DCX 8510 chassis that exist in a fabric, but only on the number of other chassis connected to a DCX 8510 via ICLs. This license is recognized/displayed when operating with FOS v7.0.1 but enforced with FOS v7.1.0 or later.

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

WAN Rate Upgrade 1 License — The WAN Rate Upgrade 1 license provides the additional WAN throughput up to 10 Gbps on Brocade 7840. The base configuration of Brocade 7840 without the WAN Rate Upgrade 1 license provides WAN throughput up to 5 Gbps.

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

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

Temporary License Support

The following licenses are available in FOS v7.4 as Universal Temporary or regular temporary licenses:

- Fabric (E_Port) license
- Extended Fabric license
- Trunking license
- High Performance Extension license
- Advanced Performance Monitoring license (feature not supported)
- Fabric Watch license (feature not supported)
- Integrated Routing license
- Advanced Extension license
- Advanced FICON Acceleration license
- 10GbE FCIP/10GFibre Channel license
- FICON Management Server (CUP)
- Enterprise ICL license
- Fabric Vision license
- WAN Rate Upgrade 1 license
- WAN Rate Upgrade 2 license

Note: Temporary Licenses for features available on a per slot basis enable the feature for any and all slots in the chassis.

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

Supported Switches

FOS v7.4 supports the following platforms:

- 300, 5100, 5300, 7800, VA-40FC, Brocade Encryption Switch, DCX, DCX-4S
- 6510, 6505, 6520, 7840, DCX 8510-8, DCX 8510-4
- FC8-16, FC8-32, FC8-48, FC8-64, FX8-24, FS8-18, FCOE10-24
- FC16-32, FC16-48, FC16-64, FC8-32E, FC8-48E
- 5410, M5424, 5430, 5431, 5432, 5450, 5460, 5470, 5480, NC-5480
- 6545, 6546, 6547, 6548, M6505

Access Gateway mode is also supported by Fabric OS v7.4, and is supported on the following switches: the Brocade 300, 5100, VA-40FC, 5410, 5430, 5431, 5432, 5450, 5460, 5470, 5480, NC-5480, M5424, 6545, 6546, 6547, 6548, M6505, 6510, 6505.

Standards Compliance

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

The FCOE10-24 blade conforms to the following Ethernet standards:

- IEEE 802.1D Spanning Tree Protocol
- IEEE 802.1s Multiple Spanning Tree
- IEEE 802.1w Rapid reconfiguration of Spanning Tree Protocol
- IEEE 802.3ad Link Aggregation with LACP
- IEEE 802.3ae 10G Ethernet
- IEEE 802.1Q VLAN Tagging
- IEEE 802.1p Class of Service Prioritization and Tagging
- IEEE 802.1v VLAN Classification by Protocol and Port
- IEEE 802.1AB Link Layer Discovery Protocol (LLDP)
- IEEE 802.3x Flow Control (Pause Frames)

The following draft versions of the Converged Enhanced Ethernet (CEE) and Fibre Channel over Ethernet (FCoE) Standards are also supported on the FCOE10-24 blade:

- IEEE 802.1Qbb Priority-based Flow Control
- IEEE 802.1Qaz Enhanced Transmission Selection
- IEEE 802.1 Working Group) DCB Capability Exchange Protocol (Proposed under the DCB Task Group of IEEE 802.1
- FC-BB-5 FCoE (Rev 2.0)

Technical Support

Contact your switch supplier for hardware, firmware, and software support, including product repairs and part ordering. To expedite your call, have the following information immediately available:

1. General Information

Technical Support contract number, if applicable

Switch model

Switch operating system version

Error numbers and messages received

supportSave command output and associated files

For dual CP platforms running FOS v6.2 and above, the supportsave command gathers information from both CPs and any AP blades installed in the chassis

Detailed description of the problem, including the switch or fabric behavior immediately following the problem, and specific questions

Description of any troubleshooting steps already performed and the results

Serial console and Telnet session logs

Syslog message logs

2. Switch Serial Number

   The switch serial number is provided on the serial number label, examples of which are shown here:

   The serial number label is located as follows:

Brocade Encryption Switch, VA-40FC, 300, 5100, 5300, 6510, 6505, 6520 — On the switch ID pull-out tab located on the bottom of the port side of the switch

Brocade 7800, 7840 — On the pull-out tab on the front left side of the chassis underneath the serial console and Ethernet connection and on the bottom of the switch in a well on the left side underneath (looking from front)

Brocade DCX, DCX 8510-8 — Bottom right of the port side

Brocade DCX-4S, DCX 8510-4 — Back, upper left under the power supply

3. World Wide Name (WWN)

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

   If you cannot use the **wwn** command because the switch is inoperable, you can get the primary WWN from the same place as the serial number, except for the Brocade DCX/DCX-4S and DCX 8510-8/DCX 8510-4. For the Brocade DCX/DCX-4S and DCX 8510-8/DCX 8510-4 access the numbers on the WWN cards by removing the Brocade logo plate at the top of the non-port side. The WWN is printed on the LED side of both cards.

4. License Identifier (License ID)

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

   Use the **licenseIdShow** command to display the License Identifier.

FOS Migration Considerations

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

FOS Upgrade and Downgrade Special Considerations

DCX/DCX-4S/DCX8510-8 units with FCOE10-24 blades running any FOS v7.3.x can be non-disruptively upgraded to FOS v7.4.0a. This upgrade is non-disruptive to both FC and FCoE traffic (when using FCOE10-24 blades). In FOS versions prior to v7.1.0, firmware upgrade is disruptive to FCoE traffic.

Any firmware activation on Brocade 7800, or DCX, DCX-4S, DCX 8510-8, DCX 8510-4 with FX8-24 will disrupt I/O traffic on the FCIP links.

For FCIP, the best practice is to always operate the switch or blade at both ends of the tunnel with the same level of Fabric OS, down to the maintenance release. Fabric OS upgrades should be done on both ends of the FCIP tunnel concurrently.

Firmware downgrade from FOS v7.4 to FOS v7.3.0c or earlier verisons on Brocade 7840 should be avoided. Otherwise, the Brocade 7840 may become faulty. (Downgrading to FOS v7.3.0b5 can be used as a workaround.)

Disruptive upgrades to Fabric OS v7.4.0a are allowed and supported from FOS v7.2.x (up to a two-level migration) using the optional "-s" parameter with the *firmwaredownload* command.

If there are multiple node EGs (encryption groups) in a fabric, please complete firmwaredownload on one node at a time before downloading on another node.

Recommended Migration Paths to FOS v7.4.0a

Migrating from FOS v7.3

- Any 8G or 16G platform running any FOS v7.3.x firmware can be non-disruptively upgraded to FOS v7.4.0a.

Migrating from FOS v7.2

- Any 8G or 16G platform operating at FOS v7.2.x must be upgraded to FOS v7.3.x before non-disruptively upgrading to FOS v7.4.0a.
- Disruptive upgrade to FOS v7.4.0a from FOS v7.2 is supported.
- Firmware clean install to FOS v7.4.0a from FOS v6.4 or later without retaining any configuration is supported.

Important Notes

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

Brocade Network Advisor Compatibility

Brocade Network Advisor greatly simplifies the steps involved in daily operations while improving the performance and reliability of the overall SAN and IP networking environment. Brocade Network Advisor unifies, under a single platform, network management for SAN, LAN and converged networks. Brocade Network Advisor provides a consistent user experience, across the entire Brocade portfolio of switches, routers and adapters.

Brocade Network Advisor provides health and performance dashboards, with an easy-to-use graphical user interface and comprehensive features that automate repetitive tasks. With Brocade Network Advisor, storage and network administrators can proactively manage their SAN environments to support non-stop networking, address issues before they impact operations, and minimize manual tasks.

Brocade Network Advisor is available with flexible packaging and licensing options for a wide range of network deployments and for future network expansion. Brocade Network Advisor 12.4.0 is available in

- SAN-only edition
- IP-only edition
- SAN+IP edition.

For SAN Management, Network Advisor 12.4.0 is available in three editions:

- **Network Advisor Professional***:* a fabric management application that is ideally suited for small-size businesses that need a lightweight management product to manage their smaller fabrics. It manages two FOS fabric at a time and up to 300 switch ports. It provides support for Brocade FC switches, Brocade HBAs / CNAs, and Fibre Channel over Ethernet (FCoE) switches.
- **Network Advisor Professional Plus**: a SAN management application designed for medium-size businesses or departmental SANs for managing up to thirty-six physical or virtual fabrics (FOS) and up to 2,560 switch ports. It supports Brocade backbone and director products (DCX 8510-4/DCX-4S, 48Ks, etc.), FC switches, Fibre Channel Over IP (FCIP) switches, Fibre Channel Routing (FCR) switches/ Integrated Routing (IR) capabilities, Fibre Channel over Ethernet (FCoE) / DCB switches, and Brocade HBAs / CNAs.
- **Network Advisor Enterprise**: a management application designed for enterprise-class SANs for managing up to one hundred physical or virtual fabrics and up to 15,000 switch ports. Network Advisor SAN Enterprise supports all the hardware platforms and features that Network Advisor Professional Plus supports, and adds support for the Brocade DCX Backbone (DCX 8510-8/DCX) and Fiber Connectivity (FICON) capabilities.

More details about Network Advisor's new enhancements can be found in the *Network Advisor 12.4.0 Release Notes*, *Network Advisor 12.4.0 User Guide*, and *Network Advisor 12.4.0 Installation, Migration, & Transition Guides*.

Notes:

- Brocade Network Advisor 12.4.0 or later is required to manage switches running FOS 7.4.0 or later.
- The Brocade Network Advisor seed switch should always have the highest FOS version used in the fabric.

WebTools Compatibility

FOS v7.4.0 is qualified and supported with Oracle Java version 7 update 76 and Java version 8 update 40. Please refer to the "Other Important Notes and Recommendations" section for more details.

SMI Compatibility

It is important to note that host SMI-S agents cannot be used to manage switches running FOS v7.4.

If users want to manage a switch running FOS v7.4 using SMI-S interface, they must use Brocade Network Advisor's integrated SMI agent.

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. Brocade recommends using 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 prior to installing on your switch. Use only FOS versions that are supported by the provider.
- For a list of the effective end-of-life dates for all versions of Fabric OS, visit the following Brocade Web site: http://www.brocade.com/en/support/product-end-of-life.html

Supported Products and FOS Interoperability	
4900, 7500, 7500e, 5000, 200E, 48K Brocade 4012, 4016, 4018, 4020, 4024, 4424	v6.2.2 or later [5]
Brocade 5410, 5480, 5424, 5450, 5460, 5470, NC-5480	v6.2.0 or later [5]
Brocade DCX, 300, 5100, 5300	v6.1.0e and later [1 5 7]
VA-40FC	v6.2.1_vfc [5], v6.2.2 or later [5]
Brocade DCX-4S	v6.2.0 or later [5 7]
Brocade DCX with FS8-18 blade(s), Brocade Encryption Switch	v6.1.1_enc or later [5]
Brocade 7800, DCX and DCX-4S with FCOE10-24 or FX8-24 blades	V6.3.0 or later
Brocade 8000[9]	V6.1.2_CEE [1] or later
Brocade DCX/DCX-4S with FA4-18 blade(s)	DCX requires v6.0.x or later [5] DCX-4S requires 6.2.x or later [4 7]
Brocade DCX 8510-8/DCX 8510-4	FOS v7.0 or later
Brocade DCX 8510-8/DCX 8510-4 with FC16-64 blade	FOS v7.3.0 or later
Brocade DCX 8510-8 with FCOE10-24 blade	FOS v7.3.0 or later
Brocade 6510	FOS v7.0 or later
Brocade 6505	FOS v7.0.1 or later
Brocade 6520	FOS v7.1 or later
Brocade 7840	FOS v7.3.0 or later
5430	FOS v7.1 or later [9]
5431, 6547, M6505	FOS v7.2 or later [9]
6548, 5432	v7.2.1 or later [9]
6545, 6546	v7.3.1 or later [9]
48000 with FA4-18 blade(s), Brocade 7600	V6.2.2 or later [5]
Mi10k, M6140 (McDATA Fabric Mode and Open Fabric Mode)	Not Supported

Multi-Protocol Router Interoperability	
Brocade 7500 and FR4-18i blade	V6.2.2 and higher [3 5 7]
McDATA SANRouters 1620 and 2640	Not Supported

NOS (VDX Platform) Interoperability	
Brocade VDX6710, VDX6720, VDX6730	NOS v2.1.1 or later [6]
Brocade VDX8770	NOS 3.0 or later
Brocade VDX6740	NOS 5.0 or later

Notes:

[1.] When directly attached to a Host or Target that is part of an encryption flow.

[2.] These platforms may not be directly attached to hosts or targets for encryption flows.

[3.] McDATA 1620 and 2640 SANRouters should not be used with FOS-based routing (FCR) for connections to the same edge fabric.

[4.] FA4-18 is not supported in a DCX/DCX-4S that is running FOS v7.0 or later

[5.] If operating with **FOS v6.2.2e** or earlier, Adaptive Networking QoS must be disabled when connecting to 16G FC platform. Otherwise, ISL will segment.

[6.] Connectivity to FC SAN is established via VDX6730 connected to FCR running FOS v7.0.1 or later. FCR platforms supported include 5100, VA-40FC, 5300, 7800, DCX, DCX-4S, DCX 8510-8, DCX 8510-4, 6510, 6520 (requires FOS v7.1 or later). For higher FCR backbone scalability (refer to separate "Brocade SAN Scalability Guidelines" documentation for details), please use 5300, 6520, DCX, DCX-4S, DCX 8510-8, and DCX 8510-4.

[7.] FR4-18i and FC10-6 are not supported on DCX/DCX-4S on FOS v7.1 or later.

[8.] Brocade 8000 is not supported with FOS v7.2 or later.

[9.] Represents the earliest major FOS version. These embedded platforms running respective dedicated FOS versions can also interoperate with FOS v7.3.

Zoning Compatibility Note:

Users are recommended to upgrade to the following versions of firmware when interoperating with a switch running FOS v7.0 or later in the same layer 2 fabric to overcome some of the zoning operations restrictions that otherwise exist:

Main code level	Patch code levels with full zoning compatibility
FOS v6.2	FOS v6.2.2d or later
FOS v6.3	FOS v6.3.2a or later
FOS v6.4	FOS v6.4.1 or later

If there are switches running FOS versions lower than the above listed patch levels in the same fabric as a switch with FOS v7.0 or later, then cfgsave and cfgenable operations **initiated** from these switches will fail if the zoning database is greater than 128KB. In such scenarios zoning operations such as cfgsave/cfgenable can still be performed successfully if initiated from a switch running FOS v7.0 or later.

SNMP Support

FOS v7.4.0 documents the supported MIBs in the Fabric OS MIB Reference document.

For information about SNMP support in Fabric Operating System (FOS) and how to use MIBs, see the Fabric OS Administrator's Guide.

Obtaining the MIBs

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

1. On your web browser, go to http://my.brocade.com.
2. Login with your user name and password.
3. Click the downloads tab.
4. On the downloads tab, under Product Downloads, select All Operating Systems from the Download by list.
5. Select Fabric Operating System (FOS), and then navigate to the release.
6. Navigate to the link for the MIBs package and either open the file or save it to disk.

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

Blade Support

DCX/DCX-4S Blade Support

Fabric OS v7.4 software is fully qualified and supports the blades for the DCX/DCX-4S noted in the following table:

DCX/DCX-4S Blade Support Matrix	
16-, 32-, 48- and 64-port 8Gbit port blades (FC8-16, FC8-32, FC8-48, FC8-64)	Supported with FOS v6.0 and above (FC8-64 requires FOS v6.4) with any mix and up to 8/4 of each. No restrictions around intermix.
FC10-6	Not supported on FOS v7.1 or later
Intelligent blade	Up to a total of 8/4 intelligent blades. See below for maximum supported limits of each blade.
Virtualization/Application Blade (FA4-18)	Not supported on FOS v7.0 or later
FCIP/FC Router blade (FR4-18i)	Not supported on FOS v7.1 or later
Encryption Blade (FS8-18)	Up to a maximum of 4 blades of this type.
Extension Blade (FX8-24)	Up to a maximum of 4 blades of this type.
FCoE/L2 CEE blade FCOE10-24	Up to a maximum of 4 blades of this type. Not supported in the same chassis with other intelligent blades or the FC8-64 port blade.
FC16-32, FC16-48, FC16-64, FC8-32E, FC8-48E	Not supported

Table 1 Blade Support Matrix for DCX and DCX-4S with FOS v7.4

Note: The iSCSI FC4-16IP blade is not qualified for the DCX/DCX-4S.

DCX 8510-8/DCX 8510-4 Blade Support

Fabric OS v7.4 software is fully qualified and supports the blades for the DCX 8510-8 and DCX 8510-4 noted in the table below.

DCX 8510-8/DCX 8510-4 Blade Support Matrix	
FC16-32, FC16-48 16G FC blades	FOS v7.0 or later.
FC16-64 blade[2,3]	FOS v7.3 or later.

DCX 8510-8/DCX 8510-4 Blade Support Matrix	
FC8-64 64 port 8Gbit port blade	With any mix and up to 8/4 of each. No restrictions around intermix. **Note:** FC8-16, FC8-32, FC8-48 blades are *not* supported on DCX 8510 platforms.
FC8-32E, FC8-48E1	FOS v7.0.1 or later.
Intelligent blade	Up to a total of 8/4 intelligent blades. See below for maximum supported limits of each blade.
FCIP/FC Router blade (FR4-18i)	Not supported.
Virtualization/Application Blade (FA4-18)	Not Supported
Encryption Blade (FS8-18)	Up to a maximum of 4 blades of this type.
Extension Blade (FX8-24)	Up to a maximum of 4 blades of this type.
FCoE/L2 CEE blade FCOE10-24	Supported at slot 1 position only on DCX 8510-8 with FOS v7.3.0. Supported in the same chassis with FC16-32 and FC8-32E blades only. Not supported with any other port blades or intelligent blades in the same chassis. Not supported in DCX 8510-4 chassis.

Table 2 Blade Support Matrix for DCX 8510-8 and DCX 8510-4 with FOS v7.4

Note: The iSCSI FC4-16IP blade is not qualified for the DCX 8510-8/DCX 8510-4.

1. Note that 16G SFP+ is not supported in FC8-32E and FC8-48E blades

2. 8510 core blade QSFPs, part numbers 57-1000267-01 and 57-0000090-01, are not supported in FC16-64. The QSFPs supported in FC16-64, part number 57-1000294-01, are not supported on 8510 core blades either.

3. E_port connections on FC16-64 blade have the following restriction: connecting a QSFP port between a FC16-64 blade and an ICL QSFP port on a core blade is not supported.

Power Supply Requirements for Blades in DCX/DCX-4S				
Blades	**Type of Blade**	**DCX/DCX-4S** @110 VAC (Redundant configurations)	**DCX/DCX-4S** @200-240 VAC (Redundant configurations)	**Comments**
FC10-6[1], FC8-16, FC8-32, FC 8-48, FC8-64	Port Blade	2 Power Supplies	2 Power Supplies	Distribute the Power Supplies evenly to 2 different AC connections for redundancy.
FR4-18i[1]	Intelligent Blade	Not Supported	2 Power Supplies	

[1] Note that FC10-6 and FR4-18i are not supported with FOS v7.1 or later.

Power Supply Requirements for Blades in DCX/DCX-4S				
Blades	**Type of Blade**	**DCX/DCX-4S** @110 VAC (Redundant configurations)	**DCX/DCX-4S** @200-240 VAC (Redundant configurations)	**Comments**
FS8-18, FX8-24, FCOE10-24	Intelligent Blade	Not Supported	DCX: 2 or 4 Power Supplies DCX-4S: 2 Power Supplies	• For DCX with three or more FS8-18 Blades, (2+2) 220 VAC Power Supplies are required for redundancy. • For DCX with one or two FS8-18 Blades, (2) 220 VACPower Supplies are required for redundancy. • For DCX-4S, (2) 220 VAC Power Supplies provide redundant configuration with any supported number of FS8-18 Blades. • For both DCX and DCX-4S with FX8-24 blades, (1+1) 220 VAC Power Supplies are required for redundancy.

Table 3 Power Supply Requirements for DCX and DCX-4S

Typical Power Supply Requirements Guidelines for Blades in DCX 8510-8 (For specific calculation of power draw with different blade combinations, please refer to Appendix A: Power Specifications in the 8510-8 Backbone Hardware Reference Manual)					
Configured Number of Ports	**Blades**	**Type of Blade**	**DCX 8510-8** @110 VAC (Redundant configurations)	**DCX 8510-8** @200-240 VAC (Redundant configurations)	**Comments**
Any combination of 8Gb or 16Gb ports with QSFP ICLs	FC8-64, FC16-32, FC16-64, FC8-32E	Port Blade	4 Power Supplies	2 Power Supplies	200-240 VAC: 1+1 Power Supplies 110 VAC: 2+2[1] Power Supplies
256 16Gb ports + QSFP ICLs	FC16-32, FC16-48 (Maximum of fully populated FC16-32 blades), FC16-64	Port Blade	4 Power Supplies	2 Power Supplies	200-240 VAC: 1+1 Power Supplies 110 VAC: 2+2[1] Power Supplies Max 8 FC16-32 port blades
256 8Gb ports + QSFP ICLs	FC8-32E, FC8-48E (Maximum of fully populated FC8-32E blades)	Port Blade	4 Power Supplies	2 Power Supplies	200-240 VAC: 1+1 Power Supplies 110 VAC: 2+2[1] Power Supplies Max 8 FC8-32E port blades

Typical Power Supply Requirements Guidelines for Blades in DCX 8510-8 (For specific calculation of power draw with different blade combinations, please refer to Appendix A: Power Specifications in the 8510-8 Backbone Hardware Reference Manual)					
Configured Number of Ports	**Blades**	**Type of Blade**	**DCX 8510-8** @110 VAC (Redundant configurations)	**DCX 8510-8** @200-240 VAC (Redundant configurations)	**Comments**
192 16Gb Ports & max 2 intelligent blades (FX8-24 / FS8-18/combination) with QSFP ICLs	FC16-32, FC16-48, FC16-64, FX8-24, FS8-18	Port / Intelligent Blade	4 Power Supplies	2 Power Supplies	200-240 VAC: 1+1 Power Supplies 110 VAC: 2+2[1] Power Supplies Max four FC16-48 port blades and max 2 Intelligent blades
192 8Gb Ports & max 2 intelligent blades (FX8-24 / FS8-18/ combination) with QSFP ICLs	FC8-32E, FC8-48E, FX8-24, FS8-18	Port / Intelligent Blade	4 Power Supplies	2 Power Supplies	200-240 VAC: 1+1 Power Supplies 110 VAC: 2+2[1] Power Supplies Max four FC8-48E port blades and max 2 Intelligent blades
336 16Gb ports + QSFP ICLs	FC16-48 (Maximum of seven FC16-48 blades, with one empty port blade slot)	Port Blade	4 Power Supplies	2 Power Supplies	200-240 VAC: 1+1 Power Supplies 110 VAC: 2+2[1] Power Supplies Max 7 FC16-48 port blades
336 8Gb ports + QSFP ICLs	FC8-48E (Maximum of seven FC8-48E blades, with one empty port blade slot)	Port Blade	4 Power Supplies	2 Power Supplies	200-240 VAC: 1+1 Power Supplies 110 VAC: 2+2[1] Power Supplies Max 7 FC8-48E port blades
384 16Gb ports + QSFP ICLs	FC16-48	Port Blade	Not Supported	4 Power Supplies	200-240 VAC: For DCX 8510-8, four (2+2)1 220 VAC Power Supplies are required
384 16Gb ports + QSFP ICLs	FC16-64	Port Blade	4 Power Supplies	2 Power Supplies	200-240 VAC: 1+1 Power Supplies 110 VAC: 2+2[1] Power Supplies

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

Typical Power Supply Requirements Guidelines for Blades in DCX 8510-8 (For specific calculation of power draw with different blade combinations, please refer to Appendix A: Power Specifications in the 8510-8 Backbone Hardware Reference Manual)					
Configured Number of Ports	**Blades**	**Type of Blade**	**DCX 8510-8** @110 VAC (Redundant configurations)	**DCX 8510-8** @200-240 VAC (Redundant configurations)	**Comments**
384 8Gb ports + QSFP ICLs	FC8-48E	Port Blade	4 Power Supplies	4 Power Supplies	200-240 VAC: For DCX 8510-8, four (2+2)[1] 220 VAC Power Supplies are required
Any combination of 8Gb or 16Gb ports and intelligent blades with QSFP ICLs	FC16-32, FC16-48, FC8-64, FC8-32E, FC8-48E, FS8-18,FX8-24	Intelligent Blade / Combination	Dependent on configuration. Requires power calculation for specific configuration	2 or 4 Power Supplies, depending on configuration	For DCX 8510-8, four (2+2)[1] 220 VAC Power Supplies are required when any special purpose blade are installed
512 16Gb ports	FC16-64	Port Blade	4 Power Supplies	2 Power Supplies	200-240 VAC: 1+1 Power Supplies 110 VAC: 2+2[1] Power Supplies
512 16Gb ports + QSFP ICLs	FC16-64	Port Blade	4 Power Supplies	2 Power Supplies	200-240 VAC: 1+1 Power Supplies 110 VAC: 2+2[1] Power Supplies

Table 4 Power Supply Requirements for DCX 8510-8

Typical Power Supply Requirements Guidelines for Blades in DCX 8510-4 (For specific calculation of power draw with different blade combinations, please refer to Appendix A: Power Specificationsin the 8510-4 Backbone Hardware Reference Manual)					
ConfiguredNumber of Ports	**Blades**	**Type of Blade**	**DCX 8510-4** @110 VAC (Redundant configurations)	**DCX 8510-4** @200-240 VAC (Redundant configurations)	**Comments**
96 ports max with QSFP ICLs	FC16-32, FC8-32E	Port Blade	2 Power Supplies	2 Power Supplies	1+1 redundancy with 110 or 200-240 VAC power supplies
Any combination of 8Gb or 16 Gb ports and intelligent blades with QSFP ICLs	FC16-32, FC16-48, FC16-64, FC8-32E, FC8-48E, FC8-64, FS8-18, FX8-24	Intelligent Blade / Combination	Not Supported	2 Power Supplies	200-240 VAC: 1+1 Power Supplies

Table 5 Power Supply Requirements for DCX 8510-4

Scalability

All scalability limits are subject to change. Limits may be increased once further testing has been completed, even after the release of Fabric OS. For current scalability limits for Fabric OS, refer to the *Brocade Scalability Guidelines* document, available under the *Technology and Architecture Resources* section at http://www.brocade.com/compatibility

Other Important Notes and Recommendations

Adaptive Networking/Flow-Based QoS Prioritization

- Any 8G or 4G FC platform running FOS v6.2.2e or lower version of firmware cannot form an E-port with a 16G FC platform when Adaptive Networking QoS is enabled at both ends of the ISL. Users must disable QoS at either end of the ISL in order to successfully form an E-port under this condition.

  Users can disable QoS via portcfgQos --disable command. Please consult Fabric OS Command Reference manual for details related to portcfgQoS command.

- When using QoS in a fabric with 4G ports or switches, FOS v6.2.2 or later must be installed on all 4G products in order to pass QoS info. E_Ports from the DCX to other switches must come up AFTER 6.2.2 is running on those switches.
- When FOS is upgraded from v7.1.x to v7.2.0 or later:

If the Adaptive Networking license was NOT installed in v7.1.x, all ports will have QOS disabled following the firmware upgrade and links will come up in normal mode.

If the Adaptive Networking license was installed in v7.1.x, there will be no change in port QOS mode following the upgrade.

If the remote port supports QOS and QOS is not explicitly disabled on the local or remote port, the link will come up in QOS mode. Otherwise, the link will come up in normal mode.

- If FOS v7.2 or later is factory installed (or by firmwarecleaninstall), Adaptive Networking features are always available. This matches the behavior of the Brocade 6520 and all products shipping with prior versions of FOS and with the Adaptive Networking license factory installed.

Ports will come up in AE mode by default

If the remote port supports QOS and is not explicitly disabled, the link will come up in QOS mode. Otherwise, the link will come up in normal mode.

Access Gateway

Users who want to utilize Access Gateway's Device-based mapping feature in the ESX environments are encouraged to refer to the SAN TechNote GA-TN-276-00 for best implementation practices. Please follow these instructions to access this technote:

1. Log in to http://my.brocade.com
2. Go to Documentation > Tech Notes.
3. Look for the Tech Note on Access Gateway Device-Based Mapping in VMware ESX Server.

D_Port

- The 16Gb QSFP optics used in FC16-64 blade do not support electrical loopback and optical loopback tests. Support is limited to:

Link traffic tests across the 16Gb QSFPs

Roundtrip link latency measurements

Link distance measurements for links that are longer than 100 meter

- D_Port support with HBA/Adapter from Qlogic and Emulex begins with FOS v7.3.0a. FOS v7.3.1a or earlier FOS versions require the Fabric Vision license to support D_Port with 3rd party vendor HBAs. FOS v7.4.0 adds the support for D_Port with 3rd party vendor HBAs with the combination of Fabric Watch license and Advanced Performance Monitoring license. Please refer to Qlogic and Emulex documentation for specific adapter models and firmware levels required.

Edge Hold Time

- Edge Hold Time (EHT) default settings for FOS v7.x have changed from those in some FOS v6.4.x releases. The following table shows the Default EHT value based on different FOS release levels originally installed at the factory:

Factory Installed Version of FOS	Default EHT Value
FOS v7.X	220 ms
FOS v6.4.3x	500 ms
FOS v6.4.2x	500 ms
FOS v6.4.1x	220 ms
FOS v6.4.0x	500 ms
Any version prior to FOS v6.4.0	500 ms

Gen 5 platforms and blades are capable of setting an EHT value on an individual port basis. On 8G platforms EHT is set on an ASIC-wide basis, meaning all ports on a common ASIC will have the same EHT setting. Extra care should be given when configuring EHT on 8G platforms or Gen 5 platforms with 8G blades to ensure E_Ports are configured with an appropriate Hold Time setting.

When using Virtual Fabrics and creating a new Logical Switch when running FOS v7.1.0 or later, the default EHT setting for the new Logical Switch will be the FOS default value of 220ms. However, with FOS v7.1.0 and later, each Logical Switch can be configured with a unique EHT setting that is independent of other

Logical Switches and the Default Switch. Any Gen 5 ports (Condor3 based) assigned to that Logical Switch will be configured with that Logical Switch's EHT setting. Any 8G ports (Condor2 based) will continue to share the EHT value configured for the Default Switch.

For more information on EHT behaviors and recommendations, refer to the Brocade SAN Fabric Resiliency Best Practices v2.0 document available on www.brocade.com.

Encryption Behavior for the Brocade Encryption Switch (BES) and FS8-18

- SafeNet's KeySecure hosting NetApp's LKM (SSKM) is supported for data encryption operations with SSKM operating in PVM mode. Please see SSKM documentation for operating in PVM mode for details. Operation in HVM mode is not supported
- RASlog SPC-3005 with error 34 may be seen if the link key used by a BES/FS8-18 is re-established. Please refer to the LKM/SSKM Encryption Admin Guide for the workaround. Also, please ensure that two (2) SSKM's are present in the deployment for workaround to be performed.
- For crypto tape operations, please ensure to use Emulex FC HBA firmware/drivers 2.82A4/7.2.50.007 or higher. Use of lower level firmware/drivers may result in hosts not being able to access their tape LUNs through a crypto target container.
- Adding of 3PAR Session/Enclosure LUNs to CTCs is now supported. Session/Enclosure LUNs (LUN 0xFE) used by 3PAR InServ arrays must be added to CryptoTarget (CTC) containers with LUN state set to "cleartext", encryption policy set to "cleartext". BES/FS8-18 will not perform any explicit enforcement of this requirement.
- The Brocade Encryption switch and FS8-18 blade do not support QoS. When using encryption or Frame Redirection, participating flows should not be included in QoS Zones.
- The RSA DPM Appliance SW v3.2 is supported. The procedure for setting up the DPM Appliance with BES or a DCX/DCX-4S/DCX 8510 with FS8-18 blades is located in the Encryption Admin Guide.
- Support for registering a 2nd DPM Appliance on BES/FS8-18 is blocked. If the DPM Appliances are clustered, then the virtual IP address hosted by a 3rd party IP load balancer for the DPM Cluster must be registered on BES/FS8-18 in the primary slot for Key Vault IP.
- With Windows and Veritas Volume Manager/Veritas Dynamic Multipathing, when LUN sizes less than 400MB are presented to BES for encryption, a host panic may occur and this configuration is not supported in the FOS v6.3.1 or later release.
- Hot Code Load from FOS v7.3.x to FOS v7.4 is supported. Cryptographic operations and I/O will be disrupted but other layer 2 FC traffic will not be disrupted.
- When disk and tape CTCs are hosted on the same encryption engine, re-keying cannot be done while tape backup or restore operations are running. Re-keying operations must be scheduled at a time that does not conflict with normal tape I/O operations. The LUNs should not be configured with auto rekey option when single EE has disk and tape CTCs.
- Gatekeeper LUNs used by SYMAPI on the host for configuring SRDF/TF using in-band management must be added to their containers with LUN state as "cleartext", encryption policy as "cleartext" and without "-newLUN" option.
- BES/FS8-18 will reject the SCSI commands WRITE SAME, ATS(Compare and Write/Vendor Specific opcode 0xF1) and EXTENDED COPY, which are related to VAAI (vStorage APIs for Array Integration) hardware acceleration in vSphere 4.1/5.x. This will result in non-VAAI methods of data transfer for the underlying arrays, and may affect the performance of VM related operations.
- VMware VMFS5 uses ATS commands with arrays that support ATS. BES/FS8-18 does not support this command set. Use of a workaround procedure is required in order to configure encryption in a VMFS 5 environment. Please refer to Brocade Tech Note "Deployment Options for VMware VMFS-5 with Brocade Encryption" for details.
- XIV storage arrays that have been upgraded to firmware 11.2x or later required to support encryption on thin provisioned LUNs will report all XIV data LUNs as TP=Yes.

FCIP (Brocade 7800 and FX8-24)

- Any firmware activation will disrupt I/O traffic on FCIP links.
- Latency measurements supported on FCIP Tunnels:1GbE & 10GbE - 200ms round trip time and 1% loss.
- After inserting a 4G SFP in GE ports of an FX8-24 blade or 7800 switch, sometimes "sfpshow" output might display "Cannot read serial data!". Removing and re-inserting the SFP should resolve this issue. It is recommended that users perform sfpshow immediately after inserting the SFP and ensure SFP is seated properly before connecting the cables.
- When running FOS v7.2.0 or later, if the new FCIP Circuit Group feature is configured on any FCIP Circuits, a downgrade operation to pre-FOS v7.2.0 will be blocked until the feature is removed from the FCIP configuration(s).

Extension (Brocade 7840)

- Brocade 7840 does not support FCIP connection to Brocade 7800 or FX8-24.
- FOS v7.4 does not support 10G speed on the 24 16G FC ports on Brocade 7840.
- FOS v7.4 does not support VEX port on Brocade 7840.
- Running offline diagnostic tests results in FCIP tunnels down. Reboot the switch after offline diagnostic tests to recover the tunnels.
- Brocade 7840 supports Brocade 10 Gbps Tunable DWDM 80KM SFP+ optical transceiver. Following CLI command can be used to configure the transceiver usage in Brocade 7840.

  - portcfgge ge_num --set -channel <channel_num>

  The channel number can have a value of 1 through 102. The detailed explanation of the values are provided in the product data sheet at the following link:

  http://www.brocade.com/downloads/documents/data_sheets/product_data_sheets/10gbe-tunable-dwdm-80km-sfp-ds.pdf

- When Brocade Network Advisor (BNA) v12.3.2 is used to download firmware on Brocade 7840, BNA reports success of firmware download prematurely when 7840 has not reached High Availability state. Customers for 7840 using BNA to download firmware should wait for extra fifteen minutes after BNA reports success to resume a work load.
- Firmware downgrade from FOS v7.4 to FOS v7.3.0c or earlier should be avoided. Otherwise, the Brocade 7840 may become faulty. (Downgrading to FOS v7.3.0b5 can be used as a workaround.)
- FOS v7.4 does not support HCL with IP Extension.
- Fast deflate compression is supported only with FC traffics only, not with IP Extension.
- IP fragmentation is not supported on the LAN side ports.
- When running IPSec, it is recommended that both sides of the extension tunnel are running the same FOS version.
- When IP Extension traffic volume is high, the target device may back pressure the LAN interface of the Brocade 7840 via Ethernet pause. The target side 7840 will go into flow control. While the 7840 is under flow control, it is possible that non-TCP frames destined for the target device will be dropped. TCP frames will be unaffected. When the target device is a TS7720, this can cause the automated PINGs to be lost. This can result in an alert raised by the local TS7720 indicating frame loss at the remote end. In these cases, the data load is unaffected and this error should be ignored. This feature can be disabled on the TS7720.

FCoE/DCB/CEE (FCOE10-24)

- When upgrading a DCX/DCX-4S with one or more FCOE10-24 blades from FOS v6.x to FOS v7.0.0 or later, the user should carefully review Chapter 5 of the FOS v7.0.0 Converged Enhanced Ethernet Administrator's Guide.

- Ethernet L2 traffic with xSTP Hello timer set to less than or equal to 3 seconds may experience momentary traffic disruption during HA failover.
- Hot plugging a CP with firmware level less than FOS v6.3.0 into a DCX or DCX-4S with an active FCOE10-24 blade will result in the new standby CP not coming up.
- When operating in Converged Mode, tagged traffic on the native VLAN of the switch interface is processed normally. The host should be configured not to send VLAN tagged traffic on the switch's native VLAN.
- When operating in Converged Mode, tagged frames coming with a VLAN tag equal to the configured native VLAN are dropped.
- The Converged Network Adapter (CNA) may lose connectivity to the FCOE10-24 if the CNA interface is toggled repeatedly over time. This issue is related to the CNA and rebooting the CNA restores connectivity.
- The FCOE10-24 support only one CEE map on all interfaces connected to CNAs. Additionally, CEE map is not recommended for use with non-FCoE traffic. QoS commands are recommended for interfaces carrying non-FCoE traffic.
- Before upgrading to FOS v6.4.1_fcoe/v6.4.1_fcoe1/v7.0.0 or later, if the CEE map "default" value already exists, the same "default" value is preserved after upgrading to FOS v6.4.1_fcoe/v6.4.1_fcoe1/v7.0.0 or later. However, if the CEE map "default" is not configured before upgrading to FOS v6.4.1_fcoe/v6.4.1_fcoe1/v7.0.0 or later, then after upgrading to FOS v6.4.1_fcoe/v6.4.1_fcoe1/v7.0.0 or later, the following CEE map "default" will be created automatically:

  cee-map default

  priority-group-table 1 weight 40 pfc

  priority-group-table 2 weight 60

  priority-table 2 2 2 1 2 2 2 2
- When upgrading from FOS v6.3.x or v6.4.x to FOS v6.4.1_fcoe/v6.4.1_fcoe1/v7.0.0 or later, the CEE start up configuration dcf.conf file will be incompatible with the FCoE provisioning changes implemented in v6.4.1_fcoe and later releases. Users can save the dcf.conf file as a backup and apply it once the firmware upgrade is completed to get the DCX/DCX-4S to the same startup configuration as in the older release.
- It is recommended that Spanning Tree Protocol and its variants be disabled on CEE interfaces that are connected to an FCoE device.
- The Fabric Provided MAC Address (FPMA) and the Fibre Channel Identifier (FCID) assigned to a VN_Port cannot be associated with any single front-end CEE port on which the FLOGI was received.
- LLDP neighbor information may be released before the timer expires when DCBX is enabled on a CEE interface. This occurs only when the CEE interface state changes from active to any other state. When the DCBX is not enabled, the neighbor information is not released until the timer expires, irrespective of the interface state.
- The FCoE login group name should be unique in a fabric-wide FCoE login management configuration. If there is a login group name conflict, the merge logic would rename the login group by including the last three bytes of the switch WWN in the login group name. As long as the OUI of the switch WWNs are identical this merge logic guarantees uniqueness in any modified login group name (switches with the same OUI will have unique last 3 bytes in WWN). However, if the participating switches have different OUIs but identical last three bytes in the switch WWNs, then the merge logic will fail to guarantee uniqueness of login group names. This will result in one of the login groups being dropped from the configuration. This means, no device can login to the login group that is dropped as a result of this name conflict. Users must create a new login group with a non-conflicting name to allow device logins.
- Ethernet switch services must be explicitly enabled using the command *"fosconfig –enable ethsw"* before powering on an FCOE10-24 blade. Failure to do so will cause the blade to be faulted (fault 9). Users can enable ethsw after upgrading firmware without FC traffic interruption.
- Upgrading firmware on a DCX or DCX-4S with one or more FCOE10-24 blades from FOS v6.4.1_fcoe1 to FOS v7.0 or later will be non-disruptive to FCoE traffic through FCOE10-24 blades and FC traffic.

- Upgrading firmware on a DCX or DCX-4S with one or more FCOE10-24 blades from FOS v6.3.x, v6.4.x, and v6.4.1_fcoe to FOS v7.0 or later will be disruptive to any traffic through the FCOE10-24 blades.
- When rebooting a DCX or DCX-4S with an FCOE10-24 blade, Qlogic CNA and LSAN zoning, the switch will become very unresponsive for a period of time. This is due to the CNA sending excessive MS queries to the switch.
- The FCOE10-24 can handle 169 small FCoE frames in bursts. If you are using the FCOE10-24, and you delete a large number of v-ports with HCM, some of the v-ports may not appear to be deleted. To correct this, disable and re-enable FCoE with the following CLI commands:

  switch:admin>fcoe –disable slot/port

  switch:admin>fcoe --enable slot/port
- When a FCOE10-24 blade is powered off during configuration replay, the interface specific configuration won't get applied. Later when FCOE10-24 blade is powered on, all physical interfaces will come up with default configurations. User can execute "copy startup-config running-config" command to apply the new configuration after powering on the FCOE10-24 blade.
- When IGMP Snooping is disabled on a VLAN, all configured IGMP groups are removed from that VLAN. User has to reconfigure the IGMP groups after enabling the IGMP snooping on that VLAN.
- FOS v7.3 adds the support of FCOE10-24 blade in DCX 8510-8 chassis with following limitations:

Only one FCOE10-24 blade is supported at the fixed slot 1 position. Inserting the blade into other slot positions, however, will not fault the blade.

An FCOE10-24 blade can co-exist with FC16-32 and FC8-32E blades only in a DCX 8510-8 chassis.

Only supports FCoE direct attach.

Layer2 Ethernet traffic is not supported.

If an FCoE10-24 blade is inserted into a DCX 8510-8 chassis, it is required to reboot the chassis or slot poweroff/poweron core blades. A chassis reboot or slot poweroff/poweron core blades must also be performed if the FCoE10-24 blade is removed and replaced with another blade type.

FCR and Integrated Routing

- With routing and dual backbone fabrics, the backbone fabric ID must be changed to keep the IDs unique.
- VEX edge to VEX edge device sharing will not be supported.
- The man page and help display of *fcrlsanmatrix --display* and *fcrlsan --show* command syntax should be corrected as below:

  fcrlsanmatrix --display -lsan | -fcr | -all

  fcrlsan --show -enforce | -speed | -all

Forward Error Correction (FEC)

- Though FEC capability is generally supported on Condor3 (16G capable FC) ports when operating at either 10G or 16G speed, it is not supported with all DWDM links. Hence FEC may need to be disabled on Condor3 ports when using DWDM links with some vendors by using 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 7.x Compatibility Matrix for supported DWDM equipment and restrictions on FEC use.
- To connect between a switch and an HBA at 16 Gbps, both sides must be in the same mode (fixed speed, and FEC on or off) for them to communicate at that rate. If only one port has FEC enabled, neither port will be able to see the other. If the ports are in dynamic mode, then they may connect, but not at 16 Gbps.

FICON

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

FL_Port (Loop) Support

- FL_Port is not supported on FC16-32, FC16-48, FC16-64, FC8-32E, FC8-48E, Brocade 6510, Brocade 6505, Brocade 6520, or Brocade 7840.
- The FC8-48 and FC8-64 blade support attachment of loop devices.
- Virtual Fabrics must be enabled on the chassis and loop devices may only be attached to ports on a 48-port or 64-port blade assigned to a non-Default Logical Switch operating with the default 10-bit addressing mode (they may not be in the default Logical Switch).
- A maximum of 144 ports may be used for connectivity to loop devices in a single Logical Switch within a chassis in 10-bit dynamic area mode on DCX-4S.
- A maximum of 112 ports may be used for connectivity to loop devices in a single Logical Switch within a chassis in 10-bit dynamic area mode on DCX.
- Loop devices continue to be supported when attached to ports on the FC8-16, FC8-32 with no new restrictions.

Flow Vision

- Users must not specify well known FC addresses, domain controller addresses or CUP Port ID (in FMS mode) for either the source or the destination device field while defining flows.
- Flow Vision does not support port swap. Users must not create flows on ports that are already swapped and users must not swap the ports on which the flows are currently defined.
- After a HA reboot, a flow generator flow can be created if the source or the destination port is F-Port. But traffic will not be initiated. Toggling the port will enforce the restriction again to simulated ports.
- Flow Monitor does not support flows with defined LUN parameters on ingress ports on 8G platforms.
- Flow Generator traffic over VE port is supported only if no other traffic is running on any of the VE ports on that blade or switch platform. If Flow Generator traffic is run over a VE port and production traffic is run over another VE port, then the production traffic may be effected..
- The all F-Port learning flow *sys_mon_all_fport* does not support fabric mode. In a chassis with virtual fabric enabled, this flow can only be activated for a logical switch at a time.

ICLs on DCX/DCX-4S

- If a DCX with an 8-link ICL license is connected to a DCX with a 16-link license, the DCX with the 16-link license will report enc_out errors. The errors are harmless, but will continue to increment. These errors will not be reported if a DCX with a 16-link license is connected to a DCX-4S with only 8-link ICL ports.
- If ICL ports are disabled on only one side of an ICL link, the enabled side may see enc_out errors.

Port Initialization

Users may observe that a port is in “Port Throttled” state when an F_Port is being initialized. This is mostly an informational message that is shown in switchshow output indicating systematic initialization of F_Ports.

However, a port may remain in “Port Throttled” state for an extended period of time and may never come online if it fails to negotiate speed successfully with the neighboring port. Users are advised to check the speed setting of the neighboring switch port to determine the cause of the speed negotiation failure.

Example Output:

```
74    9   10   36ed40   id    N8      In_Sync   FC  Disabled (Port Throttled)
```

Port Mirroring

- Port Mirroring is not supported on the Brocade 7800.

Virtual Fabrics

- When creating Logical Fabrics that include switches that are not Virtual Fabrics capable, it is possible to have two Logical Switches with different FIDs in the same fabric connected via a VF incapable switch. Extra caution should be used to verify the FIDs match for all switches in the same Logical Fabric.
- A switch with Virtual Fabrics enabled may not participate in a fabric that is using Password Database distribution or Administrative Domains. The Virtual Fabrics feature must be disabled prior to deploying in a fabric using these features.
- ISL R_RDY mode is not supported in a base switch with FOS version 7.0 or higher.

WebTools

- WebTools since FOS v7.1.0 has a "SupportSave" interface. It only collects, however, information specific to WebTools. It does not contain the same information as collected by supportSave initiated through CLI or Brocade Network Advisor.
- When launching WebTools on a computer without Internet access, it could take up to 5 minutes to complete because the certificate revocation check performed for the WebTools application takes time to timeout. Users can turn off the certification revocation check on the Java control panel as a workaround.
- FOS v7.4.0 is qualified and supported with Oracle Java version 7 update 76 and Java version 8 update 40. Oracle enforces the latest JRE update to be used to launch WebTools. After JRE expiration date users will see the message "Your Java version is out of date" when launching WebTools. Users can either ignore the message by selecting the later option to proceed with launching WebTools, or install the latest JRE release and then launch WebTools.

Zoning

- There are limitations to zoning operations that can be performed from a FOS v6.x switch that is in the same fabric as a FOS v7.0 or later switch if the FOS v6.x switch is not running the recommended firmware version. Please see Fabric OS Interoperability section for details.

Read Diagnostics Parameters

- RDP on FOS v7.4 is not compatible with RDP on FOS v7.3 switches. FOS v7.3 only supports the Read Diagnostics Parameters (RDP) feature between Brocade switches both running FOS v7.3.

Link Cable Beaconing

- The Link Cable Beaconing (LCB) feature on FOS v7.4 is not compatible with the implementation in FOS v7.3.0 – FOS v7.3.0c. LCB is only supported on ISLs between two Brocade switches both running FOS v7.3.0 – FOS v7.3.0c, or both running FOS v7.3.1 or above.Support with third party vendor devices is only available with FOS v7.3.1 or above with fix for defect 540720.

Miscellaneous

- Users must also keep the RADIUS accounting port (Authentication Port+1) open in the firewall to ensure proper working of the RADIUS authentication.
- Using a Windows anonymous FTP server for supportsave collection:
- When using anonymous ftp, to avoid long delays or failure of simultaneous supportsave collections when AP blades are present in a director chassis, the number of unlimited anonymous users for a Windows FTP server should be configured as follows:
- Number of anonymous FTP connections = (Number of director chassis) + (Number of installed Application Blades x 3)

- RASlog message AN-1010 may be seen occasionally indicating “Severe latency bottleneck detected”. Even though it is a “Warning” message, it is likely to be a false alarm and can be ignored.
- It is important to note that the outputs of *slotshow –p* and *chassisShow* commands also display the maximum allowed power consumption per slot. These are absolute maximum values and should not be confused with the real-time power consumption on 16G blades. The chassisshow command has a “Power Usage (Watts):” field that shows the actual power consumed in real-time on 16G blades.
- Class 3 frames that have been trapped to CPU will be discarded in the following scenarios on DCX/DCX-4S/DCX 8510 during the following conditions:
- HA failover on DCX/DCX-4S/DCX 8510 platforms while running FOS v7.0 or later firmware
- Firmware upgrade from v7.0 to a later release on Brocade 300, 5100, VA-40FC, 5300, 6510
- Firmware upgrade from v7.0.1 to a later release on Brocade 6505
- Firmware upgrade from v7.1.0 to a later release on Brocade 6520
- The QSFP information in the *sfpShow* output will indicate the ID field as all zeros. This is as designed.

  ras080:FID128:root> sfpshow 5/32
  QSFP No: 8 Channel No:0
  Identifier: 13 QSFP+
  Connector: 12 MPO Parallel Optic
  Transceiver: **0000000000000000** 16_Gbps id
- It is recommended that for directors with more than 300 E_Ports, the switch be disabled prior to executing the “switchCfgTrunk” command (used to disable or enable trunking on the switch).
- During non-disruptive firmware upgrades, E_Ports in R-RDY mode may cause some frame drops on the E-port links.
- The Brocade Network Advisor seed switch should always have the highest FOS version used in the fabric.
- For login authentication through RADIUS, Brocade switch should be able to reach RADIUS servers through TCP authentication port (default 1812) and accounting port (default 1813). Both of these ports must be kept open in any firewall settings.
- When a firmware upgrade on a Brocade 6510 switch initiated through Brocade Network Advisor results with “failed to enforce new iptable rules” error message, the switch could be inaccessible via SSH and/or Telnet. Activating (from console) a new policy with the rules of the default active policy will restore access to the switch.
- The Location ID parameter under the *configure* CLI affects routing calculations, and should remain set to the default value of 0 for normal use. Do not change the value unless explicitly instructed to do so by a Brocade Support engineer.
- Fabric OS Command Reference contains an error for the command *creditRecovMode*. The *creditRecovMode –fe_crdloss* configures time-out based credit loss detection of Condor-2 front-end ISL links. However, this feature is NOT enabled by default.
- Support for the 16G 2km ICL QSFP optics has the following notes:

The maximum number of ICL ports with the 2km ICL QSFP can be supported in an 8510 backbone switch with the two kilometer distance is 10, which requires 16 credits configured per Virtual Channel. More ports can be supported with less distance and fewer credits. Full 16 ICL ports can be supported with 11 credits configured per Virtual Channel for upto 1,375 meters.

Before the ICL ports with the 2km ICL QSFP come online, switchShow CLI command may display the port states as in-sync or shifting in and out of port fault.

The sfpShow CLI command displays the 16G 2km ICL QSFP incorrectly as “Length Cu: 3 (units m)” instead of the correct value 0.

Firmware downgrade from FOS v7.3.1 to a prior version is blocked if ICL ports with 2km ICL QSFP optics are present in the switch.

- The maximum number of ports supported for slow drain device quarantine in the same zone with a slow-draining device port is 32. If the 32-port zone limit is exceeded, the quarantine action will not be taken. Once the 32-port zone limit is reached, any new zoned device or port coming online will not be quarantined.

Defects

Closed with Code Change in Fabric OS v7.4.0a

This section lists the defects with Critical, High and Medium Technical Severity closed with a code change.

Defect ID: DEFECT000554782	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.4.0	**Technology Area:** Firmware upload/download
Symptom: Unable to download v7.4.0 firmware with unsupported performance monitor configurations on base switch.	
Condition: Moving a default switch with TopTalker on as a base switch leads to unsupported TopTalker configurations on the base switch. Firmware download to v7.4 is blocked at this point and there is not a command to clear the toptalker as well.	
Workaround: Donot make a logical switch configured with TopTalker as base switch.	

Defect ID: DEFECT000539584	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** System
Reported In Release: FOS7.4.0	**Technology Area:** Optics
Symptom: 2KM QSFP ICL ports may see link errors such as CRC and FEC errors. The link errors may result in credit or frame loss and trigger link reset.	
Condition: Errors may be seen after any conditions that causes the port to be toggled, such as a portdisable or switchdisable.	
Recovery: Clear the stats. Toggle the port and check for link errors.	

Defect ID: DEFECT000542995	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Virtualization
Reported In Release: FOS7.2.1	**Technology Area:** Access Gateway
Symptom: Customer encounters a panic when enabling access gateway through webtools and then running commands through the CLI subsequently.	
Condition: Enable AG mode in the switch through webtools.	
Recovery: Auto-recovery after panic dump.	

Defect ID: DEFECT000546724	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** FICON
Reported In Release: FOS7.4.0	**Technology Area:** FICON CUP
Symptom: Observed " -- FICU_DGB_MSG_001(D) -- Function - ficu_api_deliver_msg_from_remote_CUP() FICU Error RC(-14)" on the console.	
Condition: Normal switch operation, the message is seen when the IPC system is unable to deliver an IPC message to FICUD.	
Recovery: No recovery necessary. No loss of functionality, it is an informational non-essential message	

Defect ID: DEFECT000547349	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** System
Reported In Release: FOS7.4.0	**Technology Area:** CLI
Symptom: Powering on a slot which had quarantined port doesn't result in the port getting moved to quarantined state, until an hafailover is done	
Condition: Powering on the slot which has quarantined port	
Workaround: Remove ports from quarantined list before slotpoweroff using "sddquarantine --clear <slot/port>"	

Defect ID: DEFECT000547765	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.0.2	**Technology Area:** BB Credits
Symptom: Link reset events encountered on internal back-end (BE) port trunks while there are no link errors or credits lost.	
Condition: Under conditions of heavy congestion that cause frames to be dropped at internal Back-End ports and Front-End E-ports at the same time. If multiple overlapping frame drops are detected, then a Link Reset may be observed on a link even though no credits were actually lost. This defect only affects 8G Platforms.	
Workaround: Disable Front-End E-ports credit recovery.	
Recovery: Remove the source of congestion that is causing frame drops.	

Defect ID: DEFECT000547921	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Virtualization
Reported In Release: FOS7.3.1	**Technology Area:** Access Gateway
Symptom: In an AG fabric or NPIV environment, device is not found or HBA detects SCSI command timeout and fabric switch stops routing AG switch/NPIV device traffic.	
Condition: This may occur when fabric switch is configured for session based zoning and a device connected to AG switch or an NPIV device that is not in any zone database, is enabled. This causes all traffic going through the same fabric switch F-port to be disrupted. This issue only impacts 16G fabric switch running FOSv7.4.0, FOSv7.3.1 and FOSv7.2.1d	
Workaround: Use hard zoning on fabric switch, or add the device into zoning database first before bringing it online.	
Recovery: Upon hitting this issue, the user may bring up ANY zoned member on AG switch or NPIV,that is using the fabric switch F-Port, to recover.	

Defect ID: DEFECT000548463	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.1.1	**Technology Area:** Port Bring-up
Symptom: Kernel panic encountered on a CP while taking over the Active Role, due to heartbeat loss, causing a cold recovery of the system.	
Condition: This may be encountered only when processing FDISC with duplicate PWWNs.	

Defect ID: DEFECT000548978	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.4.0	**Technology Area:** Monitoring and Alerting Policy Suite
Symptom: During the firmware upgrade from v7.3.0 to v7.4.0, the MAPS Back-End port BAD_OS rule violations are reported for every port in the AP blades (FX8-24). The errors happen and are reported at the end of the firmware upgrade on both CP's.	
Condition: Topology: If there are any AP blades in the chassis, the BAD_OS errors may be seen after the firmware upgrade completes and the MAPS rules monitoring these counters will get triggered.	
Recovery: None of the blades in the switch, or VE ports in the AP blades get affected. So no recovery procedure is needed when the problem is seen.	

Defect ID: DEFECT000549030	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.4.0	**Technology Area:** Diagnostic Port (D_Port)
Symptom: Dport test between two FC16-64 blades fail.	
Condition: If Dport on demand, or dynamic Dport or static Dport is in effect, the Dport test between two FC 16-64 blades may fail.	
Workaround: Disable Dport configuration and do not allow dynamic or on demand Dport to run.	
Recovery: Use "portdporttest --exit" to exit failed Dport test. Disable Dport configuration and do not allow dynamic or on demand Dport to run. Toggle the port.	

Defect ID: DEFECT000549168	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.4.0	**Technology Area:** Extended Fabrics
Symptom: If any VE ports are disabled non-persistently before a non-disruptive firmaredownload is performed on 7840 then, those VE ports will come up as online after the non-disruptive firmwaredownload	
Condition: Non-disruptive firmwaredownload on 7840 to FOS 7.4.0 where VE ports have been disabled non-persistently.	
Workaround: Persistently disable any disabled VE ports prior to a non-disruptive firmwaredownload.	
Recovery: Disable the VE port(s) after the non-disruptive firmwaredownload. Persistently disabled VE ports are not affected.	

Defect ID: DEFECT000549278	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.4.0	**Technology Area:** FCIP
Symptom: The 'portshow lan-stats --per-flow --tcp' command incorrectly reports 0 for the TCP TX bytes field even when LAN traffic is active.	
Condition: Issuing the 'portshow lan-stats --per-flow --tcp' command.	

Defect ID: DEFECT000549477	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS

Symptom: MAPS might generate a transient MAPS-1021 RASLOG message to indicate switch in Critical state due to faulty port rule/thresholds has violated during CEC testing. Effect of this RASLOG does not stay very long (less than few minutes) and MAPS generates a healthy message.
Condition: This happens during CEC IML test.

Defect ID: DEFECT000551522	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.4.0	**Technology Area:** Tunnel Management
Symptom: At the start of non-disruptive firmware download[HCL] on VE ports if there is a Tunnel outage and the tunnel comes online later, it can result in DP-Recovery and all VEs on that DP will be disrupted.	
Condition: Tunnel outage at the start of HCL	

Defect ID: DEFECT000551787	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.4.0	**Technology Area:** Routing
Symptom: IO is disrupted after HA Failover for FCR imported devices that are configured for Staged Pair	
Condition: In an FCR setup with Staged Pair Matching configured	
Recovery: Wait approximately 6 minutes for FCR to re-import the devices after the HA Failover	

Defect ID: DEFECT000552474	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** FICON
Reported In Release: FOS7.2.1	**Technology Area:** FICON emulation
Symptom: Unable to run Teradata with Teradata FICON emulation enabled on the FCIP tunnel.	
Condition: When Teradata emulation is enabled on an FCIP tunnel and a read operation presents early ending status for a short read. This leads to an error in the FICON Teradata emulation logic and subsequent IOs fail.	
Workaround: Disable Teradata emulation on the FCIP Tunnel.	

Open Defects in Fabric OS v7.4.0

This section lists the open defects with Critical, High and Medium Technical Severity as of March 31, 2015 in Fabric OS v7.4.0

Defect ID: DEFECT000455926	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.2.0	**Technology Area:** TIZ - Traffic Isolation Zoning
Symptom: Devices outside of fail-over disabled TI zone will have portcam entries if there is an alternative path, other than the TI zone, to reach the device in remote switch	
Condition: Devices that are excluded from connectivity to each other in accordance with the TIZ configuration, are visible to each other in the Name Server. Devices will get the details of the zoned devices and PLOGIs sent to these devices will be dropped, sent to Non TI zoned devices	

Defect ID: DEFECT000463170	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.2.0	**Technology Area:** Ethernet Interface
Symptom: ipsecconfig command may hang the command line	
Condition: ipsecconfig --disable command may hang and not work properly. Subsequent disable/re-enables may fail.	

Defect ID: DEFECT000470634	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.2.0	**Technology Area:** Flow Vision: Flow Monitor
Symptom: A static and a learning flow cannot monitor the same traffic at two ports on the same chip.	
Condition: A static and a learning flow created on same chip where the traffic on the static flow is a subflow for the learning flow.	

Defect ID: DEFECT000471762	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.2.0	**Technology Area:** Flow Vision: Flow Monitor
Symptom: Two bi-directional flows monitoring a common subset of traffic do not monitor the frame and byte parameters for one of the flows.	
Condition: Two bi-directional (option -bidir) flows on the same chip monitoring a common subset of traffic and with one of the device parameters (srcdev or dstdev) not specified.	

Defect ID: DEFECT000487388	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** Flow Vision: Flow Generator
Symptom: Some flow generator flows may get deactivated due to system limitations. As a result, they will not generate frames. The deactivation reason is not available in the flow status output.	
Condition: A generator flow may get deactivated automatically for the following known reasons: 1. PID/WWN is not available locally and they might have changed on local system (due to domain change). 2. A blade is replaced by another blade that may not have capability of generating frames. 3. Source ID and Destination ID is same. 4. All 39 VCs are currently used by existing flows and no more flows can be created for the same port. 5. A real devices connected to the port. 6. The flow generator is not being supported by new port type.	

Defect ID: DEFECT000489154	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.0.0	**Technology Area:** SNMPv2, SNMPv3 & MIBs
Symptom: SNMP get/walk against a IPaddresstable (OID1.3.6.1.2.1.4.34) return IP address in ASCII code format. for example 48.49.48.46.48.51.50.46.48.48.48.46.48.52.49 for 010.032.000.041	
Condition: SNMP applications that query IPAddresstable are affected.	
Workaround: Convert ASCII code into characters.	

Defect ID: DEFECT000497518	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.3.0	**Technology Area:** Port bring up
Symptom: F-port comes online and remains as G-port, on FC16-64	
Condition: CP failover during switch disable/enable or slotpoweroff/on on a 8510 platform with 8G hosts attached.	
Workaround: Change speed to fixed 8G using portcfgspeed or change configuration to not allow E-port capability using portcfgeport.	
Recovery: Disable and then re-enable host port.	

Defect ID: DEFECT000498330	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** Diagnostic Port (D_Port)
Symptom: Increase in er_unroutable and er_other_discard counts in port statistics on the local D-Port when the switch at the remote end of the link is rebooted or HA rebooted.	
Condition: When a link which has static D-Port configured between two switches and the switch at one end of the link is rebooted or HA fail over is done.	

Defect ID: DEFECT000502603	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Other
Reported In Release: FOS7.3.0	**Technology Area:** Other
Symptom: If "supportsave" command is executed through remote fosexec command, before completion of previously executed "supportsave" command then user may not get the message "supportSave is already running from another connection, please retry later" from all the domains (in case of "all" option) or on the specific domain, where the command is in progress. Instead "Command is initiated." message will be displayed.	
Condition: If user tries to issue "supportsave" through remote fosexec command, while the same command is already in progress, it will not display the expected error message from "supportsave" command.	

Defect ID: DEFECT000503071	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.3.0	**Technology Area:** Extended Fabrics
Symptom: FICON Channel(s) takes IFCCs (Interface Control Checks) during init when two parallel 10Gb tunnels are present.	
Condition: Two 8510-8 Logical Switches joined into a Logical Fabric with Base Fabrics (XISL) FCIP tunnels. The tunnel Configuration are parallel 10Gb tunnels with a single circuits and no emulation.	
Workaround: Use only 1 FCIP tunnel in the Base Fabric or E-Port ISL links in the Base Fabric.	
Recovery: Disable one of the FCIP tunnels, leaving just one tunnel available.	

Defect ID: DEFECT000503761	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.0	**Technology Area:** SNMPv2, SNMPv3 & MIBs
Symptom: SNMP-v3 get/set request will fail with decryption error while SNMP-v3 user privacy protocol set to AES256.	
Condition: Configuring SNMP-v3 with privacy protocol set to AES256, SNMP-v3 get/set request will fail.	
Workaround: Use other SNMP privacy protocols like DES and AES128 for SNMP-v3 account.	
Recovery: Use snmpconfig --default snmpv3 to default the SNMP-v3 configuration and reconfigure it again.	

Defect ID: DEFECT000507871	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** Frame Viewer
Symptom: If framelog is disabled before HAFailover, then after HAFailover framelog will get enabled	
Condition: The defect will be hit only if the following sequence happens: 1. Install new firmware 2. Change framelog config using framelog --disable 3. HAFailover After HAFailover completes, framelog will show enabled and disabling or changing framelog configuration will not be effective	
Recovery: Recovery is to do a HAFailover again and restore framelog configuration to default (enabled)	

Defect ID: DEFECT000509850	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.0	**Technology Area:** Web Tools
Symptom: Unable to view the current updated FCIP details after clicking Refresh Now Option.	
Condition: Changes to the FCIP tunnels in the 7840 platform are not updated in the WebTools views.	
Workaround: Navigate to another tab and return to see the updated values of FCIP Tunnel.	

Defect ID: DEFECT000510618	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** supportShow
Symptom: When supportsave is invoked from BNA the following raslog is seen on the switch. [SS-1001], 525, SLOT 7 | CHASSIS, WARNING, DCX_155, supportSave's upload operation to host IP address 10.38.162.10 aborted. This indicates that a specific support module file transfer was not complete and failed.	
Condition: [SS-1001], 525, SLOT 7 | CHASSIS, WARNING, DCX_155, supportSave's upload operation to host IP address 10.38.162.10 aborted. The above raslog is seen only when there is a network issue while transferring support files frlom the switch to the remote host. SupportSave would continue to transfer the remaning support files to the remote host.	
Workaround: Verify all arguments provided with supportsave. This could also be because of an intermittent network issue. Supportsave can be retried to collect the data tat was not transferred.	
Recovery: Verify all arguments passed with supportsave and check network connectivity to the remote host. Retry Supportsave	

Defect ID: DEFECT000511843	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** Flow Vision: Flow Mirroring
Symptom: The “No of Mirrored Frames” counter may not be equal to the sum of “No of RX Mirrored Frames” counter “and “No of TX Mirrored Frames” counter, when a mirror port is specified in a flow definition.	
Condition: The condition is seen after the "No of Mirrored Frames" counter overflows.	

Defect ID: DEFECT000512534	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** Flow Vision: Flow Monitor
Symptom: An FCR fabric flow does not monitor, when SFID and DFID of the flow are on the same ASIC chip.	
Condition: Create a monitor flow on a FCR backbone E-port using SFID and DFID options, where the SFID and DFID are on the same ASIC chip.	
Workaround: Create a flow with both SID, DID wildcards, and SFID, DFID wildcards. Example: flow --creat fmon -fea mon -ingrport 20 -srcdev '*' -dstdev '*' -sfid '*' -dfid '*'	

Defect ID: DEFECT000512746	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** Flow Vision: Flow Monitor
Symptom: A WWN based flow will not be deactivated automatically, when the WWN of the generator port is changed using the command 'fapwwn".	
Condition: WWN of the generator port is changed using the command 'fapwwn'.	
Recovery: Deactivate and activate the flow manually.	

Defect ID: DEFECT000515289	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.1.2	**Technology Area:** Monitoring and Alerting Policy Suite (MAPS)
Symptom: IPfilter policies not enforced on standby CP, until after hafailover, and may be enforced on IPFC address on VF.	
Condition: This (bypassing IPfilter policies enforcement) is encountered on standby CP.	

Defect ID: DEFECT000517763	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.2.0	**Technology Area:** Firmware upload/download
Symptom: Firmwaredownload fails when using scp to download from the built in BNA server	
Condition: This may be encountered only when scp is used to download from the built in scp server	
Workaround: use ftp or the external server for firmwaredownload	

Defect ID: DEFECT000523863	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** FICON
Reported In Release: FOS7.2.0	**Technology Area:** FICON
Symptom: Channel Detected Errors, may see an error indicating a protocol timeout, the CUP continues to run.	
Condition: System Reset Received by CUP	
Recovery: If the CUP stops communicating, vary CUP Path back online (vary offline/online)	

Defect ID: DEFECT000524532	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.2.1	**Technology Area:** Bottleneck Detection
Symptom: Unwarranted Bottleneck Detection alerts may be encountered on a switch.	
Condition: This issue stems from a failing API leading to incorrect computations. When applying consistent latency into the switch, the AN-1003 messages for the specific F_Port show very low affected percentages with a slowdown value of 0.	

Defect ID: DEFECT000525068	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** Monitoring and Alerting Policy Suite (MAPS)
Symptom: MAPS dashboard history shows incorrect value of greater than 100% for RX, TX, UTIL usage.	
Condition: This can happen when MAPS is monitoring the system.	

Defect ID: DEFECT000529293	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.1	**Technology Area:** Ethernet Interface
Symptom: IFMODESET command does not change the mode of the interface.	
Condition: This is seen when the CLI command "ifmodeset" is run in non-interactive mode	
Workaround: Use interactive mode of this CLI command to set AN or Speed	

Defect ID: DEFECT000532917	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** System
Reported In Release: FOS7.2.0	**Technology Area:** CLI
Symptom: The cli command hareboot, which is designed for performing a non-disruptive reboot of a non-disruptive switch is available to admin level user on a director class switch.	
Condition: hareboot can be run on a Director class switch.	

Defect ID: DEFECT000533422	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.2.1	**Technology Area:** FC-FC routing
Symptom: Fabric router switch may observe panic upon receiving invalid frame from edge switch.	
Condition: This happens when fabric router running FOS7.2.x or earlier receives unknown Fibre Channel Common Transport (FC_CT) request from edge switch with zero sized payload. This does not apply to FOS v7.3.x or later.	
Recovery: Disable edge switch port and upgrade.	

Defect ID: DEFECT000534748	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** System
Reported In Release: FOS7.4.0	**Technology Area:** CLI
Symptom: The switch names longer than 15 characters will be truncated to 15 characters in the switch name field of "islshow" output.	
Condition: When user executes "islshow" CLI command, user will notice that only up to 15 characters of switchname get displayed.	

Defect ID: DEFECT000536765	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.2.1	**Technology Area:** Name Server / Zoning
Symptom: Switch panics and becomes non-responsive as a result of a large number of ports and devices coming online and logging in concurrently.	
Condition: Uncommon scenario that can happen when concurrent ports and devices coming online and logging in keeping the switch CPU too busy to keep up processing	
Recovery: Powercycle or reboot the switch	

Defect ID: DEFECT000537487	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Management
Reported In Release: FOS7.4.0	**Technology Area:** Web Tools
Symptom: When the IP address is provided for specific logical switch context, the default switch context will be launched.	
Condition: Launching WebTools for logical switch context which has IPFC and subnet mask address configured.	
Workaround: Launch WebTools for the default switch context and navigate to specific logical switch context.	

Defect ID: DEFECT000537498	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.4.0	**Technology Area:** Web Tools
Symptom: Switch hardware view shows the blade status LED as black instead of amber, if the FC16-64 port blade is in faulty state.	
Condition: Switch hardware view shows the blade status LED as black when the FC16-64 port blade goes to faulty state.	

Defect ID: DEFECT000539134	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.1.1	**Technology Area:** Routing
Symptom: When observing porterrshow and portperfshow on E_Ports to an embedded switch, the throughput is observed to not be evenly distributed. The distribution appears to be 2:1 ratio.	
Condition: - Exchange-based routing. - Incoming data to local switch is arriving on two ISLs. - The incoming data is routed to two ISLs (the two ISLs showing the imbalance)	
Workaround: Add an additional ISL or trunk the existing links	

Defect ID: DEFECT000539584	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** System
Reported In Release: FOS7.4.0	**Technology Area:** Optics
Symptom: 2KM QSFP ICL ports may see link errors such as CRC and FEC errors. The link errors may result in credit or frame loss and trigger link reset.	
Condition: Errors may be seen after any conditions that causes the port to be toggled, such as a portdisable or switchdisable.	
Recovery: Clear the stats. Toggle the port and check for link errors.	

Defect ID: DEFECT000541425	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.4.0	**Technology Area:** Logging
Symptom: "syslog-ng: no process killed" message is displayed on console.	
Condition: This could happen when some syslog activity requires syslog daemon to be restarted. There is no impact to syslog functioanlity and in all cases syslog daemon was seen to work properly.	
Recovery: No recovery required as there is no functionality loss.	

Defect ID: DEFECT000541427	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.0.1	**Technology Area:** POST - Power-on Self-Test
Symptom: switch will panic when the user runs portloopback tests within one hour after hafailover.	
Condition: This would happen only on C3 platforms.	
Workaround: Run portloopback/diag tests 1 hour after hafailover.	

Defect ID: DEFECT000542995	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Virtualization
Reported In Release: FOS7.2.1	**Technology Area:** Access Gateway
Symptom: Customer encounters a panic when enabling access gateway through webtools and then running commands through the CLI subsequently.	
Condition: Enable AG mode in the switch through webtools.	
Recovery: Auto-recovery after panic dump.	

Defect ID: DEFECT000546095	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Virtualization
Reported In Release: FOS7.2.0	**Technology Area:** Virtual Fabrics
Symptom: Switch reboot occurred during simultaneous invocation of lfcfg command.	
Condition: Occurs when lfcfg is invoked simultaneously by different users.	
Workaround: Refrain from invoking lfcfg command simultaneously.	

Defect ID: DEFECT000546417	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.1	**Technology Area:** SNMPv2, SNMPv3 & MIBs
Symptom: After upgrade to FOS 7.3.1, SNMP traps would not be seen in BNA master log.	
Condition: If switch is configured with IPFC address and if we change IP address of a switch, the traps are sent using IPFC address instead of chassis/switch IP address.	
Recovery: CP failover after both CPs migrated to new firmware or after IP address change.	

Defect ID: DEFECT000546719	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.4.0	**Technology Area:** FC-FC routing
Symptom: Proxy creation failure may be observed along with raslog message WARNING FCR-1021 00 0x0004 Local LSAN device entries exhausted while updating LSAN zone %s device entries.	
Condition: In a large Meta SAN, if 10,000 proxy devices already exist and there is an attempt to add more proxy devices, the proxy device creation will be failed.	
Recovery: Run fcrproxyconfig CLI command to determine the total number of proxy devices in the switch. If the total count shows 10,000 proxy devices, use "fcrproxyconfig -r" to remove some proxy devices.	

Defect ID: DEFECT000546724	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** FICON
Reported In Release: FOS7.4.0	**Technology Area:** FICON CUP
Symptom: Observed " -- FICU_DGB_MSG_001(D) -- Function - ficu_api_deliver_msg_from_remote_CUP() FICU Error RC(-14)" on the console.	
Condition: Normal switch operation, the message is seen when the IPC system is unable to deliver an IPC message to FICUD.	
Recovery: No recovery necessary. No loss of functionality, it is an informational non-essential message	

Defect ID: DEFECT000546994	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.1	**Technology Area:** Brocade Network Advisor
Symptom: Supportsave initiated from BNA fails, using same credentials from CLI, supportsave works	
Condition: This would happen only when special character is used	
Workaround: Configuring BNA FTP password with no special character.	

Defect ID: DEFECT000547173	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.4.0	**Technology Area:** Logging
Symptom: On chassis based systems, when syslog is configured, configured server details are not reflected on the standby CP.	
Condition: Applicable only on chassis based systems when syslog server is configured only on active CP.	
Workaround: Configure the syslog server details on both active and standby CPs.	
Recovery: Configure the server details after HA to ensure that the logs are updated.	

Defect ID: DEFECT000547349	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** System
Reported In Release: FOS7.4.0	**Technology Area:** CLI
Symptom: Powering on a slot which had quarantined port doesn't result in the port getting moved to quarantined state, until an hafailover is done	
Condition: Powering on the slot which has quarantined port	
Workaround: Remove ports from quarantined list before slotpoweroff using "sddquarantine --clear <slot/port>"	

Defect ID: DEFECT000547835	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.4.0	**Technology Area:** Monitoring and Alerting Policy Suite (MAPS)
Symptom: FOS does not generate MAPS-1010 RASLOG meessage if BNA fences the F_port.	
Condition: It is applicable if the switch or fabric is monitored by BNA and port decommission is configured and enabled. If BNA is unable to decommission an F-Port it then fences the port as a fall back action and in this case MAPS-1010 RASLOG message is not generated. Note, port decommission action always fences associated port so, if BNA fails to decommission F_port then it fences the port.	

Defect ID: DEFECT000547921	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Virtualization
Reported In Release: FOS7.3.1	**Technology Area:** Access Gateway
Symptom: In an AG fabric or NPIV environment, device is not found or HBA detects SCSI command timeout and fabric switch stops routing AG switch/NPIV device traffic.	
Condition: This may occur when fabric switch is configured for session based zoning and a device connected to AG switch or an NPIV device, that is not in any zone database, is enabled. This causes all traffic going through the same fabric switch F-port to be disrupted. This issue only impacts 16G fabric switch running FOSv7.4.0, FOSv7.3.1 and FOSv7.2.1d	
Workaround: Use hard zoning on fabric switch, or add the device into zoning database first before bringing it online.	
Recovery: Upon hitting this issue, the user may bring up ANY zoned member on AG switch or NPIV, that is using the fabric switch F-Port, to recover. .	

Defect ID: DEFECT000548153	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.4.0	**Technology Area:** Flow Vision: Flow Generator
Symptom: Flow Generator traffic through the VE port may affect real I/O traffic on the same or other VE ports.	
Condition: Flow Generator traffic through the VE port with real I/O traffic on the same or other VE ports.	
Workaround: Flow Generator traffic over VE port is supported only if no other traffic is running on any of the VE ports on that blade or switch platform.	

Defect ID: DEFECT000548700	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.4.0	**Technology Area:** Flow Vision: Flow Monitor
Symptom: A learning flow created on an egress port shows frame size as "--" after multiple monitoring resets or the total frame size is sometimes off by 8 bytes.	
Condition: User has a learned monitoring flow created on the egress port.	
Recovery: Deactivate and reactivate the flow.	

Defect ID: DEFECT000548721	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS6.4.3	**Technology Area:** Fabric Watch
Symptom: A E-port is fenced even after port fencing has been disabled.	
Condition: This issue would only happen if E-port and port classes are configured with the same thresholds for ST area. Disable port fence did not take care of the earlier fenced E-port properly under this condition.	
Workaround: Use the E-Port only threshold to monitor the State change of ISLs alone OR to monitor all the ports in general, choose a different threshold value for E-port threshold and port class threshold (probably E-Port threshold + 5).	
Recovery: Bouncing the port	

Defect ID: DEFECT000548978	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.4.0	**Technology Area:** Monitoring and Alerting Policy Suite (MAPS)
Symptom: During the firmware upgrade from v7.3.0 to v7.4.0, the MAPS Back-End port BAD_OS rule violations are reported for every port in the AP blades (FX8-24). The errors happen and are reported at the end of the firmware upgrade on both CP's.	
Condition: Topology: If there are any AP blades in the chassis, the BAD_OS errors may be seen after the firmware upgrade completes and the MAPS rules monitoring these counters will get triggered.	
Recovery: None of the blades in the switch, or VE ports in the AP blades get affected. So no recovery procedure is needed when the problem is seen.	

Defect ID: DEFECT000549030	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.4.0	**Technology Area:** Diagnostic Port (D_Port)
Symptom: Dport test between two FC16-64 blades fail.	
Condition: If Dport on demand, or dynamic Dport or static Dport is in effect, the Dport test between two FC 16-64 blades may fail.	
Workaround: Disable Dport configuration and do not allow dynamic or on demand Dport to run.	
Recovery: Use "portdporttest --exit" to exit failed Dport test. Disable Dport configuration and do not allow dynamic or on demand Dport to run. Toggle the port.	

Defect ID: DEFECT000549140	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Security
Reported In Release: FOS7.4.0	**Technology Area:** Security Vulnerability
Symptom: CVE-2013-4548: With AES-GCM configured, it's possible to bypass intended ForceCommand and login-shell restrictions via packet data that provides a crafted callback address. CVE-2014-2532: A remote user can modify AcceptEnv variable to bypass intended environment variable restrictions	
Condition: CVE-2013-4548 : Configurations where SSH ciphers use AES GCM for SSH connection CVE-2014-2532: Use of root account and editing of the SSH configuration file.	

Defect ID: DEFECT000549168	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.4.0	**Technology Area:** Extended Fabrics
Symptom: If any VE ports are disabled non-persistently before a non-disruptive firmaredownload is performed on 7840 then, those VE ports will come up as online after the non-disruptive firmwaredownload	
Condition: Non-disruptive firmwaredownload on 7840 to FOS 7.4.0 where VE ports have been disabled non-persistently.	
Workaround: Persistently disable any disabled VE ports prior to a non-disruptive firmwaredownload.	
Recovery: Disable the VE port(s) after the non-disruptive firmwaredownload. Persistently disabled VE ports are not affected.	

Defect ID: DEFECT000549278	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.4.0	**Technology Area:** FCIP
Symptom: The 'portshow lan-stats --per-flow --tcp' command incorrectly reports 0 for the TCP TX bytes field even when LAN traffic is active.	
Condition: Issuing the 'portshow lan-stats --per-flow --tcp' command.	

Defect ID: DEFECT000549417	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Management
Reported In Release: FOS7.4.0	**Technology Area:** Telnet
Symptom: If dynamic port name is configured on the switch, any change in port name will not be handled by MAPS dynamic group for which "feature" is specified as port name. After change in port name, the group membership may not reflect correct members.	
Condition: Using MAPS and dynamic port naming	

Defect ID: DEFECT000549434	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.4.0	**Technology Area:** Monitoring and Alerting Policy Suite (MAPS)
Symptom: Moving an F-Port from one logical switch to another logical switch causes the port to be marked as slow drain.	
Condition: After a latency is induced on a port, the port has to be moved to a different logical switch and enabled within 1 minute.	
Workaround: If transient latency is seen on a port, wait for 1 minute before moving the port to another logical switch.	

Defect ID: DEFECT000549477	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.4.0	**Technology Area:** Monitoring and Alerting Policy Suite (MAPS)
Symptom: MAPS might generate a transient MAPS-1021 RASLOG message to indicate switch in Critical state due to faulty port rule/thresholds has violated during CEC testing. Effect of this RASLOG does not stay very long (less than few minutes) and MAPS generates a healthy message.	
Condition: This happens during CEC IML test.	

Defect ID: DEFECT000549485	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.4.0	**Technology Area:** Tunnel Management
Symptom: ESM-1101 Error message seen with the following signature: hclLog.h:0 ESM MSG Status:DP:1:DELETE STARTED:STAT:0x4.	
Condition: This can occur during a tunnel deletion or portcfgdefault on a VE port operation.	
Recovery: The condition is self-recovered. The command is retried internally to ensure cleanup.	

Defect ID: DEFECT000549856	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** System
Reported In Release: FOS7.4.0	**Technology Area:** CLI
Symptom: When a Quarantined port is moved out of the current Logical Switch, the port is listed as -1/-1 in the output of 'sddquarantine --show' executed in the current Logical Switch	
Condition: Moving a quarantined port in disabled state to a different Logical Switch in a chassis based switch	
Workaround: Remove the port from quarantined state using sddquarantine --clear <slot/port> before moving the port to a different logical switch	

Defect ID: DEFECT000550089	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.4.0	**Technology Area:** Flow Vision: Flow Monitor
Symptom: Predefined learn flow statistics does not increment in a Backbone-to-Edge setup after monitoring traffic for some time.	
Condition: Predefined monitor learn flow is active with continuous traffic.	
Recovery: Deactivate and reactivate the predefined learn flow.	

Defect ID: DEFECT000550437	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.4.0	**Technology Area:** FCIP
Symptom: Inconsistent tunnel state between the 'portshow fciptunnel --circuit' command and the 'portshow fciptunnel --qos --circuit' command when one of the circuits under the tunnel is disabled. In the non-QoS display, the tunnel shows in a degraded state. In the QoS display, the tunnel shows up. This is only a state reporting issue and traffic will remain running over the other circuits that are in an online state.	
Condition: This will occur when any circuits under a tunnel are administratively disabled and when all other circuits are in an online state.	

Defect ID: DEFECT000550519	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.4.0	**Technology Area:** FCIP
Symptom: Periodic smart data collection will not happen for the ports with SFP installed on 7840 and the sfpshow command will list them as "Not Available"	
Condition: Periodic smart data collection will be skipped if the CPU load has exceeded its threshold value	
Recovery: Users can issue the force read option "sfpshow <slot/port> -f" to read the smart data values.	

Defect ID: DEFECT000550520	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.4.0	**Technology Area:** FCIP
Symptom: Switchshow displays LAN port as online when no Ethernet cable is attached in 7840	
Condition: Switchshow is run on 7840 where once present Ethernet cable has been removed for a LAN port	
Recovery: Disable and enable the affected port	

Defect ID: DEFECT000550554	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** FICON
Reported In Release: FOS7.4.0	**Technology Area:** FICON CUP
Symptom: With CUP Diagnostics and zOS HealthChecker, a port that reports a SlowDrain or Bottleneck Detected event, may persist in reporting this state, even though the condition has cleared.	
Condition: The CUP may persist in reporting this port performance problem, when actually, the problem has been cleared.	
Recovery: Vary the port offline and online or for E-ports, disable and enable the port.	

Defect ID: DEFECT000550634	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.4.0	**Technology Area:** Firmware upload/download
Symptom: firmwarecleaninstall with sftp option fails	
Condition: sftp protocol is not supported for this CLI however, the CLI usage help indicates that it is supported.	
Workaround: Use scp or ftp option to run firmwarecleaninstall	

Defect ID: DEFECT000550681	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.4.0	**Technology Area:** FCIP
Symptom: 7840 becomes non-operational (faulty).	
Condition: A 7840 becomes non-operational (faulty) as a result of another firmwaredownload being run while a previous non-disruptive firmwaredownload is in progress.	
Workaround: Do not initiate another firmwaredownload while a previous non-disruptive firmwaredownload is already in progress.	
Recovery: Reboot the 7840.	

Defect ID: DEFECT000550920	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.4.0	**Technology Area:** Equipment Status
Symptom: 7800 gets stuck in faulty state after upgrade.	
Condition: Upgrade 7800 from v7.3.1 -> v7.4.0_bld43.	
Recovery: Powercycle the switch	

Defect ID: DEFECT000551057	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.4.0	**Technology Area:** Monitoring and Alerting Policy Suite (MAPS)
Symptom: "sddquarantine --clear all" clears the SDD port list but "sddquatantine --show" indictaes that it does not delete the local quarantine devices in the device fabric list.	
Condition: Devices continue to appear in the fabric list after "sddquarantine --clear all" has been run to clear the quarantined ports.	
Recovery: portdisable and portenable the local ports which are shown in quarantined state in the fabric list	

Defect ID: DEFECT000551522	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.4.0	**Technology Area:** Tunnel Management
Symptom: At the start of non-disruptive firmware download[HCL] on VE ports if there is a Tunnel outage and the tunnel comes online later, it can result in DP-Recovery and all VEs on that DP will be disrupted.	
Condition: Tunnel outage at the start of HCL	

Defect ID: DEFECT000551784	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** System
Reported In Release: FOS7.4.0	**Technology Area:** Component
Symptom: MetaSAN with backbone containing two FCR switches that are bound together by means of FCR binding, adding a new backbone switch without any binding results in the new backbone switch learning the zones from the FCR bound switches	
Condition: Add a new backbone switch without any binding to a backbone that contains FCR switches that are bound together by means of FCR binding.	
Workaround: Bind the newly added FCR switch to itself. That way it is present in the FCR binding matrix and will reject any zone updates sent from other FCR bound switches.	

Defect ID: DEFECT000551787	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.4.0	**Technology Area:** Routing
Symptom: IO is disrupted after HA Failover for FCR imported devices that are configured for Staged Pair Matching.	
Condition: In an FCR setup with Staged Pair Matching configured	
Recovery: Wait approximately 6 minutes for FCR to re-import the devices after the HA Failover	

Closed with Code Change in Fabric OS v7.4.0

This section lists the defects with Critical, High and Medium Technical Severity closed with a code change as of March 31, 2015 in Fabric OS v7.4.0.

Defect ID: DEFECT000417089	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Security
Reported In Release: FOS7.1.0	**Technology Area:** Fabric Authentication
Symptom: Invalid VF numbers can be specified in TACACS+	
Condition: If 0 is configured for the role list in tacacs/radius/ldap server configuration, userconfig --show will show '0' also in the role list details.	
Workaround: Avoid configuring the value '0' for role list	

Defect ID: DEFECT000420903	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Management
Reported In Release: FOS7.0.0_pha	**Technology Area:** Web Tools
Symptom: Graphic for external management port is lit with no connection for 6547 switch.	
Condition: When RJ45 cable is removed from the switch faceplate, Webtools still shows external management port with solid green LED.	

Defect ID: DEFECT000431369	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Management
Reported In Release: FOS7.0.2	**Technology Area:** SNMPv2, SNMPv3 & MIBs
Symptom: Mib browser displays ascii-hex of populated fcportflag value. For example it displays "30" for 0, "31" for 1, where expected display is "0", "1".	
Condition: This is seen only for the MIB display of fcportflag.	

Defect ID: DEFECT000436921	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** System
Reported In Release: FOS6.3.1_dcb	**Technology Area:** CLI
Symptom: Console may hang, leading to switch Panic from unexpected termination of daemons from Out of Memory condition.	
Condition: This may be observed while performing supportsave or other CLI management operations	

Defect ID: DEFECT000453829	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.2.0	**Technology Area:** Routing
Symptom: Traffic could be extra slow with BufOpMode enabled	
Condition: For the FC8-32 and FC8-48 port blade, routing from an E-Port to an F-Port on the same ASIC	
Workaround: slotpoweroff then slotpoweron.	

Defect ID: DEFECT000457373	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Virtualization
Reported In Release: FOS7.0.2	**Technology Area:** Access Gateway
Symptom: BR5480 embedded switch displays invalid message without functional impact.	
Condition: Invalid message "Request F-N Port Mappings for Access Gateway Change from SW" is observed while running in native switch mode.	
Recovery: No impact to switch functionality.	

Defect ID: DEFECT000472607	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** System
Reported In Release: FOS7.2.0	**Technology Area:** CLI
Symptom: Brocade 6510 switch may become inaccessible via SSH and/or Telnet when a firmware upgrade of the switch initiated through Brocade Network Advisor results with “failed to enforce new iptable rules” error message,.	
Condition: It's a race condition caused by an existing ineffective file locking mechanism.	
Workaround: Activating (from console) a new policy with rules of default active policy will restore access to the switch. such as: Ipfilter –clone new_rules –from default_ipv4 Ipfilter –activate new_rules	

Defect ID: DEFECT000473541	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** System
Reported In Release: FOS6.4.3	**Technology Area:** CLI
Symptom: Large number of threads in environmental daemon (emd) cause system to run out of memory and panic.	
Condition: Over 100 portshow CLIs are concurrently running on a director.	
Workaround: Limit the number of concurrent CLIs to under 50 at a time.	

Defect ID: DEFECT000479904	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS6.4.3	**Technology Area:** Firmware upload/download
Symptom: Firmware Migration might result in a switch panic due to a weblinker termination	
Condition: In rare cases, a firmware download might cause a weblinker termination followed by a panic	
Recovery: In chassis base system reboot the standby CP. In a pizza box, reboot the switch.	

Defect ID: DEFECT000483272	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Other
Reported In Release: FOS7.3.0	**Technology Area:** Other
Symptom: Management applications may not recognize switches with new OUIs.	
Condition: Switches shipped with new OUIs 00-14-38, A0-D3-C1, and 88-94-71	

Defect ID: DEFECT000483437	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Management
Reported In Release: FOS7.2.0	**Technology Area:** Web Tools
Symptom: On Web Tools, the cascaded switch Icon in Fabric Tree gets greyed out and the pop up shows the status as "Unmonitored".	
Condition: This issue occurs when a switch is running FOS version v7.2.0 or higher while the remote switch is running FOS version v7.1.x or lower, and one of switches has VF enabled while the other switch has VF disabled. This issue will not occur if all switches are running FOS version v7.2.0 or higher, regardless of whether VF is enabled or disabled.	
Workaround: Run same FOS version on all switches in the fabric.	

Defect ID: DEFECT000484261	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.2.1	**Technology Area:** Frame Monitoring
Symptom: CLI command "sloterrshow" reports timeout frame. However, “framelog –show” does not capture the timed out frame.	
Condition: This discrepancy with respect to timeout frames maybe noted when comparing outputs of CLI commands "sloterrshow" and “framelog –show”	

Defect ID: DEFECT000484766	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.2.1	**Technology Area:** FCIP
Symptom: Port persistent disable feature doesnt work for GE ports on FX8-24 across any reboot or hareboot operations,	
Condition: GE ports on FX8-24 are not persistently disabled across a reboot, hareboot, or firware download operations.	
Recovery: Use FOS CLI to manually disable GE ports	

Defect ID: DEFECT000484991	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.2.0_hit	**Technology Area:** Web Tools
Symptom: Webtools displays internal ports without server blades as blinking amber LED	
Condition: When the internal ports are not connected to server blades.	
Recovery: Cosmtic issue where WebTools should not display color LED if server blade is not installed.	

Defect ID: DEFECT000485217	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Security
Reported In Release: FOS7.3.0	**Technology Area:** Fabric Authentication
Symptom: On the 7840 platform, if the bannerSet message is 1022 character or more, the CLI hangs. Banner less than 1020 can be set without any issue.	
Condition: For 7840 platform only and if bannerSet message size is greater than 1021 characters	
Workaround: Use a banner size less than 1021 characters	
Recovery: < ctrl-c> is required to exit bannerSet	

Defect ID: DEFECT000488832	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Virtualization
Reported In Release: FOS7.1.1	**Technology Area:** Virtual Fabrics
Symptom: During testing, embedded switch intermittently fails after reboot.	
Condition: After high reboot count, with less than 127 targets, switch will occasionally not respond to name server queries.	

Defect ID: DEFECT000489311	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Management
Reported In Release: FOS6.4.1	**Technology Area:** User Accounts
Symptom: Running "ifconfig eth0 down" on the console may lead to a panic and reboot of the switch.	
Condition: This may occur when the switch becomes unaccessible via the management port and the CLI command "ifconfig eth0 down" is executed from the serial console	

Defect ID: DEFECT000490648	
Technical Severity: Low	**Probability:** Medium
Product: FOS	**Technology:** Other
Reported In Release: FOS7.1.1	**Technology Area:** Other
Symptom: Admin role is not authorized to invoke the “errdump –all" command.	
Condition: Fabric OS Command Reference was not indicating that the “errdump –all" command displays messages for the entire chassis for a user with chassis permissions.	

Defect ID: DEFECT000491910	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.2.1	**Technology Area:** Logging
Symptom: SNMP query connUnitPortStatCountBBCreditZero or CLI portstats64show could display an unexpected large value for tim64_txcrd_z counter in a very brief time	
Condition: This issue will be seen when there is a FC traffic slowness in fabric and statistic counter wraps.	
Workaround: Customer could use portstatsshow command to get the correct counter value.	

Defect ID: DEFECT000492704	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS6.4.3	**Technology Area:** FC-FC routing
Symptom: "CRC error with good EOF" errors detected and may cause credit loss.	
Condition: This may be seen on DCX-4S: 1. With FC8-64 blades installed in - Slot 7 ports 155, 76 or - Slot 2 port 154. 2. Core blade 3/19,3/26, 6/70	
Recovery: Auto Tuning/Manual Tuning	

Defect ID: DEFECT000493407	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.0	**Technology Area:** SNMPv2, SNMPv3 & MIBs
Symptom: By default FOS SNMP will allow SNMP v1/v3 SET operation.	
Condition: FOS SNMP write access is enabled by default.	
Workaround: User have to use snmpconfig –set seclevel command to change the security level to "no access" in order to block SNMP SET option.	

Defect ID: DEFECT000494270	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Security
Reported In Release: FOS7.1.0	**Technology Area:** Fabric Authentication
Symptom: Customer might see devices reported as unauthorized when they try to login to a switch even when DCC policy is configured properly. Sometimes when the DCC policy is activated, some of the ports might bounce.	
Condition: The WWN that starts with "80" has the most possibility to hit this issue. The issue might also be seen when the device WWNs starts with "C0", "50", "20", or "10".	
Workaround: Avoiding the device WWN that starts with "80" or greater from DCC policy would resolve the issue.	

Defect ID: DEFECT000497464	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Other
Reported In Release: FOS7.3.0	**Technology Area:** Other
Symptom: 8G port blade displays auto max speed 16G when previous port blade was 16G and had auto max speed configured.	
Condition: A 16G port blade configured with auto max speed or 16G is blade swapped with an 8G blade.	
Workaround: Modify the port configuration to auto speed negotiate on the 16G port blade before blade swap with an 8 G port blade/	
Recovery: Modify the port configuration to a supported speed using portcfgspeed CLI or reset the port to default auto speed negotiation (ASN) using portcfgdefault CLI.	

Defect ID: DEFECT000497810	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.1.1	**Technology Area:** Diagnostic Port (D_Port)
Symptom: Core blade faults when dport tests are being run on ICL ports and ports are disabled.	
Condition: Disable port under testing	
Workaround: Don't disable ports when dport tests are in progress.	

Defect ID: DEFECT000498723	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** Port Log
Symptom: Portperfshow does not display traffic for E-Port while portdportesting is running.	
Condition: When portdporttest is running on ports.	
Workaround: Don't run portperfshow when a portdporttest is running.	

Defect ID: DEFECT000499012	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.0	**Technology Area:** Platform Services
Symptom: Unable to stop the autoboot using the ESC key to get into command shell.	
Condition: This is encountered during boot up, where the escape sequence key is not functioning properly.	

Defect ID: DEFECT000499177	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Other
Reported In Release: FOS7.3.0	**Technology Area:** Other
Symptom: Some hosts from an edge fabric may fail to discover the LUNs in another edge fabric.	
Condition: After doing a switchdisable of all the switches in the edge fabric and doing simultaneous switchenable of the disabled switches.	
Recovery: Toggle the port, host and target. If condition persists, switchdisable/enable the switch.	

Defect ID: DEFECT000499356	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.0	**Technology Area:** SNMPv2, SNMPv3 & MIBs
Symptom: CLI command "snmptraps --block/unblock -port [slot]port | ALL" appears to permit configuration for portsbeyond the valid range for a switch, without flagging any errors.	
Condition: This issue is seen when attempting to configure snmptraps for ports beyond the valid range for a given switch. No Error messages are shown to the user. However the problem itself is benign, with no functionality impact.	

Defect ID: DEFECT000499566	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** Flow Vision: Flow Generator
Symptom: The 'flow --delete all' command will deactivate all the predefined flows in the system.	
Condition: The 'flow --delete all' command will delete all the user defined flows after a confirmation but also has the side effect of deactivating all predefined flows.	
Workaround: Individually delete user defined flows instead of using --delete all.	

Defect ID: DEFECT000499809	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.0	**Technology Area:** Web Tools
Symptom: In a chassis with large scale of EX-ports, user may occasionally see Weblinker subsystem restart.	
Condition: If there are large scale of EX-ports configured in chassis, user may see Weblinker restart due to timeout. However this is a very rarely to happen.	

Defect ID: DEFECT000500085	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Management
Reported In Release: FOS7.2.0	**Technology Area:** NTP - Network Time Protocol
Symptom: Switches in the fabric are unable to communicate with the NTP server.	
Condition: When the BR5647 is insert into the embedded chassis or when the chassis CMM is rebooted, the CMM will push the NTP network configuration for internal communication to external fabric wide.	
Recovery: Reconfigure NTP address in any other non-embedded switch in the fabric.	

Defect ID: DEFECT000500362	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Other
Reported In Release: FOS7.3.0	**Technology Area:** Other
Symptom: Customer may see QOS High/Low priority enabled ports default to Medium priority after hareboot on switches.	
Condition: The priority change will occur while processing sync dump, if Special Zones (Redirect or Traffic Isolation) are present in the database along with QOS Zone.	
Recovery: To recover the correct priority, execute the cfgsave and cfgenable commands. If the priority is not restored, execute the cfgdisable and cfgclear commands, and then re-create the same zone configuration and enable zone configuration. If both steps fail, reboot the switch to recover the correct priority.	

Defect ID: DEFECT000500423	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.3.0	**Technology Area:** Routing
Symptom: Routing Queries issued through MVS may not return the correct set fabric paths for the identified SID/DID pair when DBR is used. Port metrics for all E-Port PDB's returned for a Diagnostic Query may exhibit information that is unrelated to the specified SID/DID pair.	
Condition: 1. FMS enabled 2. FICON . MVS environment, with switch managed by host 3. DBR Routing Policy configured in the fabric.	

Defect ID: DEFECT000500567	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.3.0	**Technology Area:** Routing
Symptom: Customer may see traffic disruption if ICL connections are not symmetric when 8G edge blade is present.	
Condition: When 8G edge port blade is present and ICL connections are not symmetric (which is a recommended use case).	
Workaround: Avoid configuring asymmetric ICL connections.	
Recovery: Reconfigure the ICL connection as symmetrical.	

Defect ID: DEFECT000501658	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Management
Reported In Release: FOS7.0.1	**Technology Area:** NTP - Network Time Protocol
Symptom: Switch panics after time server daemon failed to sync time with server.	
Condition: This may occur from an Ethernet network issue in the fabric resulting in a failure to resolve DNS names into IP addresses.	
Workaround: Use IP address instead of DNS server name in clock server configuration. Alternately do not configure DNSconfiguration in switch.	

Defect ID: DEFECT000502340	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** Flow Vision: Flow Generator
Symptom: It's possible to create and activate a WWN based generator flow on an E-port which is neither a source nor destination device and will generate frames.	
Condition: Creation of generator flow on an E-port with either source or destination device different from the ingress or egress port. For a generator flow, if both source device and ingress port are specified, then they should point to the same port. Similarly for destination device and egress port.	

Defect ID: DEFECT000503900	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** Flow Vision: Flow Generator
Symptom: Firmware downgrade to pre-FOS7.3.0 releases will fail with "simport enabled" message, when a slot with SIM port is powered off or empty.	
Condition: The issue will happen only when a slot having SIM ports is empty or powered off and firmware downgrade is initiated.	
Workaround: If possible, remove SIM port configurations before blade removal or powering down.	
Recovery: Reinsert or power-on the blade and remove the SIM port configurations.	

Defect ID: DEFECT000503942	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.0	**Technology Area:** EZSS Switch Manager
Symptom: Unable to configure 7840 using EZ Setup	
Condition: In some cases the EZ Setup for 7840 may fail with ambigous error message and display issues.	
Recovery: Relaunch EZ Manager to restart EZ Setup	

Defect ID: DEFECT000504187	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS6.3.2	**Technology Area:** QoS: SID/DID traffic prioritization
Symptom: Some ports on Brocade 5480 switch may exhibit CRC errors	
Condition: This stems from the serdes tuning on this switch not being set to optimum setting.	

Defect ID: DEFECT000504254	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Other
Reported In Release: FOS7.1.1	**Technology Area:** Other
Symptom: Intermittent systemverification failures may be encountered when the number of test runs are increased to 50 or more.	
Condition: This problem is encountered only when the parameters for systemverification test are modified to a different value which the system does not support. This works as expected under normal circumstance, with supported values.	

Defect ID: DEFECT000504585	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.0	**Technology Area:** SNMPv2, SNMPv3 & MIBs
Symptom: Slowness in SNMP polling and performance data collection.	
Condition: Seen in rare cases when APM is enabled.	

Defect ID: DEFECT000504635	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Security
Reported In Release: FOS7.3.0	**Technology Area:** Fabric Authentication
Symptom: In trunked FCR edge to backbone link (E-Port to EX-Port), new hash type in authentication does not display new hash type in portshow output when toggle the link(E-port) after changing the HASH.	
Condition: In a trunked E-port link, new master port does not show the proper authentication details when we toggle the current master E-Port link alone instead of whole trunk ports.	
Workaround: Toggle all ports in the trunk group at the same time.	

Defect ID: DEFECT000505389	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Other
Reported In Release: FOS7.3.0	**Technology Area:** Other
Symptom: Switch may be Disabled due to internal ports not being Online	
Condition: This may be encountered in rare circumstance on a Brocade 7840 switch	

Defect ID: DEFECT000505510	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** Monitoring and Alerting Policy Suite (MAPS)
Symptom: MAPS don't allow user to delete bad rules.	
Condition: When user creates more than recommended number of rules per policy, MAPS will not show all the rules present in the policy and will not allow bad rules to be deleted. The recommend maximum supported number is 200 rules per policy.	
Workaround: User MAPS pre-define rules.	

Defect ID: DEFECT000505940	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Other
Reported In Release: FOS7.3.0	**Technology Area:** Other
Symptom: Ambigous eError message when removing 7840 WAN Rate Upgrade 2 license using WebTools and there IP interface configured.	
Condition: When the 7840 has IP interfaces configured on GE ports and the WAN Rate Upgrade 2 license is removed through WebTools	
Workaround: Correct error message displays in FOS CLI when removing the WAN Rate Upgrade 2 license and IP interfaces are configured.	

Defect ID: DEFECT000507007	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** Flow Vision: Flow Generator
Symptom: User may only see 256 sub-flows when the predefined flow "sys_gen_all_simports" is activated in 512 port chassis and activation of the predefined flow may result in high CPU usage.	
Condition: When user activates the predefined flow "sys_gen_all_simports".	

Defect ID: DEFECT000507532	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** Monitoring and Alerting Policy Suite (MAPS)
Symptom: This is a display issue of dashboard. DB shows wrong or NULL flow name if user does slotpoweroff/on	
Condition: This is a cosmetic display issue seen on dashboard only when user performs slotpoweroff/on.	

Defect ID: DEFECT000508628	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Security
Reported In Release: FOS7.3.0	**Technology Area:** Fabric Authentication
Symptom: 7840 does not authenticate to RSA server configured for factor authentication for RADIUS.	
Condition: 7840 does not responds to RADIUS Access-Challenge packet	
Recovery: Not Applicable.	

Defect ID: DEFECT000508975	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Management
Reported In Release: FOS7.0.0	**Technology Area:** CLI
Symptom: When enabling Message of the Day (MOTD) on Fabric OS after upgrading from FOS Versions v6.x to v7.x , the MOTD is not displayed for the SSH session.	
Condition: This happens when switch starts at Fabric OS V6.x, and is then upgraded to v7.x FOS Versions where MOTD exists.	

Defect ID: DEFECT000509006	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.0	**Technology Area:** CLI
Symptom: E-Port disabled after enabling TTS FEC on an existing online E-Port.	
Condition: After enabling TTS FEC on an existing online E-Port.	
Recovery: Disable FEC TTS configuration on the E-Port.	

Defect ID: DEFECT000509898	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Other
Reported In Release: FOS7.3.0	**Technology Area:** Other
Symptom: Switchshow and portcfgshow displays ports configuration as "Auto Negotiate" when configured as fixed speed after firmeare download to FOS 7.3.0	
Condition: After a firmware download to FOS v7.3.0 from previous release, switchshow and portcfgshow displays port configuration as auto negotiate when configured as fixed speed. The actual link speed is the configured speed.	
Recovery: Perform a hareboot or hafailvoer after the firmware download to FOS v7.3.0.	

Defect ID: DEFECT000510291	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.3.0	**Technology Area:** FCIP
Symptom: 7840 FCIP tunnel or circuit bounces as well as C3 frame discard when running flow generator traffic across FCIP tunnels	
Condition: Running flow generator traffic over FCIP using small frames (<2kB). Running flow generator traffic at a rate that is higher than the available bandwidth over the FCIP tunnel.	
Workaround: Run a flow generator session that utilizes full FC frame sizes (2kB) and that also does not over commit the FCIP tunnel.	

Defect ID: DEFECT000510334	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Other
Reported In Release: FOS7.0.2	**Technology Area:** Other
Symptom: In an encryption environment (BES or FS8-18), the addition of a LUN to a crypto target container fails getting either device is busy or timeout when trying to configure.	
Condition: Issue can be seen when there are more ITLs configured in the LUN or encryption engine was stressed with heavy I/O.	

Defect ID: DEFECT000511542	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.2.1	**Technology Area:** supportShow
Symptom: Running supportsave on a director switch with faulted FC8-48E blades may lead to panic and cold recovery.	
Condition: This may occur when supportsave is run with blades in faulted state with reason code of PCI timeout (90) or power issues (28)	

Defect ID: DEFECT000511719	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.0	**Technology Area:** Web Tools
Symptom: Unable to view HA status of the 7840 FCIP tunnel from WebTools to determine if firmware download will be disruptive.	
Condition: WebTools does not display the HA status of a 7840 FCIP tunnel prior to firmware download	
Workaround: View the 7840 FCIP tunnel HA status from FOS CLI	

Defect ID: DEFECT000512293	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.0	**Technology Area:** Ethernet Interface
Symptom: For 7840 platform, the management link doesn't come up when eth0 (Magament inteface) speed and duplex is forced to 100Mbps/Half-duplex and rolling error message seen on console.	
Condition: When the 7840 platform eth0 is configured to 100Mbps half duplex.	
Workaround: Use speed of 100Mbps/Full-duplex instead of 100Mbps/Half-duplex.	

Defect ID: DEFECT000512507	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.2.0	**Technology Area:** Routing
Symptom: Observed performance issue on FX8-24 when there are exactly two equal bandwidth FCIP tunnels.	
Condition: Only applicable when there are two incoming paths (E-ports, trunks, EX-ports) on a given FX8-24 or BR7800 ASIC Chip.	
Workaround: Use one or greater than two incoming path to FX8-24 and 7800, or configure one of the links with a slightly lower bandwidth.	

Defect ID: DEFECT000512866	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** Monitoring and Alerting Policy Suite (MAPS)
Symptom: Customer could see MAPS alert related to SLOT, PS, FAN, WWN etc. during HA failover.	
Condition: During HAfailover and firmwaredownload, MAPS rule "BLADE_STATE==OUT" is triggered for an empty slot and FRU Health "Out of Range" violation logged happened.	
Recovery: There is no functionality error. User can ignore these alters.	

Defect ID: DEFECT000513327	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.3.0	**Technology Area:** FCIP
Symptom: FCIP Circuit will bounce due to Keep Alive Timeout.	
Condition: Customer is running bi-directional, hi-traffic load using large block sizes (512kB or greater) running over a network with 250ms delay and hitting 1% packet loss.	
Recovery: This is self recovers via circuit bounce.	

Defect ID: DEFECT000513450	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Other
Reported In Release: FOS7.3.0	**Technology Area:** Other
Symptom: FCOE device doesn't login after portcfgdefault	
Condition: After portcfgdefault, the VF-Port comes up as FCoE enabled, but the device doesn't login into the switch.	
Recovery: Toggling of the VF-Port by executing fcoe --disable/enable <port #> will allow the device to login	

Defect ID: DEFECT000513544	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.1.1	**Technology Area:** Management Server
Symptom: During code upgrade, standby CP may run into repeated msd panics and may not come online to standby ready mode.	
Condition: This occurs when AG node name is missing on active CP during execution of the FC-GS-3 Register Platform (RPL) command.	

Defect ID: DEFECT000513644	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.3.0	**Technology Area:** Lossless DLS
Symptom: Some parallel, equal cost paths may initially be unused for routing traffic to remote domains more than one hop away. The paths may be utilized for traffic to intermediate domains along the path but may be missing for a later domain. For those specific domains, the paths will not show up in any of the reports or CLIs that show routing data for those specific domains. (Examples include topologyShow, uRouteShow, director diagnostics for FICON, and others.) When the problem corrects itself , the customer's traffic may experience re-routes as the switch adjust routes to start using the previously missing paths. The correction of the problem to include the missing paths happens automatically within a time window of 30 minutes from when the problem happened. Many of cases where this happens should be corrected much sooner. When a re-route occurs, out of order frames are always a possibility for mutli-hop routes. In this case, since the reroutes happen at a later time than a cust	
Condition: The switches must have Lossless DLS enabled. Then, the problem can happen when parallel paths to an existing domain are added due to a new domain joining the fabric. For example: a diamond topology where one of the points of diamond is offline and being brought back online.	
Workaround: The switches will automatically correct the problem within 30 minutes. If the customer wants to control when the reroute happens, they could bounce one of the missing ISLs and this will cause FSPF to correct the problem. (Note: if the ISL is a trunk, all members of the trunk must be bounced to generate the necessary events.) Adding a new ISL that does not join an existing trunk group will also generates the necessary events to fix the problem.	

Defect ID: DEFECT000513806	
Technical Severity: Low	**Probability:** Low
Product: FOS	**Technology:** Other
Reported In Release: FOS7.2.0	**Technology Area:** Other
Symptom: Sorting switch events by date does not function properly in webtools	
Condition: This issue is seen in webtools, only when sorting events on the Time column, following an upgrade to Fabric OS version v7.2.0d. This sorting operation on the Time column does not function properly.	

Defect ID: DEFECT000513923	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Virtualization
Reported In Release: FOS7.2.0	**Technology Area:** Access Gateway
Symptom: ELS commands get rejected and host on AG switch can no longer communicate with the target in the 3rd party vendor fabric.	
Condition: This may happen in a Fabric with Access Gateway F-port with at least one NPIV login, and one of the NPIV logins has a PID with the domain and area portion equal to that of the target.	
Workaround: Reconfigure the fabric switch so that the domain and area portions of PIDs on Access Gateway F-ports do not match the domain and area portions of the target's PID.	
Recovery: Reboot the Access Gateway switch.	

Defect ID: DEFECT000514203	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.3.0	**Technology Area:** FCIP
Symptom: The 7840 console output shows many XTUN 1997 messages during I/O.	
Condition: An active FCIP Tunnel on a lossy or busy network.	
Recovery: No impact to IO	

Defect ID: DEFECT000514554	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.3.0	**Technology Area:** FCIP
Symptom: VE Port offline and then online after circuit modifications change the overall tunnel bandwidth.	
Condition: 1) The new Path MTU discovery feature is enabled on a circuit's IP pair 2) The tunnel has been up for more than 5 minutes 3) and the tunnel bandwidth is modified (a circuit data rate has been modified).	
Workaround: Ensure data is not running, or first disable the VE Port, change bandwdith, then re-enable the VE port. If the VE port was not disabled, a VE offline and then online event will occur.	
Recovery: The tunnel will automatically recover.	

Defect ID: DEFECT000514741	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.3.0	**Technology Area:** FCIP
Symptom: FFDC is observed for log drop message. The FFDC message is harmless in functionality, it is only for internal purpose to find out which message gets dropped.	
Condition: There could be many internal raslog messages that overrun the raslog queue, thus the message is seen	
Recovery: no action needed when this happens.	

Defect ID: DEFECT000515187	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** System
Reported In Release: FOS7.1.2	**Technology Area:** CLI
Symptom: While performing CLI command “seccertutil delkey”, the certificates/keys are truncated to zero but the "Certificate File" does not become "none". This may cause the switch to panic due to configuration inconsistencies.	
Condition: This may occur when executing the CLI command "seccertutil delkey".	

Defect ID: DEFECT000515227	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Other
Reported In Release: FOS7.3.0	**Technology Area:** Other
Symptom: After HA reboot, customer will not be able to see the enforced authentication details information in EX-port.	
Condition: HA reboot the swtich with authentication configured on EX-port.	
Workaround: Customer can find the authentication detail information on the Edge fabric E-port which is connected to the EX-port with authentication configured.	

Defect ID: DEFECT000515313	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** Fabric Watch
Symptom: While performing a supportsave, user may see benign display messages, interspersed with the supportsave output.	
Condition: This may be seen when the user attempts a supportsave operation after deleting frame monitoring.	

Defect ID: DEFECT000515403	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.1.2	**Technology Area:** supportShow
Symptom: Some command names are missing in SSHOW files of supportsave.	
Condition: This issue occurs in Director class platforms.	

Defect ID: DEFECT000515787	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.3.0	**Technology Area:** FCIP
Symptom: The CLI command 'portshow fciptunnel --reset' does not reset the connected count field properly in the FCIP tunnel statistics, and so it may show an invalid count after this command is issued.	
Condition: Issue may occur when the 'portshow fciptunnel --reset' command is issued to reset the FCIP tunnel counters.	
Workaround: Avoid using the '--reset' option with the portshow fciptunnel command.	

Defect ID: DEFECT000516108	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** Monitoring and Alerting Policy Suite (MAPS)
Symptom: QSFPs having serial number starting with "HUA" are being monitored using ALL_OTHER_SFP group. These should instead be monitored under ALL_QSFP or some other special QSFP group. All other QSFPs are correctly monitored under ALL_QSFP.	
Condition: This is encountered only with QSFPs having serial number starting with "HUA" .	

Defect ID: DEFECT000516196	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** System
Reported In Release: FOS7.3.0	**Technology Area:** CLI
Symptom: BNA users may witness failure in moving ports across LS's on Brocade 7840 switch.	
Condition: This may be encountered following the CLI command 'portCfgDefault' on GE ports of Brocade 7840 Switch.	

Defect ID: DEFECT000516255	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.3.0	**Technology Area:** FCIP
Symptom: Any replication devices using ELS (PRLI) and ELS _ACC frames as heartbeat during the replication might have potential traffic disrupted when doing non-disruptive firmwaredownload in FCR configuration.	
Condition: When replication devices on the edge fabric to 7840 through EX port. Replication devices must use ELS (PRLI) and ELS_ACC as heart beat for every few seconds. The windows for heartbeat loss is 3 minutes. IO will stop if replication device can not recover.	

Defect ID: DEFECT000516309	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Virtualization
Reported In Release: FOS7.0.0_pha	**Technology Area:** Access Gateway
Symptom: Hosts have problems logging into the fabric through an Access Gateway.	
Condition: This may be encountered under the following conditions: - Hosts are connected to an Access Gateway. - F-ports on Access Gateway have NPIV logins. - Different hosts login and logout of the same Access Gateway F-port, and - Access Gateway Persistent AL_PA feature is enabled.	
Recovery: Identify all affected F-ports with duplicate ALPA entries ag --printalpamap <port#> Disable _all_ the affected F-ports with duplicate ALPA entries portdisable <port#> ag --clearalpamap <port#> portenable <port#>	

Defect ID: DEFECT000516599	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.2.0	**Technology Area:** FCIP
Symptom: XTUN-1008 messages reported every 5 minutes in the RAS log and BNA console	
Condition: After extended uptime in a large FCIP FCP Fast Write and Open Systems Tape Pipelining configuration.	
Recovery: Reboot FCIP switch or power cycle the slot that is reporting the messages	

Defect ID: DEFECT000516611	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.1.2	**Technology Area:** Audit Log
Symptom: Always audit.cfg.class key not present in config files after upgrading to 712a	
Condition: Issue will be seen in warm recovery such as a firmware upgrade.	
Workaround: Reboot will write the key back to config file	
Recovery: Please configure any one class using auditcfg command.	

Defect ID: DEFECT000516632	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.0	**Technology Area:** CLI
Symptom: Userspace daemon mdd may crash after an extended period. This incident is benign since the daemon is automatically restarted	
Condition: This is a rare occurrence resulting from a very slow memory leak in L2 device monitoring. With the default polling rate of once per day the incident may occur about once a year. Accelerated polling will increase the frequency but the daemon is automatically restarted and the incident is rendered benign.	

Defect ID: DEFECT000516703	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.1.0	**Technology Area:** FCIP
Symptom: FICN-1062 and FICN-1063 abort messages on XRC and IFCC on host.	
Condition: This may be encountered in a large FICON disk mirroring configuration that includes base and alias devices in the connected primary controllers	
Workaround: None required – IFCCs will occur and normal channel error recovery will complete	

Defect ID: DEFECT000516934	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** Equipment Status
Symptom: FC16-64 DC power consumption is set to 160W but needs to be lowered to its actual maximum.	
Condition: FC16-64 is inserted in a 8510-8 or 8510-4 chassis, slotshow -p will display DC power consumption as 160W.	

Defect ID: DEFECT000517927	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Virtualization
Reported In Release: FOS7.2.1	**Technology Area:** Access Gateway
Symptom: Following an upgrade, BES panics when user attempts to enable access gateway.	
Condition: This is encountered on FOS v7.2.x and v7.3.x code streams; However, FOSv7.3 no longer support access gateway mode on BES switch, and FOS7.3.1 now enforces the no support.	
Workaround: Avoid enabling access gateway mode on encryption switches.	

Defect ID: DEFECT000519003	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Distance
Reported In Release: FOS6.4.3	**Technology Area:** FCIP
Symptom: FICON Tape Backup/restore jobs are failing using FICON Emulation enabled tunnels.	
Condition: FICON Emulation enabled tunnels on the 7500, FR4-18i, 7800, FX8-24 and 7840s with a new OEM virtual tape controller and micro code.	
Workaround: Disable FICON Acceleration	

Defect ID: DEFECT000519313	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Virtualization
Reported In Release: FOS7.0.2	**Technology Area:** Access Gateway
Symptom: Internal ports may not be properly enabled or disabled after boot-up.	
Condition: This may be encountered on a very busy system, where expansion commands from SVP may not get processed in time.	
Recovery: The problem is intermittent. The expansion command can be re-triggered if any of the server blades is moved.	

Defect ID: DEFECT000519655	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.1.0	**Technology Area:** FCIP
Symptom: FCIP GigE portstatsshow frame TX type counters show inaccurate counts.	
Condition: When using the CLI command: portstatsshow geX, where geX is ge1-ge5 on the 7800 platform	
Workaround: Use portstatsshow ge0 output. It includes the aggregation of the TX frame type counters for all GigE ports on the 7800 platform.	

Defect ID: DEFECT000519709	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.3.0	**Technology Area:** FCIP
Symptom: After multiple bounces, the FCIP circuit will show as degraded. This will cause the FCIP tunnel to show as degraded as well.	
Condition: The FCIP circuit/tunnel is bounced multiple times. This repeated bouncing can result in degraded condition.	
Recovery: Reboot the 7840 to recover from the FCIP circuit/tunnel degraded state.	

Defect ID: DEFECT000519965	
Technical Severity: Critical	**Probability:** Medium
Product: FOS	**Technology:** Other
Reported In Release: FOS7.1.1	**Technology Area:** Other
Symptom: FCoE AP blades may be faulted following a firmware upgrade.	
Condition: This may occur due to ethernet connectivity issues on FCOE blades that have been up for a long period of time.	

Defect ID: DEFECT000520145	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Security
Reported In Release: FOS7.3.0	**Technology Area:** Fabric Authentication
Symptom: "Authentication Failure" is displayed in switchshow output for an EX_Port.	
Condition: EX_Port is disabled with reason "Authentication Failure", when Edge Fabric is configured with FCAP authentication type alone and EX_port is configured with other authentication type.	
Recovery: Disable FCAP authentication in edge fabric switch.	

Defect ID: DEFECT000520219	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** Monitoring and Alerting Policy Suite (MAPS)
Symptom: customer cannot achieve Port Decom even though that action is configured in the rule	
Condition: This is encountered if Port Fence and Port Decom are the only actions configured in the rule	

Defect ID: DEFECT000520549	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Other
Reported In Release: FOS7.3.0	**Technology Area:** Other
Symptom: Software ASSERT error, followed by reboot, when a switch running FOS v7.3.0 in Access Gateway mode is connected to a non-Brocade Fibre Channel switch.	
Condition: The software ASSERT error may happen in a Access Gateway (AG) switch running FOS v7.3.0 only when the devices connected behind the AG switch perform FDMI registration with a non-Brocade Fibre Channel switch.	

Defect ID: DEFECT000520550	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.3.0	**Technology Area:** Routing
Symptom: SW7840 Hot Code Load encountered an ESM fatal error during Failback which resulted in cold recovery.	
Condition: This may occur when a pair of SW7840s are tunnel-linked in all 4 Logical Partitions, and an HCL is performed on just one of the two SW7840s.	
Recovery: No recovery is necessary, after the HCL completes a cold reboot, the switch and tunnel(s) are stable again.	

Defect ID: DEFECT000520567	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.3.0	**Technology Area:** FCIP
Symptom: The FOS CLI will allow an IPIF MTU to be configured below the supported minimum value of 1280 bytes.	
Condition: Anytime an IPIF is configured with an MTU lower than 1280 bytes.	
Workaround: The user should not attempt to create an IPIF with an MTU lower than 1280 bytes as this is not supported.	
Recovery: To recover, the IPIF can be deleted and recreated with an MTU set to at least 1280 bytes.	

Defect ID: DEFECT000521166	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS6.4.3	**Technology Area:** Name Server
Symptom: Corrupted frames cause nsd to panic and result in multiple switches in the fabric to cold boot.	
Condition: This may occur upon a rare hardware failure on a neighboring switch, resulting in corrupted nsd query response frames arriving at the other switches in the fabric.	
Recovery: Remove the failed blade or switch to eliminate the cause of these corrupted frames.	

Defect ID: DEFECT000521195	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** FICON
Reported In Release: FOS7.2.0	**Technology Area:** FICON
Symptom: Add ability to enable insistent domain ID (IDID) while the switch is online to permit non-disruptive upgrade v7.2.x to v7.3.	
Condition: As per design, upgrade to from FOS7.2.x to FOS v7.3 is blocked if customer has single switch fabric in FMS mode with SCC policy configured but IDID OFF. It requires a "switchdisable" in FOS v7.2.x to set IDID ON.	

Defect ID: DEFECT000521218	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.3.0	**Technology Area:** Extended Fabrics
Symptom: Host discovery issues after upgrade to FOS7.2.x in FC Routed configuration over VE/VEX ports	
Condition: These host discovery issues may be encountered following upgrade to any FOS7.2.x release from a FOS version prior to FOS7.2.0, in FC Routed configuration over VE/VEX ports	
Workaround: Downgrade to a FOS release prior to FOS7.2.0.	

Defect ID: DEFECT000521272	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.2.1	**Technology Area:** Fabric Watch
Symptom: FW-1430 raslog messages logged to indicate possible faulty temperature sensor, but with no subsequent FW-1003 messages to indicate which sensor is triggering the alarms.	
Condition: This may be encountered if the sensor issue is transient in nature and problem recovers before triggering subsequent faults.	

Defect ID: DEFECT000521398	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.1.1	**Technology Area:** Equipment Status
Symptom: Before shutdown switch due to a high temperature alert, emd encountered an assert and caused switch to panic.	
Condition: This may happen during switch shutdown following a high temperature warning "Unit will be shut down in 2 minutes if temperature remains high"	

Defect ID: DEFECT000521981	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** Flow Vision: Flow Monitor
Symptom: Defined flows on the master port are deleted	
Condition: Deactivate and delete defined flows on a slave port will delete flows on the master port.	

Defect ID: DEFECT000522361	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.1.0	**Technology Area:** Monitoring and Alerting Policy Suite (MAPS)
Symptom: 16Gbs Core blades experiencing heavy frame loss are not being faulted and impacted fabric traffic.	
Condition: When 16G blades experience excessive bad_os, enc_out etc link errors	
Recovery: Replace excessive link error blade. After upgrade to a release with fix, the blade will be faulted if link error reaches an internal monitoring threshold.	

Defect ID: DEFECT000522389	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Security
Reported In Release: FOS7.3.0	**Technology Area:** FIPS
Symptom: Openssl advisories CVE-2014-0076 and CVE-2014-3470 have been implemented as a precautionary step to patch a vulnerability identified by NIST.	
Condition: Although FOS use a version of OpenSSL that contains these vulnerabilities, none uses ECDH or ECDSA. Therefore, there is no exposure to these vulnerabilities.	
Workaround: Since there is no exposure to these vulnerabilities, no workaround is required.	

Defect ID: DEFECT000522602	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** System
Reported In Release: FOS7.3.0	**Technology Area:** CLI
Symptom: 'fabricshow -v' does not display FOS revision patch id under "Version" column.	
Condition: Display content overrun the declared array size.	

Defect ID: DEFECT000522753	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.3.0	**Technology Area:** Tunnel Management
Symptom: The FCIP Data Processor will encounter a software exception and then reload.	
Condition: While performing supportsave data collection, for the ARL module, if the FCIP Tunnels are in a particular phase of the disconnecting process this software exception will be encountered.	

Defect ID: DEFECT000522807	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** Monitoring and Alerting Policy Suite (MAPS)
Symptom: User space daemon mdd might auto restart due to memory corruption.	
Condition: This happen when more than 5 rules get trigger for more than 2-3 hours.	

Defect ID: DEFECT000522934	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.0	**Technology Area:** Web Tools
Symptom: The "user" role is not prevented from configuring the port non-DFE settings.	
Condition: Accessing WebTools as "user" role in the switch and slot views	
Workaround: DFE configuration will not be presented in Port General view	

Defect ID: DEFECT000523092	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** System
Reported In Release: FOS7.3.0	**Technology Area:** CLI
Symptom: Unable to collect supportsave on BR5460 with error msg: "The switch does not have enough disk space to run full supportSave. Available Free disk space is 27 MB."	
Condition: This is encountered when Compact Flash available free space is low	

Defect ID: DEFECT000523193	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** FICON
Reported In Release: FOS7.1.0	**Technology Area:** FICON emulation
Symptom: IFCC during tape reads - Emulation Error Code=86 during REPOSITION_PENDING_STATE	
Condition: When FICON tape read pipelining is active and the device presents Short Busy status	
Workaround: Disable FICON Read Pipelining	
Recovery: The I/O recovers on its own - no further action is required.	

Defect ID: DEFECT000523367	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** FICON
Reported In Release: FOS7.1.0	**Technology Area:** FICON CUP
Symptom: MVS displays messages IOS078I & IOS079I timeouts.	
Condition: In a very busy switch, with the CUP processing CCWs from multiple Host LPARs, e.g. many LPARS independently collecting RMF statistics from the CUP.	

Defect ID: DEFECT000523412	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.3.0	**Technology Area:** FCIP
Symptom: 7840 goes offline after about 30 days of run time.	
Condition: There is a small memory leak on the heartbeat between 7840 CP and DP, which cause the 7840 to run out of memory after about 30 days.	
Recovery: Reboot the 7840.	

Defect ID: DEFECT000523418	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.3.0	**Technology Area:** FCIP
Symptom: 7840 switch reboots due to Kernel panic.	
Condition: QSFP port (GE0 and GE1) plug-out and plug-in and the receipt of ABTS response from connected devices.	

Defect ID: DEFECT000523451	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Other
Reported In Release: FOS7.2.0	**Technology Area:** Other
Symptom: Customer may experience a cold boot on the DCX after bouncing FCoE port	
Condition: This may occur during a small timing window, when an external FCoE interface goes down, the corresponding internal FI ports is moved to temporary internal state and ELS frames arrive at the same time, triggerring a CPU busy condition.	
Recovery: Switch cold boots and recovers on its own. No further recovery action is necessary.	

Defect ID: DEFECT000523530	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Security
Reported In Release: FOS7.1.1	**Technology Area:** Encryption
Symptom: On LUN expansion, hosts showed the disk space as “un-allocated”	
Condition: The problem may be encountered in encryption environment (BES/FS8-18) when slow path and control frames are punted to software.	

Defect ID: DEFECT000523796	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.0.0	**Technology Area:** BB Credits
Symptom: Increased latency and negative performance impact may be encountered in an edge/core configured fabric.	
Condition: This may be observed when hosts exhibiting mild latency behavior are present, along with over-subscribed devices leading to congestion within the fabric.	
Workaround: Remove or Isolate latency devices into QoS zone to avoid impact to others in fabric	

Defect ID: DEFECT000523845	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Virtualization
Reported In Release: FOS6.3.2	**Technology Area:** Access Gateway
Symptom: appearance of the configuration parameter "ag.fporttrunking" differs depending on reboot/hareboot	
Condition: After non-disruptive firmware upgrade from FOS v6.2 to FOS v6.3, configuration key ag.fporttruking(introduced in FOS v6.3) created at boot stage is getting removed. And the issue persists when user performs non-disruptive firmware upgrade to higher firmware versions without reboot..	
Recovery: No other functional impact	

Defect ID: DEFECT000523906	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.0	**Technology Area:** Firmware upload/download
Symptom: The SupportSave for FICON is occasionally incomplete on a 7840.	
Condition: 7840 FICON SupportSaves are incomplete when taken from BNA. .	
Workaround: Although the SupportSave is showing incomplete, all the required information is captured.	

Defect ID: DEFECT000524168	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** Diagnostic Port (D_Port)
Symptom: AG ports get disabled, instead of coming up as N-ports.	
Condition: It happens when connecting AG to switch with On-Demand D_Port's ports.	

Defect ID: DEFECT000524177	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** Flow Vision: Flow Monitor
Symptom: Creating and activating flow monitor on inflight encryption and compression enabled ports is not blocked	
Condition: Flow monitoring is not supported on inflight encryption and compression enabled ports.	

Defect ID: DEFECT000524323	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.2.0	**Technology Area:** Firmware upload/download
Symptom: BNA 12.3.1 firmware download dialog shows switches multiple times with the same switch WWN but different firmware versions.	
Condition: When the fabric has GEN4 switches running v6.x firmware in non-VF mode.	

Defect ID: DEFECT000524328	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** Monitoring and Alerting Policy Suite (MAPS)
Symptom: User will not see rules triggered for utilization statistic.	
Condition: This only applies to FOS7.3.0 and later	

Defect ID: DEFECT000524891	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.3.0	**Technology Area:** FCIP
Symptom: 7840 kernel panic results in switch reboot.	
Condition: Zone update in large scale fabric in parallel with a lot of RASLOG messages on console can trigger this issue.	

Defect ID: DEFECT000524910	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** Equipment Status
Symptom: Switch reports fan direction incorrectly.	
Condition: This only applies to BR6505 and BR6510. CLI "chassisshow" shows "Forward" direction of the fans even though the actual flow is the correct Reverse or port-side exhaust air direction. Conversely, it shows "Reverse" direction of the fans even though the actual flow is the correct Forward or port-side intake air direction.	

Defect ID: DEFECT000525285	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** System
Reported In Release: FOS7.3.0	**Technology Area:** CLI
Symptom: CLI command "firmwaredwonload" may fail with SULB-1011 raslog message “Firmwaredownload command failed. Unexpected reboot occurred during firmware download. The command is aborted.” but with no apparent unexpected actual reboot.	
Condition: This may occur in a rare situation from a failure in setting an internal state variable. The resulting unexpected state leads firmwaredownload to infer there has been an unexpected reboot.	
Recovery: Rerun the firmwaredownload command.	

Defect ID: DEFECT000525347	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.0.2	**Technology Area:** FC-FC routing
Symptom: Customer may observe performance issues between multiple servers and storage with EX-port connected to VDX	
Condition: This may occur when there are link level errors that trigger credit loss on 16G EX port and there was prior HA warm recovery that disabled credit leak detection.	
Recovery: Bounce the port to recover	

Defect ID: DEFECT000525406	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.0.0	**Technology Area:** Buffer Credit Recovery
Symptom: When customers configure Edge Hold Time (EHT) on GEN5 switches running FOS v7.0.0, F-port and E-port do not receive configured values.	
Condition: When a user makes EHT change on a GEN5 switch running FOSv7.0.0 the problem is not corrected after upgrade to FOS v7.1 and greater which do not have this problem.	
Recovery: Upgrade to a release containing this fix, and re-run the configure command to set the correct EHT values. Alternatively, run slotpoweroff/on if the switch has already been upgraded to FOS v7.1 and above.	

Defect ID: DEFECT000525608	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.3.0	**Technology Area:** FCIP
Symptom: BLZ-5024 events on 7840 during FCIP non-disruptive firmware migration processing and tunnel bounce on the peer switch(es).	
Condition: When performing non-disruptive FCIP hot code load in a large FICON configuration.	

Defect ID: DEFECT000525834	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.0	**Technology Area:** Web Tools
Symptom: Invalid IP Address/Domain is populated in the "Please Login" WEB Tools dialog display, disregarding the configured details.	
Condition: When both ipv4/ipv6 are configured: 1. ipv4 address is shown when attempting to login via ipv6 2. ipv4 address is shown when attemping to login with domain name	

Defect ID: DEFECT000525998	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.3.0	**Technology Area:** FCIP
Symptom: 7840 kernel panic results in switch reboot	
Condition: GE SFP plug-out/plug-in and SupportSave in parallel will cause the panic due to synchronization issue.	

Defect ID: DEFECT000526158	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Other
Reported In Release: FOS7.0.2	**Technology Area:** Other
Symptom: Customer may observe increasing er_crc_good_eof and er_enc_in errors on backend ports, leading to performance problems.	
Condition: This may be be seen in a DCX 8510-8 system with FC8-64 port blades in slots 1, 2, 11, 12;	
Recovery: Additional tuning on DCX-4s with FC8-16, FC8-32, FC8-48 and FC8-64.	

Defect ID: DEFECT000526447	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.2.0	**Technology Area:** FCIP
Symptom: 7800 switch or FX8-24 blade FCIP DP complex has slow FCIP throughput	
Condition: This issue may be encountered with multiple very active FCIP Tunnels on a 7800 or FX8-24 FCIP DP complex	
Recovery: Power cycle slot or reset chassis.	

Defect ID: DEFECT000526500	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** FICON
Reported In Release: FOS7.3.0	**Technology Area:** FICON CUP
Symptom: "Detected term of ficucd" kernal panic on 7840 switch while running CUP	
Condition: Running heavy FICON CUP test traffic that generates a much larger number of Set Interval CCW requests than is normal	
Workaround: Reduce FICON CUP test traffic to avoid overloading the switch	

Defect ID: DEFECT000526546	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.0	**Technology Area:** Platform Services
Symptom: Unable to use error inject test tool to test FEC corrections if the tool doesn't support the TTS signal.	
Condition: TTS negotiation prevents analyzer and error inject test tools to verify FEC correction feature	

Defect ID: DEFECT000526777	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Management
Reported In Release: FOS7.2.0_hit	**Technology Area:** Platform Services
Symptom: When SVP sends the expansion commands, the BR6546 doesn't respond to the requests intermittantly. The result is that some of the internal ports may not be properly enabled/disabled.	
Condition: The issue happens when BR6546 is busy processing the previous request and can't respond to the new ones. And the additional polling period is larger than the SVP's retry interval so it can't catch the retry requests from SVP.	
Workaround: The issue has been fixed by optimizing the polling mechanism and the request response routines so that it won't miss the retries from SVP.	
Recovery: Combined with the fix on IOSW, the issue can be recovered if SVP sents retry request at proper intervals.	

Defect ID: DEFECT000526819	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** FICON
Reported In Release: FOS7.3.0	**Technology Area:** FICON CUP
Symptom: "Detected term of ficucd" kernal panic while running CUP	
Condition: Running heavy FICON CUP test traffic creates a Diags Query CCW for the CUP it is connected to, at the same time that an IDC Query message arrives from another CUP, that is also attached to a CHP running test traffic.	
Workaround: Reduce the FICON CUP test traffic.	

Defect ID: DEFECT000526934	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.3.0	**Technology Area:** FCIP
Symptom: CLI "portcfg ipif ge2.dp0 delete 2102:211:31:dead::2:7" returns "IP Address configuration on BCM failed" message	
Condition: Run a scrip to perform tunnel deletion/creation in a loop, issue was seen during second deletion	

Defect ID: DEFECT000527314	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.3.0	**Technology Area:** FCIP
Symptom: 7840 switch non-disruptive firmware migration failure results in cold reboot and FCIP tunnel disruption.	
Condition: When performing non-disruptive firmware migration on a 7840 switch.	
Workaround: Perform planned outage (disruptive) firmware migration.	

Defect ID: DEFECT000527376	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.3.0	**Technology Area:** FCIP
Symptom: 7840 switch panic and reboot.	
Condition: During long run testing of FICON host testing of FICON CUP with block/unblock of FC ports, 7840 switch encounters panic and reboot.	

Defect ID: DEFECT000527455	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Other
Reported In Release: FOS7.0.2	**Technology Area:** Other
Symptom: Switch incorrectly performs IP Ethernet protocol exchange: it sends GARP response to ARP request with Sender IP address of 0.0.0.0.	
Condition: When there is switch sending ARP request with Sender IP address of 0.0.0.0	

Defect ID: DEFECT000527506	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** System
Reported In Release: FOS7.1.0	**Technology Area:** Component
Symptom: I2C access failures leading to various symptoms such as: 1. slotshow command output may flag some components with an "*", indicating no i2c access to that component. 2. switchshow command output may indicate “Speed Mismatch / Incompatible SFP” 3. tempshow command output may display "unknown" 4. Console log (dmesg) may include: pcf954x_select_mux: Failed to select the I2C mux (addr=76, val=08, err=-1 id=0)!	
Condition: Brocade 6520 with the current version of software fails to properly reset or clear transient i2c faults. Consequently, Temporary or Transient errors on the I2C bus can result in what appears to be a permanent HW failure on a Brocade 6520.	
Recovery: Cold boot switch	

Defect ID: DEFECT000527848	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** FICON
Reported In Release: FOS7.2.0	**Technology Area:** FICON emulation
Symptom: FCIP FICON emulated Tape VM SPOOL DUMP jobs fail after FOS upgrade	
Condition: This may be seen upon upgrade to FOS v7.2.0d, when using FICON Tape Emulation for VM tape operations	
Workaround: Disable FCIP FICON Tape emulation or downgrade to a FOS version without fix for TR 414719	

Defect ID: DEFECT000527862	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.0	**Technology Area:** Web Tools
Symptom: Name server table column position is not persistent across relaunch	
Condition: This name server table column display issue is seen when the switch is in non AG mode.	

Defect ID: DEFECT000527974	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Security
Reported In Release: FOS6.4.0	**Technology Area:** Security Vulnerability
Symptom: Open SSL patches nine vulnerabilities: CVE-2014-3505, CVE-2014-3506, CVE-2014-3507, CVE-2014-3508, CVE-2014-3509, CVE-2014-3510, CVE-2014-3511, CVE-2014-3512, CVE-2014-5139.	
Condition: Due to these nine vulnerabilities, switch may allow an attacker to cause a Denial of Service (DoS) condition or force the client to revert to a less secure Transport Layer Security (TLS) 1.0 protocol.	

Defect ID: DEFECT000527997	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.0	**Technology Area:** Licensing
Symptom: FOS7.3.0 LicenseShow no longer shows capacity values for capacity based licenses on switches.	
Condition: Customer using "licenseshow" with FOS7.3.0 or later. Director products are not impacted.	

Defect ID: DEFECT000528010	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.3.0	**Technology Area:** FCIP
Symptom: FCIP HCL failure encountered due to a large number of FCIP objects in the configuration	
Condition: This is encountered when a large number of FCIP Objects (>> 20K FICON or FCP objects) are present.	
Workaround: Schedule a maintenance window for a disruptive FOS code load.	
Recovery: Recover environment after disruptive code load completes.	

Defect ID: DEFECT000528085	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.2.1	**Technology Area:** Name Server / Zoning
Symptom: Devices are unable to discover their targets due to failure of login (PLOGI) to the Name Server because the PLOGI never receives a response.	
Condition: This may be encountered when running FOS versions v7.2.1a or higher and back-to-back FLOGIs are sent from a device such that the second FLOGI is sent before the device receives an ACC for the first FLOGI.	

Defect ID: DEFECT000528207	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.1.0	**Technology Area:** Bottleneck Detection
Symptom: Inconsistent slot/port display format in Bottleneck Detection related RASLOG messages make it hard to read, track, and program to monitor these messages.	
Condition: This may occur when there is congestion or slow drain devices in a fabric.	

Defect ID: DEFECT000528245	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.2.0	**Technology Area:** Port bring up
Symptom: Switch may start logging SCN-1001 events for SCN queue overflow for process nsd, and MQ-1005 messages for nsd queue full. This may eventually result in CP panic.	
Condition: This may be seen in an environment with port devices that neither cut off light nor come on line, compounded with RNID storm between devices in a large flat zone. Consequently CPU gets overloaded with excessive interrupts and cannot schedule time for other user space daemons.	
Workaround: Disabling all problem ports with unstable light or fixing the speed of the port may help to limit the CPU load.	

Defect ID: DEFECT000528631	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS6.4.2	**Technology Area:** Name Server / Zoning
Symptom: Fibre Channel Common Transport (FC_CT) response to GPL query exceeds maximum allowed size and causes 3rd party HBA in a non-responsible state.	
Condition: This happens when HBA makes the GPL query to remote switch. Query to directly connected switch is not impacted.	

Defect ID: DEFECT000528657	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.2.0	**Technology Area:** Name Server / Zoning
Symptom: FCPD termination encountered when device sends malformed response with incorrect R_CTL information during FCP probing	
Condition: This occurs only when the device reponds with malformed frames during FCP probing	

Defect ID: DEFECT000528728	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.0.0	**Technology Area:** Logging
Symptom: Raslog messages C3-1006 followed by a C3-1010 message may be seen on a switch with no further operational impact.	
Condition: Single bit correctable parity errors may cause these raslog events on 16G blades. These error are self-corrected and should not be reported. .	
Workaround: Please contact Brocade support for further evaluation if necessary.	

Defect ID: DEFECT000529602	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.3.0	**Technology Area:** FCIP
Symptom: Problem can occur if the TCP connections between the switches are bouncing during the tunnel creation or establishment processing.	
Condition: During a time window, after a tunnel had informed its user of a connection request from the remote peer, the tunnel went down. The user then accepted the connection and was returned an error condition from the tunnel. The user did not properly check for an error return, and therefore did not close the connection out properly	

Defect ID: DEFECT000529905	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** System
Reported In Release: FOS7.1.1	**Technology Area:** CLI
Symptom: porterrshow may show discards occurring for a port disabled persistently, but portstatsshow output for the specific port indicate no discards.	
Condition: This discrepancy in output from the 2 CLI commands may be seen for persistently disabled ports.	

Defect ID: DEFECT000530735	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.3.0	**Technology Area:** FCIP
Symptom: 7840 switch unexpectedly reboots.	
Condition: Disabling and enabling of 7840 FC ports, which hosts are connected to, causes a slow memory leak. When continuously performs disabling and enabling FC ports for a long duration, eventually the 7840 switch runs out of memory and reboots.	

Defect ID: DEFECT000531004	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.1	**Technology Area:** Web Tools
Symptom: Switch view image is not seen for Brocade 6545	
Condition: Launching WebTools for Brocade 6545	

Defect ID: DEFECT000531192	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** FICON
Reported In Release: FOS7.2.0	**Technology Area:** FICON CUP
Symptom: During firmware upgrade, hosts lost paths due to FICON filter that was not properly cleaned up.	
Condition: On a FMS CUP enabled switch, if trunk master goes offline first, after hafailover FICON CUP filter is not properly removed.	
Recovery: Bounce trunk ports	

Defect ID: DEFECT000531265	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.3.0	**Technology Area:** Extended Fabrics
Symptom: During an upgrade of BR7800 from FOS v7.1.0 or later to FOS v7.1.2a, FOSv7.1.2b, FOSv7.3.0, v7.3.0a, v7.3.0b, v7.3.0c, the switch may go into a rolling reboot.	
Condition: This is encountered only if the switch was shipped with FOS7.1.0GA or later.	

Defect ID: DEFECT000531269	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Virtualization
Reported In Release: FOS7.3.1	**Technology Area:** Access Gateway
Symptom: Static mapped F-ports do not come back online after reboot, while all the non-static mapped ports come back online after the reboot.	
Condition: This is encountered when F-ports are statically mapped.	
Workaround: Toggle the F-port manually.	
Recovery: Disable and then enable the N-ports that the F-ports are static mapped to.	

Defect ID: DEFECT000531517	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.0.2	**Technology Area:** Port Bring-up
Symptom: Link to host failed to come up when configured at 'Fixed 4 Gbps'. Trace dump shows that the host issued NOS/OLS/LIP primitives after speed negotiation, but the switch did not respond.	
Condition: Switch port configured with "Fixed 4G" mode may get its RX incorrect when connected to 8G HBA in Auto Negotiate (AN) mode.	

Defect ID: DEFECT000531571	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.0.0	**Technology Area:** Port Bring-up
Symptom: Port blade remained faulted after a power event.	
Condition: This may occur in a rare scenario, when CP is up for a while and memory is utilized to cache file system buffers and a blade is power cycled. In this small timing window, this may lead to free memory not being readily available for blade initialization.	
Recovery: slotpoweroff/on the blade to recovery	

Defect ID: DEFECT000532108	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Security
Reported In Release: FOS6.4.3_dcb	**Technology Area:** Security Vulnerability
Symptom: Security vulnerability CVE-2014-3566 makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack.	
Condition: Following are the conditions that customers of Brocade SAN products could be exposed to this vulnerability: • An end user must use a web browser to access the FOS WebTools interface or use other HTTP clients such as Brocade Network Adviser to manage the switch. • A web browser or other HTTP client must support SSL protocol 3.0. • An intruder has to interject between an HTTP client and a SAN switch. • An intruder has to spend time monitoring the request-response formats to gain knowledge of the system operations. Total of 256 SSL 3.0 requests are required to decrypt one byte of HTTP cookies.	
Workaround: End users should configure web browsers or Brocade Network Advisor to disable SSLv3 support when accessing Brocade SAN switch. In addition, place Brocade SAN switch and other data center critical infrastructure behind firewall to disallow access from the Internet to minimize potential exposure to the attacks documented in this advisory.	

Defect ID: DEFECT000532730	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** FICON
Reported In Release: FOS7.2.0	**Technology Area:** FICON CUP
Symptom: Switch panic after Ficon daemon (FICUd) assert	
Condition: Issue is exposed due to heavy kernel processing, which caused ficud sending CUEnd to the same logical path over and over again.	

Defect ID: DEFECT000532816	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.2.0	**Technology Area:** Trunking
Symptom: Traffic disruption in normal traffic encountered following an HA-failover during firmware upgrade.	
Condition: This may happen when an E-port trunk port with FEC active bounces during HA-failover phase of the firmware upgrade process.	

Defect ID: DEFECT000532851	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Security
Reported In Release: FOS7.3.0	**Technology Area:** Security Vulnerability
Symptom: Security vulnerability CVE-2009-1895 makes it easier for local users to leverage the details of memory usage.	
Condition: The personality subsystem in the Linux kernel before 2.6.31-rc3 has a PER_CLEAR_ON_SETID setting does not clear the security-relevant compatibility flags when executing a setuid or setgid by a program, which makes it easier for local users to leverage the details of memory usage to (1) conduct NULL pointer dereference attacks,(2)bypass the mmap_min_addr protection mechanism, or(3)defeat address space layout randomization	

Defect ID: DEFECT000532888	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** FICON
Reported In Release: FOS7.1.0	**Technology Area:** FICON emulation
Symptom: I/O Errors to FICON extended device over an FCIP Tunnel with FICON Emulation features enabled.	
Condition: When running FICON channel programs to an extended device that includes Repeat Execution CCW commands (typically used in Disk I/O channel programs).	
Workaround: Disable the FCIP FICON emulation Idle Status Accept feature. The feature can be disabled via the following command: portcfg fciptunnel <slot/>vePort modify --ficon-debug NewFlags Where NewFlags includes the 0x1000 bit.	

Defect ID: DEFECT000533000	
Technical Severity: Low	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.2.1	**Technology Area:** Logging
Symptom: Execution of CLI command aaaconfig --auth "local;local" throws an error message that is misspelled.	
Condition: This is only encountered when the CLI command aaaconfig --auth "local;local" is run.	

Defect ID: DEFECT000533329	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** System
Reported In Release: FOS7.1.1	**Technology Area:** CLI
Symptom: CLI "portbuffershow" output showing higher than expected value of frame size.	
Condition: Sometime the output for command portbuffershow is over limit.	

Defect ID: DEFECT000533925	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** FICON
Reported In Release: FOS7.1.0	**Technology Area:** FICON emulation
Symptom: FCIP FICON Emulated Tape device failures with FICN-1062 in RASLOG and LastStates=0x0000423F443F	
Condition: When attempting to complete read processing and the device presents Device Busy then Device End, FICON emulation logic incorrectly generated a No-Op command with chaining instead of accepting the Device End Status.	
Workaround: Disable FICON Read Pipelining	

Defect ID: DEFECT000534282	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS6.4.3	**Technology Area:** Logging
Symptom: The raslog CDR-1008 may show up from time to time without presenting any problem for end to end traffic frames.	
Condition: This condition may occur due to CAM content discharge after the switch blade had been up for a long period of time, and needs to be refreshed.	
Recovery: If the raslog continues to show up, the user may power cycle the slot to recover.	

Defect ID: DEFECT000534413	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.2.1	**Technology Area:** Monitoring and Alerting Policy Suite (MAPS)
Symptom: "logicalgroup --show" command will show more ports than switch has under "ALL_PORTS" group. MAP-1003 RASLOG messages on non-existent ports.	
Condition: This issue happens if the customer has MAPS enabled and performs hafailover or migrate firmware to MAPS supported versions with online F_Port trunk.	
Workaround: Bring up the F_port trunk ports after hafailover,	

Defect ID: DEFECT000534507	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.4.0	**Technology Area:** FCIP
Symptom: Severe FICON workload disruption during 7840 HCL	
Condition: This is encountered when FCIP HCL is attempted on a single 7840 switch in a 7840 pair with HA and active FICON data flow,	
Workaround: Plan a disruptive firmware download.	

Defect ID: DEFECT000535664	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.3.1	**Technology Area:** FCIP
Symptom: BR7840 switch may go down as a result of DP crash from ECC errors in memory controller DIMMs.	
Condition: This may occur on BR7840 under rare situation, as a result of ECC errors.	

Defect ID: DEFECT000536455	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.0	**Technology Area:** Platform Services
Symptom: Both Active and Standy CPs panic in a director while processing Read Diagnostic Parameters (RDP) Extended Link Service (ELS) request from local device.	
Condition: This is triggered by a race condition when a local device repeatedly sends unsolicited RDP ELS request and the switch is running FOS7.3.0 or above.	
Workaround: Disable device port capable of RDP	

Defect ID: DEFECT000536632	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.4.0	**Technology Area:** POST - Power-on Self-Test
Symptom: Diagnostic test "systemverification" failed with "NON_DIAG errors detected during run"	
Condition: This is encountered when running systemverification test on BR7840	

Defect ID: DEFECT000536832	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.4.0	**Technology Area:** In-flight Compression
Symptom: Port does not come online and raslog is flooded with the following message: "Brocade6520, S0,P51(114): Port is offline due to Encryption Compression Block error."	
Condition: This is seen when Inflight Encryption is enabled on an Ex-Port.	

Defect ID: DEFECT000537093	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.1.1	**Technology Area:** OSTP - Open Systems Tape Pipelining
Symptom: Timeouts after Reservation Conflict Status with tape devices when Fastwrite and Tape-pipelining are enabled	
Condition: This occurs when multiple servers attempt to reserve the same tape device over OSTP enabled tunnel.	
Workaround: Disable OSTP on the FCIP Tunnel	

Defect ID: DEFECT000537847	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** System
Reported In Release: FOS6.3.2	**Technology Area:** CLI
Symptom: Special characters " and $ do not work properly when used in password for CLI "configupload". Other special characters like ! \ < > ( ) ` & ' | and space may appear to not work for passwords, when used in command line mode.	
Condition: " and $ may not work for interactive as well as command line modes in CLI such as "configdownload". Other special characters may appear to not work only for command line mode.	
Workaround: These special characters need to be ESC'd (add \ before each occurrence of special character) in command line mode in order to get through bash interception/interpretation.	

Defect ID: DEFECT000537848	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.4.0	**Technology Area:** FC-FC routing
Symptom: Host is unable to discover target devices in an Edge-to-Edge FCR topology.	
Condition: When some of the edge fabric switches having trunked IFLs are rebooted, resulting in Fabric ID conflicts in any of the backbone fabric FCRs, a few hosts may not be able to discover targets.	
Recovery: Enable any EX_ports that have been disabled as a result of fabric ID conflict and disable / enable the edge switch FC ports of affected hosts.	

Defect ID: DEFECT000538051	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** FICON
Reported In Release: FOS7.3.0	**Technology Area:** FICON emulation
Symptom: BR7840 FICON Emulation OXID usage overlap causes Interface Control Check error messages on the mainframe console.	
Condition: The issue can occur anytime when two or more devices are active in FICON emulation over an FCIP tunnel.	
Workaround: Disable FICON emulation features on the FCIP Tunnel.	

Defect ID: DEFECT000538092	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Virtualization
Reported In Release: FOS7.2.1	**Technology Area:** Access Gateway
Symptom: Following a FOS firmware upgrade or hareboot, traffic to and from the Access Gateway stops after the N-Port trunk master is disabled.	
Condition: This issue will occur when the following conditions occur: - hareboot for any reason, including firmwaredownload. - N-port trunk with at least two trunk members. - Trunk master of the N-port trunk is disabled.	
Workaround: Never disable the N-port trunk master when other trunk members are online. Instead, always disable all trunk members. Trunk slaves can be disabled with no issue.	
Recovery: To recover, do one of two things: 1. Bounce a host F_port on the Access Gateway. Or, 2. Disable all trunk members and then enable all trunk members.	

Defect ID: DEFECT000538492	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.3.0	**Technology Area:** OSTP - Open Systems Tape Pipelining
Symptom: Error recovery issue when the last write in a small write block is dropped.	
Condition: Data Integrity Error can be exposed when the Last Write Data Frame in a small write (8k) Across 7840 FCIP Tunnel when TP is on.	

Defect ID: DEFECT000539167	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Management
Reported In Release: FOS7.1.1	**Technology Area:** Web Tools
Symptom: Weblinker termination when the TACACS+ server is unreachable	
Condition: Happens only when user tries to login to switch which has unreachable TACACS+ server for authentication.	
Workaround: Use local or other remote authentication(LDAP/RADIUS) for login	

Defect ID: DEFECT000539290	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.2.1	**Technology Area:** Buffer Credit Recovery
Symptom: On internal back end (BE) link with 16G core blade to 8G edge blade, credit is not automatically recovered.	
Condition: In the case of 16G core blade to 8G edge blade direction, if there is credit loss on VC and the "creditrecovmod --cfg onLROnly" command is not enabled in an early release, then once the 16G credit leak interrupt is triggered, the credit leak interrupt enabled bits will not be enabled again.	
Workaround: Run creditrecovmod --cfg onLROnly before credit is depleted.	
Recovery: Slotpoweroff /on core blade to recover the BE link	

Defect ID: DEFECT000539576	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.2.1	**Technology Area:** supportShow
Symptom: TRCE-1005 will be triggerd when autoftp feature is enabled with SCP protocol.	
Condition: Happens only on systems configured with SCP protocol.	
Workaround: Use FTP or SFTP instead of SCP	

Defect ID: DEFECT000539670	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Management
Reported In Release: FOS7.4.0	**Technology Area:** Platform Services
Symptom: BR7840 becomes unusable after Firmware download from FOS7.4.0 to FOS7.3.x. Switch may show faulty rc=20015 status	
Condition: Failure may occur during the switch downgrade of FOS from FOS 7.4.0 to FOS7.3.0x on a BR7840.	
Recovery: Power cycle the failed BR7840.	

Defect ID: DEFECT000540035	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.1	**Technology Area:** Licensing
Symptom: There is a new business requirement to offer a 20 port version of the Brocade 5432 switch plus 4 "port on demand" licensed ports.	
Condition: POD was not supported before.	
Recovery: Upgrade to the new FOS version to limit the switch to 20 licensed ports. To enable the additional 4 ports, the customer would need to purchase and install the POD license.	

Defect ID: DEFECT000540245	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.1.0	**Technology Area:** FCIP
Symptom: Tunnels bounce caused FFDC event.	
Condition: This may occur if a FICON frame sequence is received with FC type of 0x1B or 0x1C, with one SOFi3 frame followed by more than 13 SOFn3 frames in sequence on an FCIP Tunnel. This is probably caused by a failed FICON adapter in a connected device.	

Defect ID: DEFECT000540469	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** FICON
Reported In Release: FOS7.1.0	**Technology Area:** FICON emulation
Symptom: Channel Detected Error message after a tape job failure.	
Condition: When running a tape write job that experiences a timeout (due to FC CRC errors occurring during the IO), the job will normally detect an MIH failure and go through error recovery and the error recovery could encounter the invalid token CDE.	
Workaround: Disable FICON Tape Pipelining or correct the cause of the FC CRC errors.	

Defect ID: DEFECT000540585	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.2.1	**Technology Area:** supportShow
Symptom: Support Save output does not include VE or GE port information	
Condition: This is seen after multiple logical switches have been created and one or more of the logical switches have been deleted and the VE ports reside in a logical switch that was created after one that was deleted.	
Workaround: Recreate empty logical switches up to the limit of logical switches in that chassis.	

Defect ID: DEFECT000540694	
Technical Severity: Critical	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.2.1	**Technology Area:** Top Talker Monitors
Symptom: Switch repeatedly logs the following raslog message: "[PS-1009], 16386, SLOT 7 | FID 128, WARNING, , Failed to add the device updates in condb database." This can mislead the customer on the number of devices supported by name server, zoning and device connectivity.	
Condition: This happens when there are large number of devices zoned together and with "Performance Monitor license". There is no impact to device connectivity, but Top talkers may not be able to display the top talking flows	

Defect ID: DEFECT000541322	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** FICON
Reported In Release: FOS7.4.0	**Technology Area:** FICON emulation
Symptom: IOS050I CHANNEL DETECTED ERROR message on mainframe console after 0x70 Status from XRC primary controller.	
Condition: This is seen during FCIP FICON XRC emulated tunnel processing of 0x70 Status from the connected DASD controller.	
Workaround: Disable FICON XRC Emulation on the FCIP Tunnel.	

Defect ID: DEFECT000541661	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Virtualization
Reported In Release: FOS7.2.1	**Technology Area:** Virtual Fabrics
Symptom: Active CP Panic may occur while running Brocade SAN Health report.	
Condition: This may be encountered in a large virtual fabric environment when running back to back CLI commands "lfcfg --showall -xxxx"	

Defect ID: DEFECT000542559	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.4.0	**Technology Area:** FCIP
Symptom: Tunnel bounce with an associated BLS-5024 FFDC event.	
Condition: This issue can occur after FCIP tunnel bounces due to WAN outage or other network issue.	

Defect ID: DEFECT000543727	
Technical Severity: Low	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** Logging
Symptom: The CP flash drive can run low on space due to the /var/log/esmd_lib.log file growing too large.	
Condition: The problem may occur on any switch other than the Brocade 7840 switch, when running with FOS7.3.0x and FOS7.3.1. The problem will not occur on the Brocade 7840 switch.	
Recovery: Manually delete the /var/log/esmd_lib.log file.	

Defect ID: DEFECT000544649	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** System
Reported In Release: FOS7.3.0	**Technology Area:** CLI
Symptom: Switch/CP panic with fabricd process terminated.	
Condition: When a lots of "fabriclog -s" commands are executed simultaneously.	
Workaround: Allow the CLI to finish before start another one.	

Defect ID: DEFECT000544986	
Technical Severity: Low	**Probability:** High
Product: FOS	**Technology:** System
Reported In Release: FOS7.3.1	**Technology Area:** Optics
Symptom: The CLI command "sfpshow <slot/port>" always returns a zero in "Length 50u (OM3)" field.	
Condition: This is seen only for OM3 50um QSFPs	

Defect ID: DEFECT000548463	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.1.1	**Technology Area:** Port Bring-up
Symptom: Kernel panic encountered on a CP while taking over the Active Role, due to heartbeat loss, causing a cold recovery of the system.	
Condition: This may be encountered only when processing FDISC with duplicate PWWNs.	

Defect ID: DEFECT000508980	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.2.0	**Technology Area:** CLI
Symptom: The SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak	
Condition: Users may be vulnerable when using SSH to login to a switch.	
Workaround: Users can use stronger MAC algorithms when using SSH clients connecting to a switch.	

Closed without Code Change in Fabric OS v7.4.0

This section lists the defects with Critical, High and Medium Technical Severity closed without a code change as of March 31, 2015 in Fabric OS v7.4.0

Defect ID: DEFECT000395600	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Other
Reported In Release: FOS7.0.1	**Technology Area:** Other
Symptom: Slow response to VLAN requests from CNA on 8000 switch	
Condition: Operating system network unable to get VLAN requests in a timely manner	

Defect ID: DEFECT000406288	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Security
Reported In Release: FOS6.4.2	**Technology Area:** Fabric Authentication
Symptom: Customer is not able to login with webtools or BNA with Radius.	
Condition: Radius server blocked cusotmer login with “Radius” only configuration, running commands with double quotes worked: aaaconfig --authspec "radius:local"	
Workaround: need to modify the control flag to SUFFICIENT in the pam configuration files login.radius , login.tacplus and login.adldap.	

Defect ID: DEFECT000449902	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Management
Reported In Release: FOS7.1.1	**Technology Area:** Web Tools
Symptom: WebTools and Brocade Network Advisory do not prompt user to place switch offline/online when changing the port configuration policy change in Access Gateway.	
Condition: When changing the port configuration policy between Auto policy and Port Group, WebTools and Brocade Network Advisor do not prompt user to place switch offline then online.	
Workaround: Manually place the switch offline then online when change the Access Gateway port configuration policy for updates to take effect.	

Defect ID: DEFECT000468595	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.2.0	**Technology Area:** SNMPv2, SNMPv3 & MIBs
Symptom: SNMP did not restore all SNMPv1 and accesscontrol settings with configdownload	
Condition: Trap recipient and access control keys will not be restored on configdownload.	
Workaround: Use the snmpconfig command to configure the settings.	

Defect ID: DEFECT000470918	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.2.0	**Technology Area:** POST - Power-on Self-Test
Symptom: POST tests do not run when standard and extended levels of testing are chosen from CMM.	
Condition: Issue happens when post test is triggered from CMM on embedded switch.	

Defect ID: DEFECT000482787	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Virtualization
Reported In Release: FOS6.2.2	**Technology Area:** Access Gateway
Symptom: Sometimes F-Port failover is not working on Access Gateway switch.	
Condition: On a switch running FOS v6.2.2x in Access Gateway mode: - Configure two N_ports (ports 17 and 18) - Map F_ports 1, 2, 3, 4 0 to Nport 18 - Map F_ports 5, 6, 7, 8 to Nport 17 - Failover policy is enabled (FO=1) and Failback policy is disabled (FO=0) - Policy is set to auto Disables port 18 with the expectation that F_ports 5,6,7,8 should failover, but switchshow indicates F_port disabled because there is no N_port	

Defect ID: DEFECT000486793	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.0.2	**Technology Area:** Fabric Watch
Symptom: CONF-1003 message will be seen when FW pause/continue options are used with -all in FOSv7.x.	
Condition: It happens only if the customer has stale keys from FOS v6.4.x or modified default FW keys.	
Workaround: Avoid using pause/continue with -all option.	

Defect ID: DEFECT000488667	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.2.1	**Technology Area:** Flow Vision: Flow Monitor
Symptom: LUN Flow monitors on DCX/DCX-4S ingress port shows zero count.	
Condition: When user installs a LUN flow monitor on the ingress port of DCX/DCX-4S, counters will always show zero count.	
Workaround: User can install LUN flow monitor on egress port.	

Defect ID: DEFECT000492786	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.0.2	**Technology Area:** Fabric Watch
Symptom: Customer can change the "thresh.env" and "thresh.res" (chassis settings) from the Logical Switch even if the user does not have chassis wide permissions.	
Condition: An account(admin/root) on a specific logical switch with chassis role user are allowed to change the chassis wide parameters when fwsettocustom and fwsettodefault are used.	

Defect ID: DEFECT000498132	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.1.1	**Technology Area:** Fabric Watch
Symptom: Configured actions for SFP monitoring will not be taken for a port if the 8G and 16G SPFs are interchanged for that port.	
Condition: It happens only when 8G SFP is replaced by 16G or vice versa.	

Defect ID: DEFECT000498502	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** Flow Vision: Flow Generator
Symptom: When user creates a WWN flow with a SID/DID and also creates a PID flow with same SID/DID while the DID is offline, both the flows would be activated but not enforced. These flows would be duplicate of one another.	
Condition: User creates a WWN flow and a PID flow with same resultant SID/DID.	

Defect ID: DEFECT000499816	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Other
Reported In Release: FOS7.0.2	**Technology Area:** Other
Symptom: CT commands do not appear to be forwarded to Name Server from FCoE device	
Condition: When attempting to bring an FCoE CNA online, the CNA is unable to discover any storage.	

Defect ID: DEFECT000500959	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Other
Reported In Release: FOS7.3.0	**Technology Area:** Other
Symptom: Framelog does not log unroutable frames.	
Condition: When there are unrouteable frames during the HA failover recovery period.	
Recovery: Unroutable frames will log after the system is in sync again	

Defect ID: DEFECT000501004	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** Flow Vision: Flow Generator
Symptom: portperfshow continues to display flow generator traffic running when flows were deactivated.	
Condition: HA failover following a series of activate/deactivate of a flow repeatedly, then deactivate the flow after HA failover.	
Recovery: Activate and deactivate the flow again.	

Defect ID: DEFECT000503823	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** APM - Advanced Performance Monitoring
Symptom: Fabric mode toptalker may not display actual toptalking flows if more than 1024 sid-did pairs are zoned with devices in the local switch.	
Condition: More than 1024 sid-did pairs are zoned for devices in local switch	
Workaround: Reduce the number of zone sid-did pairs	

Defect ID: DEFECT000512005	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Management
Reported In Release: FOS7.2.0	**Technology Area:** Platform Services
Symptom: "disable external ports" followed by "enable external ports" on embedded switch CMM interface (GUI or CLI), leads to changing external port speed from Auto Negotiate to 16Gb fixed.	
Condition: BR6547 embedded switch after "disable external ports" followed by "enable external ports" using CMM interface.	
Recovery: Reconfigure the external port speed to Auto Negotiate.	

Defect ID: DEFECT000512057	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.2.0	**Technology Area:** Fabric Watch
Symptom: Error messages start after firmware update from FOS v7.0.x to FOS v7.1.x and continue when upgrading to FOS v7.2.x. After downgrading back to 7.0.x, faulty port messages stop from Fabric Watch.	
Condition: Running FOS 7.1 and above, with a port remains in passive mode, which would simply complete speed negotiation and failing link init, results in FW-xxxx flood in RAS log.	
Workaround: Disable the port that does not cut off light	

Defect ID: DEFECT000512726	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.0.2	**Technology Area:** Fabric Watch
Symptom: Multiple FW-1038 and FW-1042 messages reported, indicating that the SFP RX and TX power are below boundary - current value 0 uwatts.	
Condition: This may occur only when a switch CPU is very busy.	

Defect ID: DEFECT000513542	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.0	**Technology Area:** CLI
Symptom: The "switchUptime" command executed via remote fosexec command (with --domain option) returns error message "error opening /etc/fabos/datefile".	
Condition: When remote domain is a logical switch that has no physical ports, the "switchUptime" command will not working through fosexec.	

Defect ID: DEFECT000513776	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Other
Reported In Release: FOS7.3.0	**Technology Area:** Other
Symptom: Name Server (NS) queue full condition leads to NS out of sync with local/remote devices and the device connectivity info will become inconsistent.	
Condition: When a new switch, which is in AllAccess mode and has local attached deviced, joins a large fabric consisting of a large number of devices (> 1000) and a large zone configuration (around 1MB) enabled, there is a possibility that the customer may see NS queue full condition. This happens due to Name Server discovery occurring before the existing fabric's zone configuration getting merged across to the new switch.	
Workaround: There are a couple workarounds for such a scenario and they are part of best-practices strategy for large fabrics. 1. When connecting a new switch to a fabric, put it in NoAccess mode. This will avoid the momentary transition to AllAccess and resultant RSCN storm to the fabric. 2. If connecting a new switch in AllAccess mode, take all devices connected to that switch offline to prevent RSCN storm.	
Recovery: Reboot the switch to recover from the error condition.	

Defect ID: DEFECT000515690	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.1.1	**Technology Area:** APM - Advanced Performance Monitoring
Symptom: In virtual fabric, some settings (fabricprincipal, sysmonitor, thconfig, portthconfig --pause/continue) are not updated in switch by configdownload operation.	
Condition: configupload with one configuration and configdownload with modified configuration.	

Defect ID: DEFECT000518620	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Other
Reported In Release: FOS7.2.1	**Technology Area:** Other
Symptom: Activation of the auto-tuning (serdestunemode --autoenable) on a switch that is also running MAPS could result in the MAPS daemon to restart. HA Sync will be temporarily lost during this time for each tuning value applied. Customer may see critical RASLOG errors such as [MAPS-1021] and multiple [MAPS-1020]	
Condition: This happens when MAPS and auto-tuning are both enabled.	
Workaround: Contact Brocade support to disable MAPS prior to running auto-tuning.	
Recovery: If auto-tuning is already started, let auto-tuning to run to completion. Do not stop auto-tuning prematurely and leave a sub-optimal value on the system, which could trigger blade fault.	

Defect ID: DEFECT000519293	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Management
Reported In Release: FOS6.4.3	**Technology Area:** Web Tools
Symptom: HAfailover is triggered by low memory condition.	
Condition: Switch is monitored by BNA and switch has ports with custom bottleneck settings	

Defect ID: DEFECT000521209	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** POST - Power-on Self-Test
Symptom: POST tests do not run as expected using CMM.	
Condition: Issue happens when POST tests are verified through CMM on embedded switches.	

Defect ID: DEFECT000521344	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.1.2	**Technology Area:** Fabric Watch
Symptom: Configuring porthconfig with area ST posts continuous alerts even after being in the same state.	
Condition: Configure ST area for portclasses(port/eport/fport/fcuport classes)	

Defect ID: DEFECT000523507	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.1.2	**Technology Area:** Fabric Watch
Symptom: Fabric Watch ST area of SFP class does not change to "pause" when executing CLI " thconfig --pause sfp -area all -port all" or gives any error to indicate that it's not supported.	
Condition: The issue is seen only when the ST area option is used with SFP class. ST is already deprecated in FOS v7.0.0 and no longer supported.	

Defect ID: DEFECT000523910	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Other
Reported In Release: FOS7.3.0	**Technology Area:** Other
Symptom: Debug messages appear on the console during portloopbacktest on a 16G platform.	
Condition: Portloopbacktest with default options from command line will result in debug messages displayed that has no impact to functionality	

Defect ID: DEFECT000524476	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** FICON
Reported In Release: FOS7.3.0	**Technology Area:** FICON
Symptom: Unable to view switch partitions and their port details through BNA.	
Condition: A logical switch having more than 256 ports, not including ICLs, that show the "No area available for PID assignment" message in switchshow.	

Defect ID: DEFECT000526298	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.1.2	**Technology Area:** Fabric Watch
Symptom: Event values that occur when portthconfig --pause is used are displayed after portthconfig --continue is executed.	
Condition: When a port is paused for certain class and area and enabled later it still has the previous values which it had during pause.	

Defect ID: DEFECT000527025	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** APM - Advanced Performance Monitoring
Symptom: CLI command fmmonitor --delmonitor <fmtype> -port 2/2 returns with "Specified Frame type doesn't exist on the specified port" even though a new fm-type was created and added to port 2/2.	
Condition: This may be seen when user moves the frame monitor installed port from one logical switch to another and then moves back the same port to the original logical switch	

Defect ID: DEFECT000528396	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS6.4.3	**Technology Area:** Fabric Watch
Symptom: Switch status changes to MARGINAL and back to HEALTHY with no contributing factor reported.	
Condition: Transient condition with no impact to traffic, switch, or fabric.	

Defect ID: DEFECT000529173	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Management
Reported In Release: FOS6.4.2	**Technology Area:** Web Tools
Symptom: 'resource not available' error message observed when configuring SCSI Monitors	
Condition: Configuring SCSI monitors with more than 4 LUN numbers	

Defect ID: DEFECT000529761	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Security
Reported In Release: FOS6.3.0	**Technology Area:** Security Vulnerability
Symptom: Bash shell security vulnerabilities (CVE-2014-6271, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187). These vulnerabilities allow certain malformed function definition to bypass privilege boundaries and execute unauthorized commands.	
Condition: To exploit these vulnerabilities in FOS requires access to the CLI interface after user authentication through console, Telnet, and SSH connections. An authenticated user account could exploit this bug to gain privileges beyond the permission granted to this account, such as executing commands with root privilege.	
Workaround: Place switch and other data center critical infrastructure behind firewall to disallow access from the Internet; Change all default account passwords; Delete guest accounts and temporary accounts created for one-time usage needs; Utilize FOS password policy management to strengthen the complexity, age, and history requirements of switch account passwords. Upgrading to a FOS version including this fix prevents exposures to the four CVEs noted in the defect Symptom. In addition, exposures to CVE-2014-6277 and CVE-2014-6278 are prevented.	

Defect ID: DEFECT000529904	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.3.1	**Technology Area:** Port Bring-up
Symptom: Bounced ISL links may not come back to full speed setting when port speed is set to AN.	
Condition: This can only happen during hafailover with a fabric rebuild. This results from all ISL's going down at the same time.	
Recovery: Bounce ports to recover from this situation.	

Defect ID: DEFECT000532529	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** System
Reported In Release: FOS6.4.3_dcb	**Technology Area:** Component
Symptom: Switch detected sshmd panic after experience PCI abort error with FCOE switch with raslog [EANV-1006] and fail over application did not kick in caused fabric disruption.	
Condition: Switch is not properly faulted after FCOE ASIC reached PCI abort error threshold.	

Defect ID: DEFECT000533496	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Other
Reported In Release: FOS7.2.1_HIL	**Technology Area:** Other
Symptom: When delete domain is performed along with CSP zeroize option on FIPS enabled module, N-ports do not login.	
Condition: This issue was caused by asynchronous handling of delete domain and CSP zeroize, which were started simultaneously.	
Workaround: Do not zeroize CSPs when deleting domain.	
Recovery: Delete domain without CSP zeroize.	

Defect ID: DEFECT000538046	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** System
Reported In Release: FOS7.1.1	**Technology Area:** Component
Symptom: Fabric Watch terminates in a busy system causing switch reboot.	
Condition: Uncommonly occurs on systems that is very busy.	

Defect ID: DEFECT000539396	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS6.4.3	**Technology Area:** Port Bring-up
Symptom: Standby CP goes into rolling reboot and encounters an assert. The CPs are unable to gain HA synchronization.	
Condition: Can be triggered by HA sync timing issue or bad hardware	

Defect ID: DEFECT000540101	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.2.1	**Technology Area:** Monitoring and Alerting Policy Suite (MAPS)
Symptom: SNMP query reports a fan speed of 0.	
Condition: Erroneous fan speed report occurs only when switch hits transient I2C failure and it will be recovered automatically.	

Defect ID: DEFECT000540198	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.1.2	**Technology Area:** Fabric Watch
Symptom: FW RAS message encountered, indicating switch status state change while LOS (Loss of signal) area of fop-port class is paused. This is not the case when LF(Link failure) area of fop-port class is paused,	
Condition: This is encountered when LOS area systemmonitor is configured as pause, and switch status policy is configured as based on port class.	

Defect ID: DEFECT000540638	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** System
Reported In Release: FOS6.4.3	**Technology Area:** Component
Symptom: Software verify on console log, followed by Kernel Panic on 4G platform.	
Condition: This may be seen with 4G platforms after it is in operation for a longer period of time spanning over a year.	
Recovery: In director, power cycle the blade in question to recover. In switch, the panic will automatically recover from this condition.	

Defect ID: DEFECT000542014	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** System
Reported In Release: FOS6.4.3_dcb	**Technology Area:** Component
Symptom: FCOE based switch is falsely faulted with PCI abort error after the system is running low on memory.	
Condition: FCOE switch is managed through BNA via in-band management, and doing SNMP query	
Workaround: Do not manage the switch via any application that send SNMP query.	
Recovery: Power cycle switch	

Defect ID: DEFECT000544788	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.2.1	**Technology Area:** Frame Monitoring
Symptom: CP reboots after perfttmon -del <port> and then running perfttmon --show <port> in fabricmode top talkers.	
Condition: Happens only when TT monitor is configured for fabricmode and show CLI is executed with port number that is already deleted.	

Appendix: Additonal Considerations for z Systems (FICON) Environments

New Features Support

Not all possible combinations of features and hardware configurations are included in the FICON qualification process. Features and hardware configurations not supported for FICON may be supported for open systems environments. This appendix articulates those features and configurations tested for FICON environments and include supplemental information for users deploying FOS-based platforms in FICON environments.

FOS v7.4.0a is IBM z Systems qualified release with several new features and enhancements for FICON environments. The new supported features and functions in this release are:

- 2KM QSFP for ICLs
- Base Switch support on the 7840
- MAPS – FMS as a MAPS action (FMS CUP)
- Dynamic Load Sharing – E_port balancing
- Forward Error Correction (FEC) for FICON Express16S
- High Integrity Fabric (HIF), required feature for FICON

Notes on New Features Supported

2 KM QSFP for ICLs

Prior to Fabric OS 7.3.0, all the FE ports and ICL ports used the same buffer credit model. In Fabric OS 7.4.0a and later, in FICON environments ICL ports support a 2 km distance. To support this distance, you must use specific QSFPs and allocate a greater number of buffer credits per port.

The following points should be considered if you are attempting to support 2 km links on ICL ports:

• Only the QSFPs that have the version number "57-1000310-01" and the serial number

"HME114323P00044" support 2 km on ICLs. The second character ('M') in this serial number indicates that the QSFP supports 2 km distance. You can also use the **sfpShow** command to identify the QSFPs that support 2 km on ICL ports.

• The new credit model does not affect the HA configuration.

• You cannot downgrade from Fabric OS 7.3.0 to any earlier version if either of the following conditions is true:

- When you have plugged in the QSFPs that support 2 km on one ore more ICL ports.

- When you have configured buffer credits using the **EportCredit** command on one or more ICL

ports.

• The **portCfgEportCredits** configuration cannot have less than 5 buffer credits or more than 16 buffer credits per VC. If there are insufficient buffer credits available, the default configuration is retained and the message *Failed: already exceeds Buffer credits allowed* is displayed.

• Only a maximum of 10 ICL ports can be configured with 2 km QSFPs with 16 buffer credits per VC.

• Only a maximum of 14 ICL ports can be configured with 2 km QSFPs with 13 buffer credits per VC.

When you configure the 15th port using **portCfgEportCredit**, the message *Failed: already exceeds Buffer credits allowed* is displayed. The remaining two ports can have only 34 buffer credits. To remedy this, disable some ports and configure the remaining ports using 13 buffer credits per VC.

• If you are using the **portCfgEportCredit** command, a maximum of 16 buffer credits can be configured on all the ICL ports when all the 16 ICL ports are in the disabled state. After enabling all the ports, until the buffer credits are available, the ports will come up with the configured buffer credits. The remaining ports will come up in degraded mode. In case of remaining QoS-enabled ports, the ports will come up without QoS enabled. If all the ICL ports are QoS enabled, there will only be 448 buffer credits available for 2 km distance support.

• Due to the 2 km QSFP module limitation, the link failure counter is not reliable during module or cable removal or insertion.

Base Switch support on the 7840

FOS v7.4 enhances Virtual Fabric support on 7840 switches to include the base switch, i.e., to support XISL. FICON users can configure E_port (ISL over FC), and VE_port (ISL over GE) in base switch. The maximum number of logical switches supported — including the base switch — remains four. Two of the logical switches can support CUP.

MAPS-FMS as a MAPS action (FMS CUP)

The Monitoring and Alerting Policy Suite (MAPS) is an optional storage area network (SAN) health monitor supported on all switches running Fabric OS 7.2.0 or later. MAPS allows you to enable each switch to constantly monitor itself for potential faults and automatically alerts you to problems before they become costly failures.

MAPS tracks a variety of SAN fabric metrics and events. Monitoring fabric-wide events, ports, and environmental parameters enables early fault detection and isolation as well as performance measurements.

MAPS provides the following set of predefined monitoring policies that allow you to immediately use MAPS on activation:

• dflt_conservative_policy

• dflt_moderate_policy

• dflt_aggressive_policy

It is recommended that all IBM z Systems customers enable MAPS after upgrading to Fabric OS version supporting MAPS and use the default aggressive policy (dflt_aggressive_policy). This policy contains rules with very strict thresholds.

FOS v7.4 introduces FICON notification as a new action that enables MAPS events to be sent to FMS with detailed event information upon rule violations. FMS CUP can translate these MAPS events into FICON-specific Health Summary Check reports via the z/OS I/O Health Checker. In order to send the MAPS triggered events notification, MAPS supports the new action configurable at rule and maps global action level.

The rules with FICON notification action are part of all three default policies such as *dflt_aggressive_policy, dflt_moderate_policy and dflt_conservative_policy*. In the active policy, if FICON notification action is configured for any triggered events, then MAPS sends the notification to FMS with event information. The following information are send to FMS:

- Triggered event rule name
- Object and its type on which the event was triggered
- Severity of the event
- Condition on which the event was triggered
- Monitoring service details and the measured value

Dynamic Load Sharing-E_Port balancing

With this enhancement, when multiple paths to a domain exist, routing policy would assign routes so that the bandwidth demands from source ports are evenly distributed among all E_Ports.

E_port balance priority allows you to balance the E_port load. You can enable the E_port balance priority feature from Web Tools. When you enable the E_port balance priority feature, the E_Port load will be even across all the E_Ports of same domain during the topology change. You can select **Rebalance** or **Rebalance**

ALL to re-balance the E_Port load on a particular logical switch or on all the logical switches, without waiting for a topology change to occur.

When the **Dynamic Load Sharing (DLS)** is disabled, **Lossless Dynamic Load Sharing (DLS)** is not supported and the **E_port Balance Priority** feature also gets disabled; but the **E_port Balance Priority** can be enabled even if the DLS is in **Off** state.

The E_port balance priority is supported on the following z Systems qualified platforms at FOS 7.4.0a:

- Brocade DCX Backbone
- Brocade DCX-4S Backbone
- Brocade DCX 8510-4 Backbone
- Brocade DCX 8510-8 Backbone
- Brocade 7800
- Brocade 7840

To enable or disable E_port balance priority , perform the following steps.

1. Open the **Switch Administration** window.

2. Select the **Routing** tab.

3. Select **On** in the **E-port Balance Priority** area to enable E_Port load balance, or select **Off** to disable E_Port load balance.

- Clicking the **Rebalance** button will perform E_Port balancing on the current logical switch only and clicking the **Rebalance All** button will perform E_Port balancing on all the logical switches available.

4. Click **Apply**, and then click **OK.**

Forward Error Correction (FEC) for FICON Express16S

With the FICON Express16S generation of features, IBM z Systems added Forward Error Correction (FEC) capabilities to the Fibre Channel link protocol. FEC allows FICON channels to operate at higher speeds, over longer distances, with reduced power and higher throughput, while retaining the same reliability and robustness that FICON has traditionally been known for.

FEC is a technique used for controlling errors in data transmission over unreliable or noisy communication channels. The technique has the sender encode messages in a redundant way by using an error-correcting code (ECC). The redundancy allows the receiver to detect a limited number of errors that might occur anywhere in the message and often corrects these errors without retransmission. FEC gives the receiver the ability to correct errors without needing a reverse channel to request retransmission of data, but at the cost of a fixed, higher forward channel bandwidth.

With FEC enabled, errors that might have started to show up with the new faster link speeds can likely be corrected by the error correction technology in the optical transmit/receive ports. End users should see fewer I/O errors, thus easing the transition to the new link technologies, reducing the potential impact to any production workloads by I/O errors. For latency reduction, the entire path (end-to-end) needs to run at 16 Gbps link speed. Likewise, each link, the entire path from the channel through the switch ports to the storage subsystem, should be protected by an FEC-capable link to minimize the risk of I/O errors.

- Though FEC capability is generally supported on Condor3 (16G capable FC) ports when operating at either 10G or 16G speed, it is not supported with all DWDM links. Hence FEC may need to be disabled on Condor3 ports when using DWDM links with some vendors by using 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 7.x Compatibility Matrix for supported DWDM equipment and restrictions on FEC use.

- To connect between a switch and an HBA at 16 Gbps, both sides must be in the same mode (fixed speed, and FEC on or off) for them to communicate at that rate. If only one port has FEC enabled, neither port will be able to see the other. If the ports are in dynamic mode, then they may connect, but not at 16 Gbps.

  NOTE: Enabling/disabling FEC is a disruptive operation

portCfgFec

Use this FOS CLI command to enable or disable Forward Error Correction (FEC) or Transmitter Training Signal (TTS) on a specified port or on a range of ports, or to display the configuration.

FEC provides a mechanism for reducing error rates during data transmissions over 16 Gbps Fibre Channel links. When FEC is enabled on a port, the sender adds systematically generated error-correcting code (ECC) to its data transmission. This mechanism allows the receiver to detect and correct errors without needing to get additional information from the sender.

By default, TTS is disabled switch-wide on all 16 Gbps platforms. If the TTS mode is enabled, the port negotiates FEC through TTS. The 16 Gbps TTS is not compatible with the more commonly used 16 Gbps 64B/66B. Thus, the TTS mode should only be enabled if a similarly TTS-capable and enabled device is connected to the port.

The Brocade implementation of FEC is supported on 16 Gbps platforms and enables the switch to recover bit errors in 16 Gbps and 10 Gbps data streams. The FEC encoding can correct one burst of up to 11 error bits in every 2,112-bit transmission. The error correction covers both frames and primitives. There is no loss of bandwidth or added transmission data rate overhead to the 16 Gbps FC link.

By default, FEC is enabled switch-wide on all 16 Gbps platforms. If FEC is already enabled on the ports, enabling FEC has no effect. If a range of ports is specified, some of which are already in the requested configuration, a notification is generated, and no action is taken for those ports only. All other ports in the specified range are updated. **Enabling or disabling FEC is disruptive to traffic.**

When used with the **–show** option, the command displays the following information for the specified ports:

Port
: The port index number

FEC Capable
: Displays YES if the port supports FEC. Displays NO if the port does not support FEC.

FEC Configured
: Displays ON if FEC is enabled on the port (default). Displays OFF if the feature is disabled.

FEC via TTS Configured
: Displays OFF if TTS is disabled on the port (default). Displays ON if the FEC negotiation via TTS feature is enabled.

FEC State
: The FEC state can be active or inactive. An active FEC state indicates that FEC is enabled and actually running. An inactive state can indicate two conditions: FEC is enabled, but not running due to some error condition (for example, FEC may not be enabled on both ends of the link). Or FEC is disabled and therefore inactive.

Use the **portCfgShow** command to display the FEC configuration along with other port parameters. Use the **islShow** command to view interswitch link-level FEC configurations. Use the **portErrshow** and **portStatShowhow** commands to monitor data transmission errors. You should see a significant reduction in CRC errors on FEC-enabled links.

FEC is supported the following links:

- Between E_Ports on all 16 Gbps platforms running Fabric OS v7.0.0 or later. Both sides of the link must be configured with port speeds of 10 Gbps and 16 Gbps.
- Between F_Ports and N_Ports in Access Gateway mode (requires Fabric OS v7.1.0 and later on the AG and the switch.

- Between Brocade 16 Gbps capable HBAs (Catapult2) Host Bus Adapters and an F_Port. The HBA must be running v3.2 or later and the switch must be running Fabric OS v7.1.0.
  FEC is compatible with QoS, Credit Recovery, and Fabric-Assigned Port WWM (FA-PWWN).
  FEC is not supported on D_Ports configured with Dense Wavelength Division Multiplexing (DWDM). The TTS mode is supported only for F_Ports. If a port initializes as an E_Port, it is disabled with a warning message and its peer port will be in "No_Light". status.

  For additional details, including examples please see the Fabric OS 7.4 Command Reference Manual.

High Integrity Fabric (HIF)

The High Integrity Fabric Feature (HIF) is required for proper operation with FICON channels. Therefore, it is recommended that customers verify HIF is enabled upon upgrade to FOS 7.3.0b or higher. If HIF is not enabled, FICON channels will go into an invalid attach state after a channel or port event occurs that requires the channels to log in to the FICON fabric.

Meeting high-integrity fabric (HIF) requirements

In a cascaded switch configuration, FICON channels use an Extended Link Service Query Security Attributes (ELS QSA) function to determine whether they are connected to a high-integrity fabric. Each switch in a high integrity fabric must have the following attributes configured:

- An insistent domain ID (IDID)
- A valid SCC policy (configured and activated)
- A fabric-wide consistency policy greater to or equal than switch connection control - strict mode (SCC:S)

NOTE

You enable the fabric-wide consistency policy on the fabric once the switch joins the fabric.

NOTE

If FMS mode is enabled before upgrading to v7.3.0, IDID, SCC_Policy, and SCC:S will be validated and the firmware attempt failed if either are incorrect. If validation is successful, HIF mode will automatically enable when the firmware installs. If a FICON channel tries to connect to a fabric switch without these features configured, the channel segments from the fabric.

Once these features are configured, you must enable the switch in High-Integrity Fabric (HIF) mode using the Fabric OS configure command. This verifies the required features are set and locks the configuration to ensure connection with the FICON channel. Once the HIF mode is set, you cannot change the IDID, fabric-wide consistency policy, and SCC policy without disabling HIF mode.

Following are considerations for using HIF mode:

- You must enable HIF mode to enable FMS mode.
- Before a Fabric OS downgrade, you must disable HIF mode. Note that this operation is not recommended for FICON and should only be used when downgrading firmware. You will receive a warning to this effect if FMS mode is enabled. If HIF is disabled, any new channel initialization would fail as the Query Security Attribute (QSA) reply from the switch to the channel will fail. The existing channel will continue to operate, however.
- Before a Fabric OS upgrade, be sure the switch has appropriate IDID, fabric-wide consistency policy, SCC policy settings are enabled so that HIF mode can enable when the firmware installs.

The following instructions are provided in the remainder of this section to configure a switch as part of a high-integrity fabric:

- Enabling insistent domain ID
- Creating and activating the SCC policy
- Enabling the fabric-wide consistency policy
- Enabling High-Integrity Fabric mode

Enabling the insistent domain ID

To enable the insistent domain ID, complete the following steps for each switch in the fabric:

1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter the configure command and step through the interactive prompts.

a. At the "Fabric parameters" prompt, type y.

b. At the "Insistent Domain ID Mode" prompt, type y.

Creating and activating the SCC policy

Creating a switch connection control (SCC) policy defines switches allowed in the fabric.

To configure and activate an SCC policy, use the following steps:

1. Connect to the switch and log in.

2. Perform one of the following steps:

•Enter the secpolicycreate command to add all switches in the fabric, if they are connected. secpolicycreate "SCC_POLICY","*"

•Enter the secpolicyadd command to add one or more members to an existing policy. The following command is an example of adding a member using device WWNs. secpolicyadd "SCC_POLICY","wwn1;wwn2"

3. Enter the secpolicyactivate command to activate the currently defined SCC policy. This activates the policy set on the local switch or all switches in the fabric, depending on the configured fabric-wide consistency policy.

Enabling the fabric-wide consistency policy

Enable the fabric-wide consistency policy after all the switches have joined the merged fabric. If there are fabric-wide data distribution (FDD) conflicts on any of the ISLs, disable the fabric-wide consistency policy on each switch in the fabric. Once the fabric has merged successfully (use fabricShow to verify), enter the following command:

fddcfg --fabwideset "SCC:S"

Following are considerations for enabling the fabric-wide security policy:

• SCC:S enforces strict mode, which is required for FICON.

• Fabric-wide consistency policy cannot be set to strict mode on an edge fabric if the fabric connects to a FCR, although FCR front and translate domains can exist in the fabric.

Enabling High-Integrity Fabric mode

Setting High-Integrity Fabric (HIF) mode on a switch verifies that the switch meets high-integrity fabric requirements through the channel's Extended Link Services Exchange Query Security Attributes (ELS QSA) function.

Setting HIF mode locks the IDID, fabric-wide consistency policy, and SCC policy settings to ensure that the fabric is of high integrity so that it can connect with the FICON channel. You cannot change these settings without disabling HIF mode.

NOTE

HIF mode must be enabled to enable FMS mode.

To enable HIF mode, use the following steps:

1. Connect to the switch and log in using an account assigned to the admin role.

2. Enter the configure command and step through the interactive prompts.

a. At the "Fabric parameters" prompt, type y.

b. At the "High Integrity Fabric Mode" prompt, type y.

If HIF configuration requirements have not been met, an error message describes what you must configure for the command to succeed. For example, the following message states that an IDID, SCC policy or fabric-wide consistency policy have not been configured for the switch. Perform additional configuration if required, then enable HIF mode.

Error: Unable to set HIF Mode. No valid IDID settings, SCC policy and/or Fabric wide(SCC:S) configuration.