Brocade Fabric OS v7.2.1d
Release Notes v1.0

November 20, 2014

Document History

Document Title	Summary of Changes	Publication Date
Brocade Fabric OS v7.2.1d Release Notes v1.0	Initial Release	November 20, 2014

Contents

Overview

Fabric OS (FOS) v7.2.1d is a patch release based on FOS v7.2.1c. All hardware platforms and features supported in FOS v7.2.1 are also supported in FOS v7.2.1d. This release also contains fixes for many defects.

This release is FICON qualified. Please refer to the *Appendix: Additional Considerations for System z (FICON) Environments* section for feature details and notes on deployment in FICON environments.

Resolution of Important Defects

This release contains fixes for a set of security vulnerabilities associated with OpenSSL and GNU Bash. Software patches are apply to the existing version of OpenSSL and Bash packages. The detail of these patches are:

- Bash vulnerabilities: CVE-2014-6271, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187 (Exposures to CVE-2014-6277 and CVE-2014-6278 are also prevented.)
- OpenSSL vulnerability: CVE-2014-3566

This release contains the following additional important fixes.

- DEFECT000526447 - 7800 switch or FX8-24 blade FCIP DP complex has slow FCIP throughput.
- DEFECT000521218 - Host discovery issues after upgrade to FOS7.2.x in FC Routed configuration over VE/VEX ports.
- DEFECT000527848 - FCIP FICON emulated Tape VM SPOOL DUMP jobs fail after FOS upgrade.
- DEFECT000490979 - FCR proxy devices stuck in initialization on a 7800 switch shipped with FOS7.1 or later firmware.

Additional Hardware Platform Support

Brocade Fabric OS v7.2.1 supports all platforms supported with FOS v7.2.0 plus the following:

- 5432 (embedded switch)
- 6548 (embedded switch)

New Features & Support

In addition to fixes for defects, FOS v7.2.1 also includes:

- Support for FIPS-140 level 2 certification for FOS v7.2.1 release stream
    - Support for NIST SP800-131A compliant cryptographic algorithms and key length
- Support for Clearlink Diagnostic Port (D-port) capability with 8G Long Wave Length (LWL) and Extended Long Wave Length (ELWL) SFPs
    - Support is not available with shortwave 8G SFPs,
    - Supported on Brocade 16G Gen5 platforms only
    - The 8G LWL/ELWL SFPs do not support electrical loopback or optical loopback tests. Support is limited to:
        - Link traffic tests across the 8G LWL/ELWL SFPs and
        - Link distance measurements for links that are longer than 100 meter.
- Support for Forward Error Correction (FEC) counters for admin users through CLI and SNMP
    - Supported on Brocade 16G Gen5 platforms only

Optionally Licensed Software

Fabric OS v7.2 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—Enables performance monitoring of networked storage resources. This license includes the Top Talkers feature.

Brocade Fabric Watch — Monitors mission-critical switch operations. Fabric Watch includes Port Fencing capabilities.

Brocade Fabric Vision – Enables MAPS (Monitoring and Alerting Policy Suite), Flow Vision, and 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 offline 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. (Functionality requires support by attached device, availability TBD).

Fabric Vision license also enables Fabric Watch and Advanced Performance Monitoring functionalities without requiring Brocade Fabric Watch or Brocade Advanced Performance Monitoring license (with FOS v7.2 and later only).

Note:

> If installed on a switch operating with FOS v7.1.x, the Fabric Vision license will be displayed as “Fabric Insight”. If installed on a switch operating with FOS v7.0.x or earlier, the Fabric Vision license will be displayed as “Unknown”. Fabric Vision features are not supported under FOS v7.1.x or earlier.

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—Adaptive Networking provides a rich framework of capability allowing a user to ensure high priority connections obtain the bandwidth necessary for optimum performance, even in congested

environments. The QoS SID/DID Prioritization and Ingress Rate Limiting features are the first components of this license option, and are fully available on all 8Gb and 16Gb platforms.

Note :

With FOS v7.2, the Adaptive Networking license has become part of the base FOS firmware, and features under this license no longer require the license to be installed. Customers that wish to have these capabilities without purchasing the license are required to upgrade to FOS v7.2 or later.

Brocade 6520 does not require the Adaptive Networking with QoS license to enable the capabilities associated with this license. These capabilities are included by default on the Brocade 6520.

Server Application Optimization — When deployed with Brocade Server Adapters, this license optimizes overall application performance for physical servers and virtual machines by extending virtual channels to the server infrastructure. Application specific traffic flows can be configured, prioritized, and optimized throughout the entire data center infrastructure. This license is not supported on the Brocade 8000.

Note :

With FOS v7.2, Server Application Optimization license has become part of the base FOS firmware, and features under this license no longer require the license to be installed. Customers that wish to have these capabilities without purchasing the license are required to upgrade to FOS v7.2 or later.

Brocade 6520 does not require the SAO license to enable the capabilities associated with this license. These capabilities are included by default on the Brocade 6520.

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, or Brocade Encryption Switch to be configured as an Ex_port or VEx_port (on some platforms) supporting Fibre Channel Routing. This eliminates the need to add an FR4-18i blade or use the 7500 for FCR purposes, and also provides double or quadruple the bandwidth for each FCR connection (when connected to another 8Gb or 16Gb-capable port). .

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 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. On the Brocade 6510, Brocade 6520 this license enables 10G FC ports.

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, 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 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.

Note that 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 ten DCX 8510 chassis connected in a core-edge topology. Refer to the Brocade SAN Scalability Guidelines document for additional information.

Temporary License Support

The following licenses are available in FOS v7.2 as Universal Temporary or regular temporary licenses:

- Fabric (E_Port) license
- Extended Fabric license
- Trunking license
- High Performance Extension license
- Advanced Performance Monitoring license
- Fabric Watch license
- 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

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 v7.2.1 supports the following existing platforms:

- 300, 5100, 5300, 7800, VA-40FC, Brocade Encryption Switch, DCX, DCX-4S
- 6505, 6510, 6520, DCX 8510-8, DCX 8510-4
- FC16-32, FC16-48, FC8-32E, FC8-48E, FC8-64, FX8-24, FS8-18 on DCX 8510-8/DCX 8510-4
- FC8-16, FC8-32, FC8-48, FC8-64, FX8-24, FS8-18, FCOE10-24 on DCX/DCX-4S
- 5410, M5424, 5430, 5450, 5480, 5470, 5460, NC-5480
- Support merged to FOS v7.2.1: 5431, 5432, 6547, 6548, M6505

Access Gateway mode is also supported by Fabric OS v7.2, and is supported on the following switches: the Brocade 300, 5100, VA-40FC, 5410, 5450, 5430, 5431, 5432, 5460, 5470, 5480, NC-5480, M5424, 6547, 6548, M6505, 6510, 6505.

The Brocade 8000 is not supported with FOS v7.2.0 and later.

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 conform 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 DCB Capability Exchange Protocol (Proposed under the DCB Task Group of IEEE 802.1 Working Group)
- 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 — 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.

1. 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 units running any FOS v7.1.x or FOS v7.2.0x can be non-disruptively upgraded to FOS v7.2.1d. This upgrade is non-disruptive to both FC and FCoE traffic (when using FCOE10-24 blades).

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.

Note:

To achieve non-disruptive firmware upgrade on 5431, 6547 and M6505 embedded switches to FOS v7.2.1d please follow the instructions given below:

5431:
Upgrade 5431 from FOS v7.0.1_hut to FOS v7.0.1_hut1 before non-disruptively upgrading it to FOS v7.2.1d.

6547:
Upgrade 6547 from FOS v7.0.0_pha3 to FOS v7.0.0_pha4 before non-disruptively upgrading it to FOS v7.2.1d.

M6505:
Upgrade M6505 from FOS v7.0.1_ sh to FOS v7.0.1_sh1 before non-disruptively upgrading it to FOS v7.2.1d.

Disruptive upgrades to Fabric OS v7.2.1d are allowed and supported from FOS v7.0.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 v7.2.1d

Migrating from FOS v7.1

Any 8G or 16G platform running any FOS v7.1. firmware can be non-disruptively upgraded to FOS v7.2.1d.

Migrating from FOS v7.0

Any 8G or 16G platform operating at FOS v7.0.x must be upgraded to FOS v7.1.x before non-disruptively upgrading to FOS v7.2.1d.

Disruptive upgrade to FOS v7.2.1d from FOS v7.0 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 provide 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 12.1.4 is available in

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

For SAN Management, Network Advisor 12.1.4 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 one FOS fabric at a time and up to 1,000 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 thirty-six physical or virtual fabrics and up to 9,000 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 12.1.4 Release Notes, Network Advisor 12.1.4 User Guide, and Network Advisor 12.1.4 Installation, Migration, & Transition Guides.

Note:

Brocade Network Advisor 12.1.4 or later is required to manage switches running FOS 7.2.1 or later.

The Brocade Network Advisor seed switch should always have the highest FOS version used in the fabric.

WebTools Compatibility

FOS v7.2.1d is qualified and supported with Oracle JRE 1.7.0 update 25, update 45, and update 51. Launching WebTools with Oracle JRE 1.7.0 update 51 through Brocade Network Advisor is only supported

on version 12.1.5 or later. With JRE 1.7.0 update 51, users could see some browser warning messages that can be ignored.

SMI Compatibility

- It is important to note that host SMI-S agents cannot be used to manage switches running FOS v7.2.

  If users want to manage a switch running FOS v7.2 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/support/end_of_life.jsp

Supported Products and FOS Interoperability	
4100, 4900, 7500, 7500e, 5000, 200E, 48K Brocade 4012, 4016, 4018, 4020, 4024, 4424	v6.2.2 or later[6]
Brocade 5410, 5480, 5424, 5450, 5460, 5470, NC-5480	v6.2.0 or later[6]
Brocade 6548, 5432	V7.2.1 of later[10]
Brocade DCX, 300, 5100, 5300	v6.1.0e and later [2 6 8]
VA-40FC	v6.2.1_vfc [6], v6.2.2 or later [6]
Brocade DCX-4S	v6.2.0 or later [6 8]
Brocade DCX with FS8-18 blade(s), Brocade Encryption Switch	v6.1.1_enc or later [6]
Brocade 7800, DCX and DCX-4S with FCOE10-24 or FX8-24 blades	V6.3.0 or later
Brocade 8000[9]	V6.1.2_CEE1 or later
Brocade DCX/DCX-4S with FA4-18 blade(s)	DCX requires v6.0.x or later [6], DCX-4S requires 6.2.x or later[5 6]
Brocade DCX 8510-8/DCX 8510-4	FOS v7.0 or later
Brocade 6510	FOS v7.0 or later
Brocade 6505	FOS v7.0.1 or later
Brocade 6520	FOS v7.1 or later
5430	FOS v7.1 or later[10]
5431, 6547, M6505	FOS v7.2 or later[10]
48000 with FA4-18 blade(s), Brocade 7600	V6.2.2 or later [6]
Mi10k, M6140 (McDATA Fabric Mode and Open Fabric Mode) [1]	Not Supported

Multi-Protocol Router Interoperability	
Brocade 7500 and FR4-18i blade	V6.2.2 and higher [4 6 8]
McDATA SANRouters 1620 and 2640	Not Supported

NOS (VDX Platform) Interoperability	
Brocade VDX6710, VDX6720, VDX6730	NOS v2.1.1 or later[7]
Brocade VDX8770	NOS 3.0 or later

Table Notes:

[1] When routing to an M-EOS edge fabric using frame redirection, the M-EOS fabric must have a FOS-based product in order to configure the frame redirection zone information in the edge fabric.

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

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

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

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

[6] 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.

[7] 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, DCX 8510-4.

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

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

[10] Represents the earliest major FOS version. These embedded platforms running respective dedicated FOS versions can also interoperate with FOS v7.2.

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

Starting with FOS v7.2.0, the *Fabric OS MIB Reference* document is not updated. You can obtain the latest MIBs from the downloads area of MyBrocade site after logging in.

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.

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.

Changes in MIBs and objects

This release introduces the following changes in MIBs and objects:

New MIBs

There are no new MIBs introduced in this release.

Updated MIBs

- **SW.mib**
  The **SwConnUnitPortStatEntry** table is updated to include the following objects.

MIB Object	Description
swConnUnitFECCorrectedCounter	Indicates Forward Error Correction (FEC) corrected blocks count.
swConnUnitFECUnCorrectedCounter	Indicates FEC un-corrected blocks count.

- **faext.mib**
  The **SwConnUnitPortEntry** table is updated to include the following objects.

MIB Object	Description
swConnUnitPortFECMode	Represents the port FEC mode.
swConnUnitPortFECState	Represents the FEC state of a port. If both SFPs connected in a link are of Brocade vendor type, the state will be active. Otherwise, it will be inactive.

Blade Support

Fabric OS v7.2 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.
Next Generation Distance Extension Blade (FX8-24)	Up to a max of 4 blades of this type.
FCoE/L2 CEE blade FCOE10-24	Up to a max 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, FC8-32E, FC8-48E	Not supported

Table 1 Blade Support Matrix for DCX and DCX-4S with FOS v7.2

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

Fabric OS v7.2 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.
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, FC8-48E	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.
Next Generation Distance Extension Blade (FX8-24)	Up to a max of 4 blades of this type.
FCoE/L2 CEE blade FCOE10-24	**Not supported on DCX 8510 in FOS v7.x**

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

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

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	
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) 220VAC Power Supplies are required for redundancy. • For DCX with one or two FS8-18 Blades, (2) 220VAC Power Supplies are required for redundancy. • For DCX-4S, (2) 220VAC 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) 220VAC Power Supplies are required for redundancy.

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

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

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, FC8-32E	Port Blade	4 Power Supplies	2 Power Supplies	200-240VAC: 1+1 Power Supplies 110VAC: 2+2[1] Power Supplies
256 16Gb ports + QSFP ICLs	FC16-32, FC16-48 (Maximum of fully populated FC16-32 blades)	Port Blade	4 Power Supplies	2 Power Supplies	200-240VAC: 1+1 Power Supplies 110VAC: 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	200-240VAC: 1+1 Power Supplies 110VAC: 2+2[1] Power Supplies Max 8 FC8-32E port blades
192 16Gb Ports & max 2 intelligent blades (FX8-24 /FS8-18/combination) with QSFP ICLs	FC16-32, FC16-48, FX8-24, FS8-18	Port / Intelligent Blade	4 Power Supplies	2 Power Supplies	200-240VAC: 1+1 Power Supplies 110VAC: 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	200-240VAC: 1+1 Power Supplies 110VAC: 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	200-240VAC: 1+1 Power Supplies 110VAC: 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	200-240VAC: 1+1 Power Supplies 110VAC: 2+2[1] Power Supplies Max 7 FC8-48E 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**
384 16Gb ports + QSFP ICLs	FC16-32, FC16-48	Port Blade	Not Supported	4 Power Supplies	200-240VAC: For DCX 8510-8, four (2+2)[1] 220V AC Power Supplies are required
384 8Gb ports + QSFP ICLs	FC8-32E, FC8-48E	Port Blade	Not Supported	4 Power Supplies	200-240VAC: For DCX 8510-8, four (2+2)[1] 220V AC 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	Not Supported	4 Power Supplies	For DCX 8510-8, four (2+2)[1] 220V AC Power Supplies are required when any special purpose blade are installed

Table 4 Power Supply Requirements for DCX 8510-8

Notes:

1. When 2+2 power supply combination is used, the users are advised to configure the Fabric Watch setting for switch marginal state to be two power supplies. Users can use the CLI switchstatuspolicyset to configure this value if the current value is set to zero. In FOS v7.0.x, the default setting for the marginal state due to missing power supplies is incorrectly set to zero, which will prevent Fabric Watch from generating notifications when the switch enters the marginal state due to missing power supplies

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 Specifications in the 8510-4 Backbone Hardware Reference Manual)					
Configured Number of Ports	Blades	Type of Blade	DCX 8510-4 @110 VAC (Redundant configurations)	DCX 8510-4 @200-240 VAC (Redundant configurations)	Comments
96 ports max with QSFP ICLs	FC16-32, 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, FC8-32E, FC8-48E, FC8-64, FS8-18, FX8-24	Intelligent Blade /Combination	Not Supported	2 Power Supplies	200-240VAC: 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 net installed), 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:
    - Log in to http://my.brocade.com
    - Go to Documentation > Tech Notes.
    - Look for the Tech Note on Access Gateway Device-Based Mapping in VMware ESX Server.

Brocade HBA/Adapter Compatibility

- Brocade HBA/Adapter should be using driver version 2.3.0.2 or later when attached to 16G ports on Brocade switches.

D_Port

- FOS v7.0.0a and later support the execution of D_Port tests concurrently on up to eight ports on the switch.
- Support of D_Port is extended to R_RDY flow control mode. The R_RDY mode is useful for active DWDM links that do not work in VC_RDY or EXT_VC_RDY flow control modes.
- A new sub-option "-dwdm" is added to "portcfgdport --enable" CLI to configure D_Port over **active** DWDM links. The "-dwdm" option will not execute the optical loopback test while performing D_Port tests as the **active** DWDM links do not provide necessary support to run optical loopback tests.

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.
- FOS 7.1.0 or later will use SHA256 signatures for the TLS certificates used to connect to the ESKM 3.0 Server using ESKM 2.0 client. Upgrade from FOS v7.0.x to FOS 7.2 and downgrade from FOS 7.2 to FOS v7.0.x would require regeneration and re-registration of CA and signed KAC certificates to restore connectivity to the key vault. Please refer to the Encryption Admin Guide for more details on ESKM/FOS compatibility matrix.
- 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.
- Before upgrading from FOS v7.0.x to FOS7.2, it is required that the RKM server running SW v2.7.1.1 should be upgraded to DPM server running SW v3.2. Please refer to DPM/FOS compatibility matrix in the Encryption Admin Guide for more details.
- 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 v7.1.x to FOS v7.2 or later 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.
- FOS 7.1.0 introduces support for "disk device decommissioning" to the following key vault types: ESKM, TEKA, TKLM and KMIP. To use disk device decommissioning feature for these key vaults, all the nodes in the encryption group must be running FOS v7.1.0 or later. Firmware downgrade will be prevented from FOS v7.2 to a FOS v7.0.x if this feature is in use. Disk Device decommissioning for DPM and LKM key vaults will continue to work as with previous firmware versions.
- FOS7.2 supports KMIP key vault type for Thales e-Security Key Authority SW v4.0.0 KMIP servers. Please refer to the KMIP Encryption Admin Guide for more details.
    - Replication feature from Thales e-Security Key Authority KMIP server is not supported with BES/FS8-18.
- In FOS 7.1.0 or later the encryption FPGA has been upgraded to include parity protection of lookup memory (ROM) within the AES engine. This change enhances parity error detection capability of the FPGA.
- 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).

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.

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.

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.

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, FC8-32E, FC8-48E, Brocade 6510, Brocade 6505 and Brocade 6520.

- 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.

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.

Native Connectivity (M-EOS interoperability)

- A switch running FOS v7.0 or later cannot form E-port connectivity with any M-EOS platform.
- Platform running FOS v7.1 or later does not support EX port configuration in Interopmode 2 or Interopmode 3.
- Device sharing between a switch running FOS v7.1 or later and McDATA fabrics is allowed via Integrated Routing platforms using FOS v7.0.x (or earlier) firmware.

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.

Port Statistics

- On 16G capable ports, the enc_in (number of encoding errors inside of frames) and enc_out (number of encoding errors outside of frames) counters will not be updated when a port is *operating* at either 10G or 16G speed. This is due to the different encoding scheme used at 10G and 16G speeds when compared to 8G/4G/2G speeds. Because of this, Fabric Watch alerts and Port Fencing based on ITW (Invalid Transmission Word) thresholds will not function as these enc_in and enc_out counters will not be incremented when operating at either 10G or 16G (ITW is computed based on enc_in and enc_out counters). Also any CLI or GUI that displays enc_in and enc_out counters will show no incrementing of these counters when a port is operating at either 10G or 16G.

  Both enc_in and enc_out counters contain valid information when a Condor3-based port is operating at speeds **other than** 10G and 16G.

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.
- FOS v7.1.0 or later supports setting logical switch context using switch name. As a result, configuring the same switch names for the logical switches in a physical chassis is not allowed.

WebTools

- Please note a documentation correction to the "Table 3 Certified and Tested Platforms" of the WebTools Administrator's Guide supporting Fabric OS v7.2.0. Unlike what is stated in the table, WebTools is not supported with the Chrome browser with FOS v7.2.0x and FOS v7.2.1. WebTools is supported with the Chrome browser with FOS v7.2.1a.
- WebTools since FOS v7.1.0 has a "SupportSave" interface. It only collects, however, information specifics 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 upto 5 minutes to complete because the certicate 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.
- Launching WebTools with Oracle JRE 1.7.0 update 51 through Brocade Network Advisor is only supported on version 12.1.5 or later. With JRE 1.7.0 update 51, users could see browser warning messages that the WebTools application requires unrestricted access or the certificate signing the application is not recognized. These messages can be ignored. In addition, users must check the "Enable Java content in the browser" box under the Security tab of Java Control Console to allow launching WebTools from BNA server clients.

Zoning

- Support for up to 2MB zone database in a fabric with only DCX/DCX-4S/DCX8510 systems. The presence of any other platform in the fabric will limit the maximum zone database to 1MB. Please note that there is no enforcement by FOS 7.1 or later to restrict users to operate within a zone database limit - it is the responsibility of the user to not exceed this limit.
- 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.
- Beginning with the FOS v6.2.0 release, all WWNs containing upper-case characters are automatically converted to lower-case when associated with a zone alias and stored as part of a saved configuration on a switch. For example, a WWN entered as either "AA.BB.CC.DD.EE.FF.GG.HH" or "aa.bb.cc.dd.ee.ff.gg.hh" when associated with a zone alias will be stored as "aa.bb.cc.dd.ee.ff.gg.hh" on a switch operating with FOS v6.2.0 or later.

  This behavioral change in saved zone alias WWN members will not impact most environments. However, in a scenario where a switch with a zone alias WWN member with upper case characters (saved on the switch with pre-FOS v6.2.0 code) is merged with a switch with the same alias member WWN in lower case characters, the merge will fail, since the switches do not recognize these zoning configurations as being the same.

  For additional details and workaround solutions, please refer to the latest FOS Admin Guide updates or contact Brocade Customer Support.

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.
- POST diagnostics for the Brocade 5100 have been modified beginning with FOS v6.3.1b and v6.4.0 to eliminate an "INIT NOT DONE" error at the end of an ASIC diagnostic port loopback test. This modification addresses BL-1020 Initialization errors encountered during the POST portloopbacktest. (Defect 263200)
- It is important to note that the outputs of slotshow –p and chassishow 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 rules of default active policy will restore access to the switch.

Defects

Closed with Code Change in Fabric OS v7.2.1d

This sections lists the defects with Critical, High, and Medium Technical Severity closed with a code change as of November 20, 2014, in Fabric OS v7.2.1d.

Defect ID: DEFECT000484537	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** System
Reported In Release: FOS7.1.1	**Technology Area:** Component
Symptom: Switch CP experienced rolling kernel panic at "indirect_read_config" during blade initalization	
Condition: When a not properly seating blade or failed blade hang the PCI bus.	
Recovery: Remove the problem blade.	

Defect ID: DEFECT000487891	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Management
Reported In Release: FOS7.0.0_pha	**Technology Area:** SNMPv2, SNMPv3 & MIBs
Symptom: Customer may encounter an FFDC from raslog KSWD-1002 "Detected termination of process snmpd".	
Condition: SNMPd termination may be encountered most likely in embedded switches that are managed by the FSM application when the application restarts.	
Workaround: Remove the switch from manageable list in application before restarting the application or avoid managing switch via FSM application.	

Defect ID: DEFECT000490979	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.2.1	**Technology Area:** FC-FC routing
Symptom: FCR LSAN devices are stuck in initializing state	
Condition: This may occur with BR7800s shipped with FOS7.1 or later code.	

Defect ID: DEFECT000498907	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Management
Reported In Release: FOS7.0.2	**Technology Area:** Web Tools
Symptom: After resetting switch to factory default with AMM Web interface on BR5470, switch goes through a limited cycle of rolling reboots.	
Condition: This happens when AMM Web interface is used to reset switch back to factory default.	

Defect ID: DEFECT000512347	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Virtualization
Reported In Release: FOS7.1.1	**Technology Area:** Access Gateway
Symptom: Logical port WWN displayed by the "portshow" CLI may change after hot code load or haReboot on a switch running in AG mode, followed by any subsequent offline/online event to the F_Port trunk ports.	
Condition: This may occur under the following conditions: - Upgrade or downgrade to firmware versions v6.1.2d, v6.2.2, or v6.3.0 and above. - Hareboot on firmware versions v6.1.2d, v6.2.2, or v6.3.0 and above. - Then disable / enable all ports of F-port trunk.	
Workaround: Cold boot of the switch in AG mode.	

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: 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: 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: 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: 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: 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. ChassiShow 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: 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: 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: 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: DEFECT000528085	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Other
Reported In Release: FOS7.2.1	**Technology Area:** Other
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: 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. 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: 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: 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 allows 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: 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 their web browsers or Brocade Network Advisor to disable SSLv3 support when accessing Brocade SAN switch. In addition, place your 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: 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: DEFECT000533422	
Technical Severity: High	**Probability:** Medium
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: It 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.	
Recovery: Disable edge switch port and upgrade.	

Closed with Code Change in Fabric OS v7.2.1c

This sections lists the defects with Critical, High, and Medium Technical Severity closed with a code change as of August 29, 2014, in Fabric OS v7.2.1c.

Defect ID: DEFECT000490120	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS6.4.3	**Technology Area:** Fabric Watch
Symptom: Fabric Watch may trigger false alarm message FW-1119 about fabric reconfiguration when no fabric build really happened.	
Condition: This may occur only when a switch CPU is very busy.	

Defect ID: DEFECT000500063	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Other
Reported In Release: FOS7.1.0	**Technology Area:** Other
Symptom: During tape I/O,BES switch or FS8-18 blade might become faulty with the message “BM-BC heartbeat dead. Sending blade fault”.	
Condition: BES Switch or FS8-18 blade might become faulty when the Encryption Engine is in stress due to heavy tape I/O.	
Recovery: Rebooting the switch should recover it.	

Defect ID: DEFECT000505294	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS6.4.3	**Technology Area:** Name Server
Symptom: Switch reboot after name server daemon termination.	
Condition: It only can happen when the customer is configured with broadcast zone.	

Defect ID: DEFECT000511932	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.3.0	**Technology Area:** Zoning
Symptom: Observed " [SCN-1001], 19909, SLOT 4 | FFDC | CHASSIS, CRITICAL, , SCN queue overflow for process nsd." on standby CP.	
Condition: It happens when there are enough zone updates done on the system.	
Recovery: No functional impact. Reboot standby CP to clear it up	

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" via CMM interface (GUI or CLI), leads to external ports changing from AN to fixed at 16Gb, forcing a need to reconfigure the ports to AN.	
Condition: This may be encountered on BR6547 switch after "disable external ports" followed by "enable external ports" using CMM interface.	
Recovery: Reconfigure the external ports to AN.	

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: 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: 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: DEFECT000515486	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Other
Reported In Release: FOS7.1.1	**Technology Area:** Other
Symptom: Director panic due to software watchdog timeout with pdmd daemon. Prior to the panic, switch logged repeat message: "FSS Error: pdm: not acked!"	
Condition: This happened after the standby CP was "REMOVED".	
Recovery: Director recovers by itself after CP reboot.	

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: 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: 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: This is seen 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: 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: DEFECT000521398	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Other
Reported In Release: FOS7.1.1	**Technology Area:** Other
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: DEFECT000525406	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Other
Reported In Release: FOS7.0.0	**Technology Area:** Other
Symptom: When customers configure Edge Hold Time (EHT) in 16G switches running FOS v7.0.0, F-port and E-port do not get expected values.	
Condition: It happens when a user makes EHT change on a 16G switch running FOSv7.0.0. FOS v7.1, v7.2 and v7.3 do not have this problem. But upgrading to these releases does not automatically correct the condition caused by FOS v7.0.0.	
Recovery: Upgrade to a release containing this fix, and re-run 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.	

Closed with Code Change in Fabric OS v7.2.1b

This sections lists the defects with Critical, High, and Medium Technical Severity closed with a code change as of July 15, 2014, in Fabric OS v7.2.1b.

Defect ID: DEFECT000401075	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Security
Reported In Release: FOS7.0.1	**Technology Area:** Fabric Authentication
Symptom: Weblinker crashes and cannot be restarted	
Condition: When one of the radius server is not responding for reasons such as port 1813 is blocked by network firewall, then next available server to authenticate the radius user triggers a NULL pointer access.	
Workaround: Unblocking the accounting port (default port 1813) is the workaround in case of accounting fails due to firewall.	

Defect ID: DEFECT000432406	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS6.4.2	**Technology Area:** Logging
Symptom: Customer observes multiple supportsave processes on switch without actively initiating a recent supportsave. These processes consume memory and may lead to switch panic when an additional supportsave is initiated.	
Condition: Hung supportsave processes left on switch.	
Workaround: Kill stale supportsave PIDs	
Recovery: After switch panic, no further recovery is needed.	

Defect ID: DEFECT000445731	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.0.2	**Technology Area:** BB Credits
Symptom: IO traffic could not be restarted after FCIP Tunnel recovered from keep-alive Timeout.	
Condition: Enhanced code to perform Link Reset to recover lost credit for FX8-24 blade. This could happen when there was link level error such as loss of sync.	
Recovery: Reset FX8-24 or connected core blade reporting the problem.	

Defect ID: DEFECT000455322	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.0.2	**Technology Area:** Fabric Watch
Symptom: An unexpectedly large number of threshold crossing "above high boundary" Fabric Watch messages may be seen.	
Condition: This may be seen during portdisable or portenable.	

Defect ID: DEFECT000467843	
Technical Severity: Medium	
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.0.2	**Technology Area:** End-to-end Performance Monitoring
Symptom: The TX counter remains at "0x0000000100000000" after clears stats of EE performance monitors.	
Condition: No special condition is required: When EE monitor counters(TX/RX) are cleared on a port, 1 in top value of EE monitor counters(Tx/Rx) are not cleared. There is no functional impact.	

Defect ID: DEFECT000471135	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.2.0	**Technology Area:** Trunking
Symptom: RTWR-1003 RASLOG messages: Loss of connectivity.	
Condition: This is a rare occurrence that may be encountered when both E-ports of a 2-E-port trunk go offline during hafailover/hareboot.	
Recovery: Disable both ports in the 2-E-port trunk, then enable them again.	

Defect ID: DEFECT000471772	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Other
Reported In Release: FOS7.2.0	**Technology Area:** Other
Symptom: After issuing cfgsave, there may be a time delay before cfgsave confirmation message is displayed. During the time delay, CPU load may be high on zoning.	
Condition: The issue may occur if the zone database is large.	
Recovery: The operation completes by itself without intervention.	

Defect ID: DEFECT000472904	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.1.0	**Technology Area:** FC-FC routing
Symptom: 16G ASIC signal equalizer (DFE) running at 8G may drift due to IDLE fill words received resulting in CRC errors and server tapes not accessible after reboot	
Condition: This may be encountered when 16G ASIC speed negotiates or is locked at 8G	

Defect ID: DEFECT000473289	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.2.0	**Technology Area:** Routing
Symptom: RTWR-1003 RAS logs.	
Condition: This problem may occur from the following sequence: 1. One switch is connected off a loop topology 2. The loop topology is physically changed to a linear topology 3. One of the switches that was in the loop undergoes an hareboot	
Recovery: Bounce an ISL connecting the switch originally outside the loop topology.	

Defect ID: DEFECT000473848	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.1.1	**Technology Area:** SNMPv2, SNMPv3 & MIBs
Symptom: authPrivSecret default keys are not being set by the CLI command snmpconfig --default snmpv1	
Condition: This will be encountered when attempting to set the default setting using the CLI command snmpconfig --default snmpv1	
Workaround: set the default values manually using snmpconfig --set snmpv1	

Defect ID: DEFECT000475084	
Technical Severity: High	
Product: FOS	**Technology:** Management
Reported In Release: FOS7.1.1	**Technology Area:** CLI
Symptom: spinfab fails with various symptoms, such as: - Test port goes into G_Port state, - Hard-Flt status, or - CRC error reported.	
Condition: This happens with LS E port with nframe=0 option.	

Defect ID: DEFECT000475645	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.0.2	**Technology Area:** End-to-end Performance Monitoring
Symptom: Updated End-to-End monitor shows previous data.	
Condition: After removing and replacing an EE monitor (with the SID and DID reversed) the data from the original EE monitor is shown instead of zeros.	

Defect ID: DEFECT000477706	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.0.2	**Technology Area:** Fabric Watch
Symptom: Following an hafailover DNS configuration may be lost, resulting in Fabric Watch email failure.	
Condition: This may be encountered when DNS settings are changed using dnsconfig, followed by an hafailover	
Workaround: configure the relay host IP address manually to work around the issue	

Defect ID: DEFECT000477948	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.1.0	**Technology Area:** Platform Services
Symptom: Toggling autoneg on a disabled ge port followed by reenabling it, may sometimes result in other ge ports going to 'no sync' state.	
Condition: This may occur upon executing the following sequence of commands : 1. portdisable <ge port> 2. portcfg autoneg <ge port> --disable 3. portcfg autoneg <ge port> --enable 4. portenable <ge port> Then note that a different ge port may go to 'No_Sync' status -	
Workaround: Use only portdisable/portenable.	

Defect ID: DEFECT000482106	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** FICON
Reported In Release: FOS7.1.0	**Technology Area:** FICON CUP
Symptom: Fbusy encountered when trying to bring up CUP connections following FCIP tunnel bounces.	
Condition: This may be seen only on FICON switches when attempting to bring up CUP connection after an FCIP tunnel is bounced.	

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: DEFECT000483878	
Technical Severity: Medium	
Product: FOS	**Technology:** Management
Reported In Release: FOS7.0.2	**Technology Area:** Ethernet Interface
Symptom: In rare cases switch may panic with Exception in kernel mode with sig: 5 during bootup.	
Condition: This occurs only when TX reset on Ethernet interface during Ethernet port initialization that had a lots of RX parity errors.	

Defect ID: DEFECT000484414	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Virtualization
Reported In Release: FOS7.0.2	**Technology Area:** Access Gateway
Symptom: Under rare conditions, Access Gateway(AG) entries stay in management server (MS) database even after removing them from the fabric. FOS firmware is expected to remove these stale entries during execution of agshow CLI command. However, due to a timing issue the stale entries may not be removed from the database when agshow CLI command is run.	
Condition: This may be observed on a switch running firmware version higher than v7.0.	

Defect ID: DEFECT000484425	
Technical Severity: Medium	
Product: FOS	**Technology:** Management
Reported In Release: FOS7.0.1	**Technology Area:** Brocade Network Advisor
Symptom: The CLI error log on the switch may report that HTTP server and weblinker processes cannot be started (WEBD-1008). Consequently BNA will not be able to manage the switch. Memory utilization of kacd process may report in excess of 57% of available memory.	
Condition: This may be encountered only on the Brocade Encryption Switch.	
Workaround: 1. Disable kvdiag 2. Configure BNA as large SAN	

Defect ID: DEFECT000485968	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Security
Reported In Release: FOS7.1.1	**Technology Area:** Fabric Authentication
Symptom: Unable to authenticate with TACACS server when setting up new Brocade switches.	
Condition: The issue will be hit if the TACACS+ Server Software converts the attribute to lower case and sends it to the switch. So far, this behavior has been encountered with TACACS+ server software (tacacs.net - version 1.2.2.0).	

Defect ID: DEFECT000486638	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** FICON
Reported In Release: FOS7.1.0	**Technology Area:** FICON CUP
Symptom: The following issue is observed often and leads to disruptive Ficon operations: "KSWD-1002 termination of process ficud".	
Condition: This may occur when there are more than 8 trunk groups in a fabric configuration.	

Defect ID: DEFECT000489686	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.1.0	**Technology Area:** FCIP
Symptom: Disk to disk backups from site to site are failing. Multiple internal ports on FX8-24 appear to have persistent -3 credit on data VC.	
Condition: A rare FPGA issue, that loops back a buffer before filling it with new FC data frames, may cause VC credit depletion.	
Recovery: Power-off/on the slot with this problem.	

Defect ID: DEFECT000490533	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.1.0	**Technology Area:** Extended Fabrics
Symptom: FDR (Fast Dump Restore) disk copy MVS jobs fail with zHPF mode enabled.	
Condition: This may occur when zHPF mode is enabled and I/Os include a large number of frames in a FC sequence	
Workaround: Disable zHPF mode on the connected mainframes.	
Recovery: No recovery exists besides restarting the job with zHPF mode disabled	

Defect ID: DEFECT000490564	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Security
Reported In Release: FOS6.4.0	**Technology Area:** Encryption
Symptom: User may experience failures on BES encryption switch in diagnostic tests such as POST Turboramtest.	
Condition: This may happen during stress testing with repeated power resets on BES.	

Defect ID: DEFECT000490754	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.0.2	**Technology Area:** BB Credits
Symptom: Switch ports connected to storage controller become unresponsive.	
Condition: This rare condition may occur with Fabric Loop (FL) port after many resets. The port may get into "Port failed due to busy buffer stuck error" state.	
Recovery: Reboot switch to recover; portdisable/port enable does not recover.	

Defect ID: DEFECT000491049	
Technical Severity: Medium	
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.2.0	**Technology Area:** Extended Fabrics
Symptom: When WAN-side-failover-cable-pulls are performed with ISL-Inflight-Encryption “on”, OLS counters are incremented.	
Condition: When ISL-Inflight-Encryption is turned "on" and the WAN cable is pulled, there is a possibility of frames getting dropped, which may result in credits not being returned, leading to a Link Reset.	

Defect ID: DEFECT000491841	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.1.0	**Technology Area:** Lossless DLS
Symptom: When F-port trunking is enabled, portdecom on the E-port may fail with "invalid remote port type"	
Condition: This portdecom failure on the E-port may be encountered when F-port trunking is enabled.	
Workaround: Disable F-port trunking, then portdecom will work.	

Defect ID: DEFECT000492224	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Other
Reported In Release: FOS7.1.0	**Technology Area:** Other
Symptom: Data path lost after recovery of faulty slots or hafailover: Zone type is not set for some devices.	
Condition: This is a rare race condition that may cause inconsistency between zoning software and ASIC hardware state during zone CAM programming.	
Recovery: Ports must be bounced to recovery from the inconsistent port software/hardware zone type state, .	

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: DEFECT000492732	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Management
Reported In Release: FOS6.4.3	**Technology Area:** Platform Services
Symptom: After auto tuning FC8-64 in DCX-4s, the blade may be faulted.	
Condition: When auto-tuning is run on FC8-64 blade in a DCX-4s, some values attempted can cause this blade or peer core blade to fault. .	
Workaround: Use manual tune	

Defect ID: DEFECT000492854	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.1.0	**Technology Area:** FC-FC routing
Symptom: Following a planned device outage, many ports are displayed as "FC Disabled (Port Throttled)". Ports do not come online for a long time.	
Condition: This may occur when a large number of devices with laser on but cannot complete link initialization with a switch. It typically occurs during device power cycle, upgrade, or running diagnostics.	
Workaround: Stage the number of devices coming online at the same time.	
Recovery: Disable the devices that cannot come online to give other ports a chance.	

Defect ID: DEFECT000492856	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.1.0	**Technology Area:** CLI
Symptom: Switch ran out of shared memory.	
Condition: Application using "shmget" fails and reports no space left on device and number of shared memory segment became zero. This happen when there is IPC timeout between daemons using IPC for communication.	

Defect ID: DEFECT000493752	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** FICON
Reported In Release: FOS7.1.0	**Technology Area:** FICON CUP
Symptom: When there is a Remote CUP, with traffic flowing across 7800 IP links, CUP can become unresponsive.	
Condition: When FICON CUP receives an ELP (Est Logical Path) and that Logical Path already exists, treat the LP as a System Reset for that Logical Path.	

Defect ID: DEFECT000495636	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.1.0	**Technology Area:** Buffer Credit Recovery
Symptom: Switch panic during CP blade replacement.	
Condition: On a very congested switch with lots of BE link resets, the event of bringing down a CP blade may cause a panic condition during the blade shutdown procedure.	

Defect ID: DEFECT000496527	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.2.0	**Technology Area:** FCIP
Symptom: Unable to run traffic on low bandwidth FCIP tunnel. Customer sees application suspends.	
Condition: This may be encountered on low bandwidth FCIP tunnels	
Workaround: If possible, increase the FCIP Circuit minimum data rate.	

Defect ID: DEFECT000499895	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.2.0	**Technology Area:** FCIP
Symptom: Uncompressed throughput on the 10GE FCIP complex drops to about 52M/Sec and never recovers.	
Condition: If some TCP connections had byte flow control indicated and others had PDU flow indicated, this could lead to a TX stall in FCIP Tunnel processing.	
Workaround: Start and stop FCIP Tunnel traffic.	

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: DEFECT000500250	
Technical Severity: Medium	
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.2.0	**Technology Area:** Fabric Watch
Symptom: FWtrap is not generated for "Power on hours" area for 16G LWL SFP when thresholds cross boundaries.	
Condition: This impacts 16GLWL trap only	

Defect ID: DEFECT000500355	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Management
Reported In Release: FOS7.0.1	**Technology Area:** Web Tools
Symptom: Unable to logon to switch using HTTP Webtools and/or BNA.	
Condition: It happens when HTTP fails to open SQLITE Database during security violation.	

Defect ID: DEFECT000500532	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Other
Reported In Release: FOS7.2.0	**Technology Area:** Other
Symptom: On BR6547, Firmware status is shown incorrectly in firmwareImageinfo object.	
Condition: FirmwareStatus is shown as "inACtive", even though firmware is active.	

Defect ID: DEFECT000500759	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Other
Reported In Release: FOS7.2.1	**Technology Area:** Other
Symptom: CRC with Good EOF errors observed on FC8-64 in BR8150.	
Condition: Port blade FC8-64 is installed in BR8150 slot 2	
Workaround: Manually tune S2/P34 to 0x195DA1DD	
Recovery: Manually tune serdes value for S2/P34 to 0x195DA1DD	

Defect ID: DEFECT000501917	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Security
Reported In Release: FOS7.2.1	**Technology Area:** Encryption
Symptom: In encryption environment with BES/FS8-18, switch or blade became faulty during initial discovery of target.	
Condition: It may happen after EE became online and during initial discovery of targets, if the target returns error for slow path commands(REPORT_LUN/INQUIRY). .	

Defect ID: DEFECT000501919	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** Diagnostic Port (D_Port)
Symptom: D-Port test PASSED with errors on D-Port Responder side.	
Condition: After electrical or optical loopback test, stats are not cleared in responder.	

Defect ID: DEFECT000502591	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.2.0	**Technology Area:** Routing
Symptom: On a switch that had pre-FOS v7.1 installed before, upgrade the switch to FOS v7.1 or later, host lost access to storage with missing route.	
Condition: If there is a port bounces during hareboot/hafailover (or as part of firmwaredownload), switches could see this problem.	
Workaround: Upgrade to a release containing defect 459831 fix (FOS v7.1.1a, v7.1.2, v7.2.0). If a later release is needed, then upgrade must be done to a release with the fix to this defect in it.	
Recovery: Port bounce alone may not fully recover. Need a slotpoweroff/on on impacted port blade or cold boot on a switch.	

Defect ID: DEFECT000503299	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Other
Reported In Release: FOS6.4.3	**Technology Area:** Other
Symptom: After FOS upgrade, CLI "swithchsow" reports multiple ports in disabled state with reason as "Not ready for F or L ports", "Switch not ready for EX_Ports"	
Condition: Occasionally, switch finds inconsistency in domain count and E-port count during HAfailover/hareboot when there is VEX-EX ports in the configuration.	
Recovery: Trigger fabric rebuild by executing "fabricprincipal -f". Manual fabric rebuild by taken offline ALL E_port/Trunks, then re-enable them or switch disable/enable.	

Defect ID: DEFECT000508529	
Technical Severity: Critical	**Probability:** Medium
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.0.0	**Technology Area:** Trunking
Symptom: High deskew values on 16G trunk ports are contributing to high fabric latency.	
Condition: It occurs during trunk forming with 16G ports. Sometimes the impact is not observed until after a hafailover/hareboot. trunkshow shows huge deskew value difference between links in a single trunk. Example of an actual trunkshow output of a high latency fabric: trunkshow : 1: 0-> 0 xxx deskew 1517 MASTER 1-> 1 xxx deskew 15	
Recovery: port disable and enable links in the trunk one by one: portdisable link1, portenabel link1; portdisable link2; portenable link2	

Defect ID: DEFECT000513920	
Technical Severity: High	
Product: FOS	**Technology:** Security
Reported In Release: FOS7.1.0	**Technology Area:** Fabric Authentication
Symptom: CVE-2014-0224: OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the "CCS Injection" vulnerability.	
Condition: FOS switches that are not running LDAP or RADIUS with PEAP-MSCHAPv2 for authentication are not running OpenSSL client mode and are not at risk. To be at risk: • The FOS product must be running authentication using LDAP or RADIUS with PEAP-MSCHAPv2 protocols. • The OpenSSL server must also be running with a version of OpenSSL that contains this vulnerability (1.0.1 or 1.0.2-beta1)	
Workaround: For users requiring LDAP or RADIUS with PEAP-MSCHAPv2 for authentication, upgrading the OpenSSL server to a version of OpenSSL that does not contain this vulnerability will prevent exposure.	

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.	

Closed with Code Change in Fabric OS v7.2.1a

This sections lists the defects with Critical, High, and Medium Technical Severity closed with a code change as of March 7th, 2014, in Fabric OS v7.2.1a.

Defect ID: DEFECT000461189	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.2.0	**Technology Area:** Web Tools
Closed In Release(s): FOS7.2.1a(Fixed)	
Symptom: Unable to launch web tools using Google chrome browser and IE11 with Java update 45 or 51	
Condition: This happens when using the latest Java update revision 45 or 51.	
Workaround: Use another browser or older java update.	

Defect ID: DEFECT000466071	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.2.0	**Technology Area:** Logging
Closed In Release(s): FOS7.2.1a(Fixed)	
Symptom: Observed verify error from name server daemon on an idle switch: "VERIFY - Failed expression: 0, file = ns.c, line = 5834...". Too many verifies can trigger a switch panic.	
Condition: When device sent PLOGI with invalid SID/DID, such as SID of 0.	
Workaround: Disable the port connecting to the device sending invalid SID.	

Defect ID: DEFECT000474833	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.0.0	**Technology Area:** FCIP Fastwrite
Closed In Release(s): FOS7.2.1a(Fixed)	
Symptom: Job failures after check condition from tape device (the next I/O is incorrectly responded to with a deferred error check condition status).	
Condition: If a tape device is accessed via a non-OSTP (Open Systems Tape Pipelining) tunnel and it returns a check condition to an I/O, FCIP FW processing would incorrectly generate a second check condition status to the next I/O for that tape device.	
Workaround: Enable OSTP on the FCIP FW enabled tunnels if there are also Tape devices accessed via the tunnel.	

Defect ID: DEFECT000475036	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.2.0	**Technology Area:** CLI
Closed In Release(s): FOS7.2.1a(Fixed)	
Symptom: CLI command "apploginhistory --show" indicates webtools connection after webtools is closed	
Condition: Close webtools and run CLI command "apploginhistory --show"	
Workaround: Use the normal exit to exit to close webtools session. i.e. On Webtools select Manage --> Exit Do not click "X" to close webtools session.	

Defect ID: DEFECT000475264	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Security
Reported In Release: FOS7.1.1	**Technology Area:** Fabric Authentication
Closed In Release(s): FOS7.2.1a(Fixed)	
Symptom: After password expiration in switches with multiple logical switches, excessive login failures may trigger repeated secd panics.	
Condition: This happens when password expires in a setup with large number of logical switches or customer triggers multiple security violations with very high frequency via scan tools	
Workaround: Disconnect the management Ethernet cable.	
Recovery: Stop security scanning tool and fix any security violation until upgrade to a code release with fix.	

Defect ID: DEFECT000477009	
Technical Severity: Critical	**Probability:** Low
Product: FOS	**Technology:** Virtualization
Reported In Release: FOS7.0.0_pha	**Technology Area:** Access Gateway
Closed In Release(s): FOS7.2.1a(Fixed)	
Symptom: A host connected to a NPIV port on an Access Gateway has multiple virtual clients. Only the physical HBA is able to login. The virtual client logins are rejected.	
Condition: The issue occurs under the following conditions: 1. F-ports have never bounced since upgrading to a FOS version with the Persistent ALPA feature. 2. The Persistent ALPA feature is enabled for the first time. 3. Virtual clients login without first bouncing the Access Gateway port where the host is connected.	
Workaround: Disable all F-ports on the Access Gateway before trying to login virtual clients.	
Recovery: Disable _all_ the affected F-ports, then enable all the affected ports. To determine which ports are affected, run this command on all F-ports: ag --printalpamap <F-port_number> If the CLI comes back with _Hash Table is empty_, then the port is affected.	

Defect ID: DEFECT000477834	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.1.0	**Technology Area:** OSTP - Open Systems Tape Pipelining
Closed In Release(s): FOS7.2.1a(Fixed)	
Symptom: In an FCIP tunnel using OSTP, tape server reports intermittent missing block errors.	
Condition: During error recovery for FC CRC errors, OSTP may incorrectly send frames out of order.	

Defect ID: DEFECT000479882	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** FICON
Reported In Release: FOS7.1.0	**Technology Area:** FICON emulation
Closed In Release(s): FOS7.2.1a(Fixed)	
Symptom: Host reported IFCCs due to aborted FICON RRS/Device Level Exception/LACK Sequence	
Condition: If a FICON Disk controller returns a device level exception frame to a read record set CCW command chain, the IFCCs will occur.	
Workaround: Disable XRC Emulation on the FCIP Tunnel	
Recovery: The mainframe will automatically recover from this error.	

Defect ID: DEFECT000484327	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.1.0	**Technology Area:** FC-FC routing
Closed In Release(s): FOS7.2.1a(Fixed)	
Symptom: Switch panic after name server detected duplicated WWPN with raslog: 2013/10/22-02:26:59, [NS-1012], 147485, SLOT 6 | FID 128, WARNING, , Detected duplicate WWPN [] - devices removed with PID 0x3ce701 and 0x3ce80	
Condition: This may occur when 1. There is physically duplicated WWPN in the environment, or 2. An interleaved offline and online sequence between two different NPIV ports may trigger a false duplicate WWPN detection.	
Workaround: Remove physically duplicate WWPN devices if any exist.	
Recovery: If there is no physically duplicate WWPN devices, switch recovers itself after panic.	

Defect ID: DEFECT000487235	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Virtualization
Reported In Release: FOS7.1.1	**Technology Area:** Access Gateway
Closed In Release(s): FOS7.2.1a(Fixed)	
Symptom: Hosts are not able to login to the Access Gateway after the Access Gateway is rebooted.	
Condition: The problem occurs under these conditions: - No Access Gateway policies are enabled -- i.e. neither Port Group policy nor Auto Policy - Access Gateway is rebooted - One or more N-ports do not come online after reboot	
Workaround: Insure all N-ports come online after an Access Gateway reboot.	
Recovery: Either bring all required N-ports online or re-map the currently offline F-ports to the online N-port(s).	

Defect ID: DEFECT000487250	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.1.1	**Technology Area:** Platform Services
Closed In Release(s): FOS7.2.1a(Fixed)	
Symptom: Host cannot connect to storage and CLI nsshow for a FC4 type device is missing FC4 type: "FC4s:fcp"	
Condition: A timing condition is observed when a device sends 2 consecutive FLOGIs without an explicit logout in between.	
Recovery: Reboot device or issue portdisable and portenable on the switch port	

Defect ID: DEFECT000487271	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Management
Reported In Release: FOS7.2.1	**Technology Area:** Brocade Network Advisor
Closed In Release(s): FOS7.2.1a(Fixed)	
Symptom: Unable to create flow with Flow Mirror feature through BNA with FOS v7.2.0x	
Condition: This happens in a race condition when the non-default switch goes to active prior to the default switch in an VF environment after a cold boot or hafailover.	
Workaround: The FOS CLI can be used to successfully create the flow.	
Recovery: User can attempt to restart the flow. If it still fails and user has to use BNA to create flow, upgrade to a FOS code revision with the fix.	

Defect ID: DEFECT000488202	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.1.0	**Technology Area:** IPsec
Closed In Release(s): FOS7.2.1a(Fixed)	
Symptom: FCIP Circuit bounces due to replay checks when running IPSec with unidirectional traffic from the lower order IP address to the higher IP address on the circuit.	
Condition: This issue may occur only when traffic is always flowing from the lower order IP address to the higher order IP address on an FCIP circuit.	
Workaround: Run traffic from the higher order IP address to the lower order IP address on the FCIP circuit.	

Defect ID: DEFECT000488790	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.1.0	**Technology Area:** Routing
Closed In Release(s): FOS7.2.1a(Fixed)	
Symptom: If a customer has more than 8 paths (E-ports and/or E-port trunks) between two switches or if the paths are of unequal bandwidth, then those paths may not have ports evenly distributed across them, as seen in topologyshow.	
Condition: This occurs under the following conditions: - When there are more than 8 E-ports/Eport Trunks between two switches. - When the E-ports/E-port Trunks between two switches are not the same bandwidth.	
Workaround: Remove the conditions causing the problem: 1. Make all E-ports/E-port trunks be the same bandwidth. 2. If after doing 1) there are still more than 8 paths, then equally increase the bandwidth on the other E-ports/E-port Trunks by reducing the number of them. Again, the bandwidth must be equal.	
Recovery: Same as the Workaround.	

Defect ID: DEFECT000489552	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Security
Reported In Release: FOS7.2.1	**Technology Area:** Encryption
Closed In Release(s): FOS7.2.1a(Fixed)	
Symptom: I/O to encrypted tape LUNs halted unexpectedly.	
Condition: When multiple tape handles got queued up which eventually prevented the processing of new commands from hosts.	
Recovery: Deleting and re-creating the CTC's	

Defect ID: DEFECT000490548	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.1.1	**Technology Area:** BB Credits
Closed In Release(s): FOS7.2.1a(Fixed)	
Symptom: Detect CRC error with good EOF on C-port(0) and on C-port(8); This could trigger buffer credit loss on these ports.	
Condition: It happens with Slot 2 port 0 and port 8 of a DCX4s with FC8-48 port cards installed in slot 2.	
Recovery: Manually tune both the port card port and the core blade ports with different values.	

Defect ID: DEFECT000491192	
Technical Severity: Critical	**Probability:** Medium
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.2.0	**Technology Area:** Routing
Closed In Release(s): FOS7.2.1a(Fixed)	
Symptom: FOSv7.2.0, 7.2.0a, 7.2.0b, 7.2.0c, 7.2.1 with user defined logical switch, hosts may be unable to reach targets due to frames being corrupted or traffic flow may appear to stop.	
Condition: This happens with customer configuration parameter "Custom.index" of 1,2,3,5, when user creates a logical switch and then moves ports with non-default configuration to it. This can happen for both FOSv7.1.x to FOSv7.2.x upgrade and with freshly installed FOSv7.2.x switches. This does not happen with "Custom.index" of 0 or 4	
Workaround: Do not create or modify logical switch until upgrade to a code revision with fix.	
Recovery: Upgrade to a FOS release with the fix (v7.2.0d) will recover and also prevent future occurrence. Downgrading from FOS 7.2.1 to a release with the fix (v7.2.0d) will not correct the problem and v7.2.0d must be downloaded a second time after initial downgrade to v7.2.0d. Upgrade FOS7.2.1 to a future 7.2.1a will address the problem. If a code upgrade is not possible, please use CLI "portcfgdefault" on each port and then cold boot switch to recover.	

Defect ID: DEFECT000492340	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.3.0	**Technology Area:** BB Credits
Closed In Release(s): FOS7.2.1a(Fixed)	
Symptom: May notice frame drops on the back end edge and core ports with FS8-18 and FX8-24.	
Condition: When FS8-18 and FX8-24 blades are used with 16G core blade chassis .	
Recovery: Upgrade code with fix and perform a power cycle of port blade to have the new credit buffer allocation scheme to take effect.	

Defect ID: DEFECT000492849	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.2.1	**Technology Area:** FCIP
Closed In Release(s): FOS7.2.1a(Fixed)	
Symptom: FCIP link became unstable after some run time and reported the following XTUN messages: 2014/02/03-09:50:40, [XTUN-1008], 12759, CHASSIS, WARNING, , FCIP Control block memory usage slot=0 DP=1 Allocated=5209344 Free=196117248 Total=201326592. 2014/02/03-09:50:41, [XTUN-1001], 12760, FID 128, ERROR, , FCIP Tunnel 16 Memory allocation failed tracker 1/247.	
Condition: On switch running with FOS 7.2.0b/c and FOS7.2.1, resource is lost when processing periodic vendor unique message ELS-PRLI coming from a disk mirroring application every 5 seconds.	

Defect ID: DEFECT000494570	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Management
Reported In Release: FOS7.2.0	**Technology Area:** Firmware upload/download
Closed In Release(s): FOS7.2.1a(Fixed)	
Symptom: Upgrading to FOS7.2.0c (which contains a fix for defect 491192) with pre-existing user-defined logical switches may lead to fabric wide performance issue or hosts not being able to see targets after a slot offline event .	
Condition: On FOS 7.2.0c, this affects Fabric IDs that do NOT contain a digit of 0, 1, 2, or 5; such as FID 3 or FID 4. FID 35 would not be affected as it contains the digit 5.	
Workaround: Do not create or modify logical switches, or bounce ports until upgrading to a code revision with fix.	
Recovery: Upgrade to a FOS release with the fix (v7.2.0d) will recover and also prevent future occurrence. Downgrading from FOS 7.2.1 to a release with the fix (v7.2.0d) will not correct the problem and v7.2.0d must be downloaded a second time after initial downgrade to v7.2.0d. Upgrade FOS7.2.1 to a future 7.2.1a will address the problem. If a code upgrade is not possible, please use CLI "portcfgdefault" on each port and then cold boot switch to recover.	

Closed with Code Change in Fabric OS v7.2.1

This sections lists the defects with Critical, High, and Medium Technical Severity closed with a code change as of December 13, 2013 in Fabric OS v7.2.1. Note: these defects are formatted with an updated defect table structure applying to all new or previously unpublished defects.

Defect ID: DEFECT000415126	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Management
Reported In Release: FOS7.1.0	**Technology Area:** CLI
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: User may see "Maximum number of rules created" when editing inactive policies (adding or removing rules from policies)	
Condition: It happens when the maximum number of ipfilter policies are present	
Workaround: Reduce the number of ipfilter policies.	

Defect ID: DEFECT000427692	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS6.4.2	**Technology Area:** Fabric Watch
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: False alarm reported about FAN with FW-1006 raslog in heavy CPU utilization switches : 2012/10/28-18:45:42, [FW-1006], 67128, SLOT 6 | FID 128, WARNING, , Env Fan 2, is below low boundary(High=3400, Low=1600). Current value is 0 RPM.	
Condition: Under heavy CPU utilization switch reported false alarm about the fan with FW-1006 raslog.	
Workaround: Issue will not be seen if switch CPU utilization is less.	

Defect ID: DEFECT000442978	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Management
Reported In Release: FOS7.1.0_blv	**Technology Area:** Platform Services
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: Embedded switch BR6458's internal copper port may be stuck at No_Sync after its peer server blade is reseated.	
Condition: A reseat of the server blade is required.	
Workaround: A gentle reseat of the server blade did not recreate the issue.	
Recovery: A gentle reseat of the server blade.	

Defect ID: DEFECT000454580	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Security
Reported In Release: FOS6.4.2	**Technology Area:** Fabric Authentication
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: With SSL configured on Active CP, a newly inserted Standby CP may panic and go through an unnecessary additional reboot.	
Condition: When SSL configured in the active CP, inserting a new standby CP whose time is later than that of Active CP & don't have SSL configured already can cause a panic & unnecessary additional reboot of standby CP after insertion.	
Workaround: Insert standby CP with hadisabled state. Login to standby CP, change standby CP's date to earlier than that of the active CP using "/bin/date" command and then execute haEnable.	
Recovery: No action required. Previous switch reboot will fix the SSL configuration issue.	

Defect ID: DEFECT000455170	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.1.0	**Technology Area:** CLI
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: On a switch without license, while changing the date using "date" command will display: "No licenses installed." Even though date properly updated by the command.	
Condition: Executing "date" command in a switch without license will throw message "No licenses installed".	
Workaround: Issue is cosmetic. unnecessary message can be ignored.	
Recovery: No recovery applicable. issue is cosmetic.	

Defect ID: DEFECT000458552	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.0.1	**Technology Area:** Port Log
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: Log entry in the portlogdump doesn't align properly with the rest of the columns.	
Condition: Zone entry not aligned properly between port , cmd and argument/payload value.	

Defect ID: DEFECT000460977	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Management
Reported In Release: FOS7.2.0	**Technology Area:** CLI
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: User can't execute switchcfgtrunk CLI in AG mode. It gives following error while executing the CLI: Error: This command is not supported in AG mode	
Condition: switchcfgtrunkport CLI is blocked in AG mode through RBAC permission check.	
Workaround: Trunking can be disabled or enabled on the ports in AG using portcfgtrunkport CLI.	
Recovery: Ports will be recovered from this state using portcfgtrunkport CLI.	

Defect ID: DEFECT000461699	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Security
Reported In Release: FOS7.1.0	**Technology Area:** Encryption
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: CVLC might crash during host login to VT or crypto configuration change.	
Condition: Issue will only be seen on Brocade Encryption Switch or FS8-18 blade. Only with higher ITL count configuration, when crypto config change is done through "cryptocfg –commit" command, CVLC might crash due to a race condition between host login and internal command timeout.	

Defect ID: DEFECT000462116	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.0.0	**Technology Area:** Platform Services
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: Director rebooted: CPs lost heartbeat and active CP was reset, standby CP panicked during take over.	
Condition: Port blade hardware failure may trigger loss of heartbeat (between two CPs)	
Recovery: Switch is recovered after reboot; replace bad port blade to prevent re-occurrence.	

Defect ID: DEFECT000463819	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.0.2	**Technology Area:** FC-FC routing
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: Class 2 GPN_FT queries may fail with excessive targets (127 targets) in the fabric.	
Condition: Occurs if any class 2 query response spans more than one FC frame and the end to end credit is unable to accommodate the response	
Workaround: Reduce the number of devices zoned together so that the number of FC frames responded by the switch for a name server query does not exceed the credit configured at the device. Else, increase the end-to-end credit configured at the device side to prevent failure in name server query.	
Recovery: Increase the credits configured at the device side.	

Defect ID: DEFECT000465422	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.2.0	**Technology Area:** Diagnostic Port (D_Port)
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: When enable D-port test through BNA, for F-port to HBA links in automatic mode, failure reason code is not shown correctly in case of test failure.	
Condition: Occurs when enable D-port Test for F-port to HBA links in Automatic mode, through BNA only.	
Workaround: Enable D-port Test through CLI to display the appropriate Failure Reasons.	

Defect ID: DEFECT000466240	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.1.0	**Technology Area:** NTP - Network Time Protocol
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: Switch reboots when using the tsclockserver command to set NTP with a DNS name longer than 32 characters	
Condition: tsclockserver command accepts list of NTP server address and switch reboot occurs when the NTP address with more than 32 characters is located at any position other than last in input NTP server address list.	
Workaround: Use IP address(IPV4) or DNS name with less than 32 characters to configure tsclockserver.	
Recovery: Switch will recover after reboot.	

Defect ID: DEFECT000466833	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS6.4.3	**Technology Area:** FC-FC routing
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: A 3rd party vendor device using 0x0000 as RXID instead of the standard default 0xffff cannot communicate with switch.	
Condition: If a vendor device uses 0x0000 as RXID of the frame instead of 0xffff during the initialization of exchange the frames will be rejected.	

Defect ID: DEFECT000467051	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.0.2	**Technology Area:** Fabric Watch
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: switchstatuspolicy shows incorrect port count which may impact the accuracy of switch status	
Condition: switchstatuspolicy incorrectly accounts for logical ports into the total physical port count.	

Defect ID: DEFECT000467204	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.0.0_pha	**Technology Area:** SNMPv2, SNMPv3 & MIBs
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: SNMPV3 user entries are not cleared when CMM executes restore default.	
Condition: Applicable only for embedded BR6547 platform	
Workaround: Default to snmpv3 configuration with "snmpconfig --default snmpv3" command.	

Defect ID: DEFECT000467965	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Management
Reported In Release: FOS7.2.0	**Technology Area:** Web Tools
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: Seed switch with lower versions (pre-v7.2.0) of Webtools, will incorrectly display switches running MAPS as "blue" and unknown.	
Condition: A fabric having seed switch running FOS version lower than V7.2.0 and checking for Switch Health in Webtools	

Defect ID: DEFECT000468458	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.2.0	**Technology Area:** FC-FC routing
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: FCR may indicate the error message "switch not ready for ex-ports" in switchshow.	
Condition: Repeated disruptive operation in blade/slot which is having E-Port and EX-Port in the FCR core switch may result in the error message "switch not ready for ex-ports" in switchshow output.	
Recovery: Toggle the affected Ex-ports.	

Defect ID: DEFECT000468549	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.0.2	**Technology Area:** FC-FC routing
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: Hyperswap fails after device gets name server query rejected with reason NSRJT_EXPL_NO_PORTID	
Condition: This is a timing issue that occurs rarely for a node device that sends back to back FLOGI within short span of time on the same port.	
Workaround: Disable and enable ports manually to complete site swap	
Recovery: Toggle affected ports.	

Defect ID: DEFECT000469507	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Security
Reported In Release: FOS7.0.1	**Technology Area:** Encryption
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: Tape backup jobs on encrypted tape may fail.	
Condition: Issue will be seen on Brocade Encryption Switch or FS8-18 blade with hosts and targets that doesn't support SRR/FCP_CONF and tape pipelining is enabled for the tape LUN.	
Workaround: Disable tape pipelining for tape LUNs corresponding to targets/CTC which don't support SRR/FCP_CONF.	

Defect ID: DEFECT000473144	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.1.1	**Technology Area:** Fabric Watch
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: The "fmmonitor" CLI command is able to change the time base on each filters. However, "thconfig" CLI command is unable to change the time base of each filters and displays "Timebase not supported by this class".	
Condition: Always seen while configuring time base for filters using "thconfig".	
Workaround: fmmonitor can be used in place of thconfig for timebase configuration for filter class.	
Recovery: fmmonitor can be used in place of thconfig for timebase configuration for filter class.	

Defect ID: DEFECT000473752	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.1.1	**Technology Area:** CLI
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: portaddress --show command when executed from Default Switch will display the details of the ports present in other logical switches too.	
Condition: Applicable only for VF enabled switches with no impact to the functionality.	

Defect ID: DEFECT000474101	
Technical Severity: Critical	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.0.0	**Technology Area:** supportShow
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: In a virtual fabric environment, a logical port stuck in an invalid/incomplete state triggered a switch panic during a switchshow/supportsave	
Condition: On a rare condition, in a VF environment, if a port is not indexed correctly, subsequent data collection will result in a panic.	

Defect ID: DEFECT000474392	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Security
Reported In Release: FOS7.1.0	**Technology Area:** Encryption
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: In a BES environment with CTC, hosts may lose access to LUNs temporarily.	
Condition: Issue will be seen on Brocade Encryption Switch or FS8-18 blade when BES/FS8-18 acting as an N port device, aborted the PLOGI in advance.	

Defect ID: DEFECT000474459	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Management
Reported In Release: FOS7.0.2	**Technology Area:** SNMPv2, SNMPv3 & MIBs
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: SNMP test traps are not received with "snmptraps --send" command when the switch is in AG mode.	
Condition: Impact AG switches running FOS version below v7.x.	

Defect ID: DEFECT000474697	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Security
Reported In Release: FOS7.1.0	**Technology Area:** Encryption
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: Host lost access to some paths of LUNs intermittently during encryption change commits.	
Condition: In encryption environment (BES/FS8-18), with higher ITL count configured, hosts configured with CTC may lose access to some paths of LUNs temporarily while committing the crypto configuration changes.	

Defect ID: DEFECT000475035	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Security
Reported In Release: FOS7.0.2	**Technology Area:** Encryption
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: BES becomes non-responsive and host paths are lost after BES replacement.	
Condition: Issue will be seen only in BES/FS8-18 after execution of “cryptocfg –replace” command on the group leader.	

Defect ID: DEFECT000476212	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Security
Reported In Release: FOS7.0.1	**Technology Area:** Encryption
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: Restore from encrypted tape may fail with I/O errors.	
Condition: With more than one initiator configured in a tape container and tape pipelining enabled for the LUN, a new login from a different host to virtual target may cause the on-going tape restore operation (with another host) to fail.	
Workaround: Disable tape pipelining for tape LUNs corresponding to targets/CTC where more than one host is configured.	

Defect ID: DEFECT000476595	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Security
Reported In Release: FOS7.0.2	**Technology Area:** Encryption
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: In a heavy I/O environment, tape mounts are rejected for LTO drives on encryption blade.	
Condition: In encryption environment (BES/FS8-18), while heavy tape I/Os or rekey is running through an Encryption Engine, host may experience failure in doing I/O to the tape drive LUNs configured in that Encryption Engine or lose access to the encrypted Disk LUNs.	

Defect ID: DEFECT000477188	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.1.1	**Technology Area:** Platform Services
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: During hafailover operation, switch reinitializes a port blade due to a false indication of a power (low voltage) issue.	
Condition: An i2c contention during an i2c read/write operation on FC8-48 or FC8-32 port blade, immediately following an hafailover, forces an i2c reset for the corresponding blade.	
Recovery: No further recovery is necessary, data path re-route is already initiated and the FRU re-initialized to remedy the situation.	

Defect ID: DEFECT000477596	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.0.2	**Technology Area:** Web Tools
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: Under rare condition Weblinker/HTTPD are terminated and restarted but still cannot service the HTTP requests. Further symptoms will **v**ary based on the current release on the switch. If the current release includes a fix for defect 409878 then All subsequent Webtools/BNA requests will be responded with the error message: "Chassis is not ready for management". Otherwise all subsequent Webtools/BNA requests will encounter no response.	
Condition: This may be encountered on very rare occasions when switches are managed by Webtools/BNA.	
Recovery: Recovery/workaround from this condition will vary based on the current release: If the current release includes a fix for defect 409878, use reboot to recover. Otherwise, hareboot/hafailover or contact support for manual HTTPD restart workaround.	

Defect ID: DEFECT000477854	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.0.2	**Technology Area:** ICLs - Inter-chassis Links
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: CRC with good EOF errors will be reported on multiple ICL ports in DCX	
Condition: This issue is seen rarely on DCX platforms	

Defect ID: DEFECT000477917	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS6.4.3	**Technology Area:** Routing
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: Spinfab fails across TI Zone when link cost is higher than that of normal E-ports.	
Condition: Testing ports bounced after link cost was changed to a higher than normal traffic E-ports between the same two domains.	
Workaround: Change the link cost without bouncing the port.	
Recovery: Set the link cost of testing port to the same as other online E-ports during spinfab test.	

Defect ID: DEFECT000478505	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Security
Reported In Release: FOS7.1.0	**Technology Area:** Encryption
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: During tape backups on an encrypted tape LUN, switch or blade might become faulty with message "BM-BC heartbeat dead. Sending blade fault".	
Condition: Issue may be seen during continuous backup of uncompressible data to encrypted tape.	

Defect ID: DEFECT000478551	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.2.0	**Technology Area:** Fabric Watch
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: For percentage unit, "portthconfig" CLI accepts value larger than 100 for TU area for fop-port configuration.	
Condition: Always seen while configuring TU area for fop-port class	
Workaround: Use the values 0-100 for TU area when unit is percentage.	
Recovery: Reconfigure value to be less than 100.	

Defect ID: DEFECT000480007	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.1.1	**Technology Area:** CLI
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: On reboot, sometimes the aptpolicy for a base switch does not reflect the configured value.	
Condition: Occurs after updating aptpolicy of a base switch is updated, followed by a reboot	
Workaround: Use the hafailover command instead of reboot.	
Recovery: Run the 'aptpolicy' command on the base switch.	

Defect ID: DEFECT000481199	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Management
Reported In Release: FOS7.2.0	**Technology Area:** Web Tools
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: Web Tools will be blocked while launching from Network Advisor 12.0.4 or lower version.	
Condition: On launching Web Tools from Network Advisor 12.0.4.	
Workaround: Launch Web Tools through Brocade Network Advisor running version 12.1.4 or higher. Or alternatively, configure "Java control panel -> Security setting -> Medium" (lower the security setting).	
Recovery: Use the latest Network Advisor version.	

Defect ID: DEFECT000481291	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Security
Reported In Release: FOS7.0.2	**Technology Area:** Encryption
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: After HAfailover of Group leader, member node is deleted from Encryption Group.	
Condition: On Chassis based encryption environment (FS8-18), when CP IPs are modified after changing the chassis IP, subsequent HAfailover of group leader will result in deletion of member node from Encryption group.	
Recovery: Reboot both the CPs of DCX (whose IP was changed) simultaneously.	

Defect ID: DEFECT000482076	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Management
Reported In Release: FOS7.1.0_blv	**Technology Area:** Licensing
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: While downloading firmware to 16G embedded switches using BNA 12.1.1, after a successful update of the first switch, an EGM license missing error is reported when attempting firmwaredownload on the second 16G embedded switch.	
Condition: Occurs if firmwaredownload is executed on a group of 16G embedded switch using BNA version 12.1.1.	
Workaround: From BNA, use individual switch operations instead of a group. Upgrade switches individually to a FOS release with a fix for this issue, then subsequent group operation will work.	

Defect ID: DEFECT000482227	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.1.0	**Technology Area:** CLI
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: 'portdecom' command on a port displays "Error: Request failed due to the local port not being in a ready state" message	
Condition: Occurs when 'portdecom' command runs on a trunk slave port that is connected to port index zero (0) on one end of the link and it is disabled already.	
Workaround: Do not issue 'portdecom" command on a disabled port	
Recovery: The trunk slave needs to be brought back online and then disabled by either 1) unplugging/plugging back in the cable for the slave port, or 2) using the 'portdisable' command on the slave port.	

Note: the following defects have been previously published and are formatted with the previous defect table structure.

Defect ID: DEFECT000361971	**Technical Severity:** High
Summary: i2c port reset on Brocade 8G SFPs	
Symptom: F-Port was logged out of switch due to laser fault during to media access.	
Risk of Fix: Low	**Probability:** Low
Feature: System Controls/EM	**Function:** PCI/I2C
Reported In Release: FOS7.0.0	

Defect ID: DEFECT000423640	**Technical Severity:** High
Summary: Upgrade the flash card driver to a newer version.	
Symptom: On rare occasions excessive writing to an old flash card may cause it to no longer be accessible during switch bootup.	
Risk of Fix: Low	**Probability:** Low
Feature: Embedded Platform Services	**Function:** Other
Reported In Release: FOS6.4.3_dcb	**Service Request ID:** ,1162762

Defect ID: DEFECT000433200	**Technical Severity:** Medium
Summary: Switch cannot be managed from WebTools or BNA though management via CLI works.	
Symptom: Under rare condition Weblinker/HTTPD are terminated and restarted but still cannot service the HTTP requests. All subsequent Webtools/BNA requests encounter the error "Chassis is not ready for management". Note: This fix does not fully resolve this issue but it provides a non-disruptive workaround for the interim period. With this fix customer may workaround/recover from this condition with hafailover/hareboot, or may contact support for manual HTTPD restart workaround. This issue is fully resolved via Defect 477596 fix in FOS v7.1.2/7.1.1b/7.2.1.	
Risk of Fix: Low	**Probability:** Low
Feature: FOS Software	**Function:** Management Embedded
Reported In Release: FOS7.0.2	**Service Request ID:** 1116227,1157961,1190

Defect ID: DEFECT000435100	**Technical Severity:** Medium
Summary: SNMPCONFIG is inconsistent on ISCSI settings	
Symptom: Disable ISCSI-mibcapability in FOSv6.3 and then upgraded to FOSv6.4, when the new firmware comes up, ISCSI- MIB is in disabled state and ISCSI-TRAPS are in enabled state.	
Risk of Fix: High	**Probability:** Medium
Feature: FOS Software	**Function:** SNMP
Reported In Release: FOS6.3.0	**Service Request ID:** 1124455

Defect ID: DEFECT000448581	**Technical Severity:** Medium
Summary: Port Rename, F-Port BB Credit & NPIV Max Login dialogs still persist even after the connection is timed out and allows user to configure the values.	
Symptom: User is erroneously allowed to configure the values even after the connection times out.	
Risk of Fix: High	**Probability:** Medium
Feature: WebMgmt	**Function:** Ports Admin
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000452801	**Technical Severity:** Medium
Summary: Switch unable to process commands	
Symptom: The Switch becomes unmanageable and will not accept FOS commands, including 'Reboot'. The only way to recover is to power cycle the switch.	
Workaround: Nonw	
Risk of Fix: Low	**Probability:** Low
Feature: FOS Software	**Function:** Management Embedded
Reported In Release: FOS7.1.0	

Defect ID: DEFECT000453711	**Technical Severity:** Medium
Summary: Certificate key is not deleted when the certificate is deleted from Non-Default switch using seccertutil command.	
Symptom: Standby CP/switch may continuously reboot with error message such as "SSLCertificateFile: file '/etc/fabos/certs/sw0/xxx.crt' does not exist or is empty on console".	
Workaround: Remove the truncated 0 size SSL certificate file and reboot	
Risk of Fix: Low	**Probability:** Medium
Feature: FOS Software	**Function:** High Availability
Reported In Release: FOS7.1.0	**Service Request ID:** 1090957

Defect ID: DEFECT000460453	**Technical Severity:** Medium
Summary: Error messages are displayed on embedded platform console during boot up and do not affect any functionality.	
Symptom: "Can not find platform: 117" and "client: connect: Connection refused" messages occurred during boot up	
Risk of Fix: High	**Probability:** High
Feature: Embedded Platform Services	**Function:** FOS Kernel Driver
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000461267	**Technical Severity:** High
Summary: Host logs in as G-port on access gateway when n-port connection is pulled	
Symptom: Host failed to login to a Access Gateway switch. FLOGIs are not replies resulting in Gport.	
Workaround: Reboot Server, AG or some manual recovery method.	
Risk of Fix: Low	**Probability:** High
Feature: Access Gateway Services	**Function:** Other
Reported In Release: FOS7.1.0	

Defect ID: DEFECT000462242	**Technical Severity:** Medium
Summary: Inconsistent enforcement of RBAC permissions for config commands run in interactive mode and in non-interactive mode	
Symptom: For Chassis and LF user role as "user", config commands(configshow/configdownload/configupload) trigger "RBAC permission denied." in interactive mode where as it works in non-interactive mode	
Risk of Fix: Low	**Probability:** High
Feature: FOS Software	**Function:** Fabric Services
Reported In Release: FOS6.3.2	**Service Request ID:** 1171446

Defect ID: DEFECT000463913	**Technical Severity:** Medium
Summary: Kernel panic occurs when running multiple supportShow commands in several logical switches	
Symptom: The switch experienced a kernel panic after running the supportShow command on multiple logical switches simultaneously on the switch.	
Workaround: Avoid running multiple supportshow from the different sessions.	
Risk of Fix: Low	**Probability:** Low
Feature: FOS Software	**Function:** Panic / OOM
Reported In Release: FOS7.1.0	**Service Request ID:** 1187706

Defect ID: DEFECT000464907	**Technical Severity:** High
Summary: Misbehaving device cause switch to panic	
Symptom: During a period of time, device sends switch non-stop 0 sized ELS frames. These 0 sized frames were not properly checked and freed, and eventually the switch panics after running of memory.	
Risk of Fix: Low	**Probability:** Low
Feature: FOS Software	**Function:** Panic / OOM
Reported In Release: FOS6.1.0_utah	**Service Request ID:** 1192317

Defect ID: DEFECT000465730	**Technical Severity:** Medium
Summary: Update asic parity error monitoring threshold and behavior.	
Symptom: Default threshold for low level Asic parity error will fault blade with a few error. New CLI options to "chassiscfgperrthr" will allow customers to adjust the values based on their environments.	
Risk of Fix: Low	**Probability:** Low
Feature: FOS Software	**Function:** ASIC Driver
Reported In Release: FOS7.1.0	

Defect ID: DEFECT000465802	**Technical Severity:** Medium
Summary: Webtools does not allow the configuration of the "Signal Loss" area for ports	
Symptom: Customer is unable to see “signal loss” area stats via Webtools while the same can be seen from CLI	
Risk of Fix: Low	**Probability:** Medium
Feature: FOS Software	**Function:** Web Management
Reported In Release: FOS7.1.1	**Service Request ID:** 1190629

Defect ID: DEFECT000465879	**Technical Severity:** High
Summary: 16Gb SFP rules for TXP and SFP Current are violated when a neighbor EPort transitions online.	
Symptom: Invalid reporting of MAPS 16G SFP rules for optic when its neighbor EPort transitions online.	
Risk of Fix: High	**Probability:** High
Feature: Advanced Monitoring Services	**Function:** Other
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000466750	**Technical Severity:** Medium
Summary: Misleading last updated time in Switch Events and Switch Information tab.	
Symptom: In Switch Events and Switch information tab, the last updated time shows the Host time instead of showing the Switch time.	
Risk of Fix: High	**Probability:** Low
Feature: WebMgmt	**Function:** Switch Explorer/Switch View
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000466943	**Technical Severity:** Medium
Summary: After a very fast portdisable/portenable test sequence in a script, the port no longer sends or receives traffic	
Symptom: If a port is enabled and then disabled within about 1 second, the next time it is enabled the port may not be able to pass traffic.	
Workaround: Allow two seconds between port enables and port disables.	
Risk of Fix: Low	**Probability:** Low
Feature: 8G ASIC Driver	**Function:** Routing
Reported In Release: FOS7.0.2	**Service Request ID:** 1195567

Defect ID: DEFECT000467589	**Technical Severity:** Medium
Summary: snmpconfig does not show community 1 during configuration on v7.1.1	
Symptom: User cannot configure "community 1" with snmpconfig --set command	
Risk of Fix: Medium	**Probability:** Medium
Feature: FOS Software	**Function:** SNMP
Reported In Release: FOS7.1.1	**Service Request ID:** 1194854

Defect ID: DEFECT000467681	**Technical Severity:** High
Summary: Blade server shows incorrect firmware version in IOM module after a switch hotplug	
Symptom: Blade server still displays older Firmware Version in IOM module after upgrade and shows none after switch hotplug	
Risk of Fix: Low	**Probability:** High
Feature: Embedded Platform Services	**Function:** Other
Reported In Release: FOS7.2.0	**Service Request ID:** 1001

Defect ID: DEFECT000467760	**Technical Severity:** Medium
Summary: Disabled port is not getting enabled after binding a port address.	
Symptom: Port is disabled after binding a port address.	
Workaround: Nonw	
Risk of Fix: High	**Probability:** Low
Feature: WebMgmt	**Function:** Ports Admin
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000468007	**Technical Severity:** High
Summary: Host discovery issues via Ex ports on ICL in multi chassis configuration	
Symptom: Host may not see all target LUNs in a topology using multi-chassis EX ports on ICL configuration	
Workaround: Portdisable enable switch ports for affected devices.	
Risk of Fix: Low	**Probability:** Medium
Feature: FC Services	**Function:** Name Server
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000468152	**Technical Severity:** High
Summary: after zone change nszonemember missing members and ports show HARD_PORT dhp bit set: 1	
Symptom: A zoning change (removal) was made from the core switch at which time the name server stopped responding, causing outages on the hosts.	
Workaround: Allow 5 minutes delay between cfgsave and cfgenable command	
Risk of Fix: Low	**Probability:** Low
Feature: FOS Software	**Function:** Fabric Services
Reported In Release: FOS7.0.2	**Service Request ID:** 1202661,1249899,7610

Defect ID: DEFECT000468188	**Technical Severity:** High
Summary: Observed MDD kept crashing when a DS was set persistently disabled	
Symptom: User may see MDD hit rolling crashing when the switch is configure VF mode and the DS switch is set disable persistently with MAPS enabled.	
Risk of Fix: High	**Probability:** Low
Feature: Advanced Monitoring Services	**Function:** Other
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000468413	**Technical Severity:** High
Summary: firmwaredownload -s on standby CP produces protocol failure in circuit setup messages on the console	
Symptom: Firmware download on the standby CP takes a long time to reach Y/N prompt and several "poll: protocol failure in circuit setup" console messages resulted.	
Risk of Fix: High	**Probability:** Low
Feature: Striker/Spike Platform Services	**Function:** VEX
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000468455	**Technical Severity:** High

Summary: QoS allowed ASIC buffer pool to become over allocated	
Symptom: Portbuffershow indicated a negative value in the remaining buffers after QoS was enabled on an extended distance link	
Risk of Fix: Low	**Probability:** Medium
Feature: 8G ASIC Driver	**Function:** ASIC Driver
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000468777	**Technical Severity:** Medium
Summary: portcfgpersistentdisable -r does not persist the reason on reboot of a 7800	
Symptom: port reason does not persist across a reboot on a 7800 switch when portcfgpersistentdisable -r is configured	
Risk of Fix: High	**Probability:** Medium
Feature: 8G Platform Services	**Function:** Other
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000468795	**Technical Severity:** High
Summary: FCIP FICON XRC Emulation Abort after Selective Reset Errors	
Symptom: If FICON XRC Emulation receives a Selective Reset for a device that is currently in Stacked Status State, the Selective Reset is incorrectly responded to by emulation processing leading to an abort sequence from the channel for the Selective Reset Exchange.	
Risk of Fix: High	**Probability:** Low
Feature: FCIP	**Function:** Emulation
Reported In Release: FOS7.0.0	**Service Request ID:** 1205859

Defect ID: DEFECT000469915	**Technical Severity:** High
Summary: nscamshow report state is unknown for remote switches	
Symptom: nsshowall fails to display PIDS for switches that are connected using long distance E_Ports.	
Risk of Fix: Low	**Probability:** Low
Feature: FOS Software	**Function:** Fabric Services
Reported In Release: FOS6.4.2	**Service Request ID:** 1209801

Defect ID: DEFECT000470123	**Technical Severity:** High
Summary: Switch running agshow panics or BNA seed switch panics when polling for AG info in a fabric with AG switches.	
Symptom: After the port connecting AG to switch bounces, before fabric management server and name server data base are stabilized, polling from BNA caused seed switch to panic, similarly run agshow on switch can cause switch to panic. The timing window for triggering the panic is very small.	
Workaround: avoid agshow CLI and managing switch via BNA.	
Risk of Fix: Low	**Probability:** Medium
Feature: FOS Software	**Function:** Fabric Services
Reported In Release: FOS7.0.0	**Service Request ID:** 1206464

Defect ID: DEFECT000470185	**Technical Severity:** High
Summary: portcfgfillword's passive option does not work	
Symptom: The passive option in portCfgFillWord does not work. When issuing: "portcfgfillword <slot/port> 3 passive". The fillword immediately takes effect on the port, regardless of port speed.	
Risk of Fix: High	**Probability:** Medium
Feature: 8G ASIC Driver	**Function:** C2 ASIC driver
Reported In Release: FOS7.2.0	**Service Request ID:** ,1190443

Defect ID: DEFECT000470487	**Technical Severity:** Medium
Summary: Fabric watch not calculating VEX port packet loss correctly.	
Symptom: Erroneous FW-1190 error messages seen on different VEX tunnels: Event: , VEXport#3/16,Packet Loss, is above high boundary(High=100, Low=0). Current value is 1176 Percentage(%). Severity: Warning	
Risk of Fix: High	**Probability:** Medium
Feature: FABRIC WATCH	**Function:** Other
Reported In Release: FOS7.2.0	**Service Request ID:** 1197444

Defect ID: DEFECT000471333	**Technical Severity:** Critical
Summary: FLOGI frame with conflicting vendor specific field triggered switch to panic in a loop.	
Symptom: Switch starts rolling reboot. After it stops, type in any command, it will show: "fabos not yet initialized". Further investigation shows device FLogi has certain Vendor Version Level (VVL) bits set unexpectedly	
Workaround: Keep the port connected to the conflicting device in disabled state or reboot the conflicting device.	
Risk of Fix: Low	**Probability:** Low
Feature: FOS Software	**Function:** Fabric Services
Reported In Release: FOS7.0.0	**Service Request ID:** 1213514

Defect ID: DEFECT000471723	**Technical Severity:** High
Summary: FLOGI ACC not being sentfrom switch in AG mode during N_Port offline/online	
Symptom: redundant HBA port fails to come online when N_Port is offline/online	
Risk of Fix: Low	**Probability:** Low
Feature: FOS Software	**Function:** Access Gateway
Reported In Release: FOS7.0.0_pha	**Service Request ID:** 1208458

Defect ID: DEFECT000471755	**Technical Severity:** High
Summary: Flow monitor does not work on internal ports on embedded platforms in access gateway mode	
Symptom: Flow monitor is not supported on internal ports of access gateway embedded platforms.	
Risk of Fix: Low	**Probability:** High
Feature: Network Patroller	**Function:** ASIC interfaces
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000471823	**Technical Severity:** High
Summary: FICON Tape Write Emulation control variables go negative causing limited tape performance	
Symptom: Write Emulation Counters go negative causing limited performance. FICON Tape window sizes are never increased from a pipeline of 1 (1 chain).	
Risk of Fix: Low	**Probability:** Low
Feature: FOS Software	**Function:** FCIP
Reported In Release: FOS7.0.0	**Service Request ID:** 1212822

Defect ID: DEFECT000472367	**Technical Severity:** High
Summary: An EX-Port goes into Mod_Invalid state after a switch disable/enable of a core backbone switch	
Symptom: When a user performs a switch disable/enable, one of the EX-Ports can go into the Mod_Invalid state with Speed Mismatch/Incompatible sfp reason	
Risk of Fix: Low	**Probability:** Low
Feature: 16G Platform Services	**Function:** FOS Kernel Drivers
Reported In Release: FOS7.2.0	**Service Request ID:** ,1235215

Defect ID: DEFECT000472563	**Technical Severity:** Medium
Summary: GA_NXT is rejected causing path loss	
Symptom: After rebooting a host, a subsequent GA_NXT is performed by that is rejected by the switch causing path fail for host storage.	
Risk of Fix: Low	**Probability:** Low
Feature: FOS Software	**Function:** Fabric Services
Reported In Release: FOS6.4.2	**Service Request ID:** 1218867

Defect ID: DEFECT000472649	**Technical Severity:** Medium
Summary: Web Tools launch issue on Embedded FOS switches	
Symptom: When using web tools to connect to admin domains error message "error loading fabric tree. null" displays	
Risk of Fix: Low	**Probability:** Low
Feature: FOS Software	**Function:** Web Management
Reported In Release: FOS7.0.2	**Service Request ID:** 1206388

Defect ID: DEFECT000472858	**Technical Severity:** High
Summary: A learning flow does not monitor all real flows on the egress port.	
Symptom: A learning flow, defined on an egress port with both generator and monitor features specified and also has either srcdev or dstdev option as '*' will monitor less number of flows than actual number of flows going through the egress port. This will only happen when the number of real flows exceeds 32.	
Risk of Fix: Low	**Probability:** Medium
Feature: Network Patroller	**Function:** Flow monitor
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000472886	**Technical Severity:** High
Summary: FCIP FICON Tape Emulation not going into read pipelining due to synchronizing status bit set in 1st command in chain	
Symptom: Slow FICON tape read performance due to long running restore/recall jobs	
Risk of Fix: Low	**Probability:** Medium
Feature: FOS Software	**Function:** FCIP
Reported In Release: FOS7.0.0	**Service Request ID:** 1219501

Defect ID: DEFECT000473053	**Technical Severity:** High
Summary: Previously defined SIM port Flow Vision flows are retained after configdefault, configupload, and configdownload operations	
Symptom: The previously defined flows reappeared when the uploaded default config file was down loaded and made effective on the switch.	
Risk of Fix: Low	**Probability:** Medium
Feature: Network Patroller	**Function:** Other
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000473063	**Technical Severity:** High
Summary: SIM ports stuck as G-port when changing a logical switch to a base switch	
Symptom: Ports that are configured as SIM ports in a logical switch are get stuck in an invalid state when the logical switch is reconfigured as Base switch	
Workaround: Remove configured SIM ports before converting logical switch to base switch	
Risk of Fix: Low	**Probability:** Medium
Feature: Network Patroller	**Function:** ASIC interfaces
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000473548	**Technical Severity:** High
Summary: When flows are monitored in MAPS, switch disable/enable or port enable/disable could trigger unexpected MAPS RASLOGs	
Symptom: Unexpected MAPS RASLOGs with large values are triggered for the flows affected by port enable/disable or switch enable/disable operations.	
Risk of Fix: Low	**Probability:** High
Feature: Advanced Monitoring Services	**Function:** Flows
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000473940	**Technical Severity:** High
Summary: C2-1013 Duplicate rte_tbl_select detected! observered after upgrade.	
Symptom: After upgrading from v6.4.3b to v7.0.2c several ports observed C2-1013 (Duplicate rte_tbl_select detected!) messages.	
Workaround: None currently.	
Risk of Fix: Low	**Probability:** Low
Feature: FOS Software	**Function:** ASIC Driver
Reported In Release: FOS7.0.2	**Service Request ID:** 1225833

Defect ID: DEFECT000473948	**Technical Severity:** High
Summary: Using BNA to distribute a modified MAPS policy across a fabric of switches and director chassis fails with a generic error message "'failed to create policy"	
Symptom: Attempt to distribute modified MAPS policy fails with a generic error message that can't be used for correcting the problem	
Risk of Fix: Low	**Probability:** Medium
Feature: Mgmt Embedded – CAL	**Function:** Other
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000474234	**Technical Severity:** Medium
Summary: Multiple aborted FICON sequences after processing emulated attention in zOS third party remote mirror	
Symptom: Third party remote mirror does successfully configure but FICN-1062 and FICN-1063 RASLOG messages and associated XTUN-1999 FTRACE messages and zOS IOS000 errors are recorded in SYSLOG	
Risk of Fix: Low	**Probability:** Low
Feature: FCIP	**Function:** FCIP-RAS
Reported In Release: FOS7.1.0	**Service Request ID:** 1226196

Defect ID: DEFECT000474717	**Technical Severity:** High
Summary: FICON Disk warm start processing causes inoperative CHPIDs through an XRC emulation enabled FCIP Tunnel	
Symptom: FICON Error: IOS001E devAddr,INOPERATIVE PATH on CHPID after the disck controller warm start was initiated.	
Workaround: Disable all FICON emulation features on the FCIP Tunnels that provide access to the Disk Subsystem.	
Risk of Fix: High	**Probability:** Medium
Feature: FCIP	**Function:** Emulation
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000475320	**Technical Severity:** Medium
Summary: Reset doesn't work for flow mirror feature when wrap is disabled	
Symptom: Unable to reset a flow mirror when wrap is disabled.	
Risk of Fix: Low	**Probability:** Medium
Feature: Network Patroller	**Function:** Flow Mirroring
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000475599	**Technical Severity:** Medium
Summary: mapssam --show does not show port type of N_port trunks for FOS switch ports attached to access gateway	
Symptom: Customer cannot identify port type of N_port trunks in AG using CLI "mapssam --show"	
Risk of Fix: Low	**Probability:** Medium
Feature: Advanced Monitoring Services	**Function:** Other
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000477049	**Technical Severity:** Medium
Summary: Unable to sort columns in name server section of FOS Web Tools	
Symptom: Data is not sorted when toggling column headers of the name server section in Web Tools	
Risk of Fix: Low	**Probability:** Medium
Feature: WebMgmt	**Function:** Name Server
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000478713	**Technical Severity:** Medium
Summary: Requesting clarification on operation of errdump --all	
Symptom: Need to verify a switch for a CLI command errdump --all shows the RASLOG of FIDs which user does not have privilege	
Risk of Fix: Low	
Feature: Man Pages	**Function:** Edit/Correct
Reported In Release: FOS7.1.1	**Service Request ID:** 1240895/P1231164

Appendix: Additional Considerations for FICON Environments

FOS v7.2.1d is FICON qualified release based on FICON contents as those in FOS v7.2.0d. All hardware platforms and features supported in FOS v7.2.0d are also supported in FOS v7.2.1d.

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.

Notes on FICON Support

- Multiple 10 Gb/sec ISLs and FCIP links can load-share between cascaded FICON directors/switches but do not load balance in a FICON configuration.
- 10-bit addressing mode is not supported in a FICON environment.
- Please refer to the *Firmware Upgrades and Downgrades* section of this document when planning an upgrade to a fabric that includes the 7800 or has any FX8-24 blades in a DCX, DCX-4S, DCX8510-8, or DCX8510-4 chassis.

Area	Comments
Cascading	There are special configuration considerations for environments with three or more switches (domain IDs) in a FICON fabric. Assistance from service support should be sought to ensure proper configuration.
Cascading	Fiber ICL configurations (with DCX8510-8/DCX8510-4) supported for FICON are the same as the supported configurations for copper ICLs (with DCX/DCX-4S).
Cascading	Encryption and compression is supported on Fibre Channel ISLs in addition to IP links.
FCIP	VEX ports are not supported on the 7800 and FX8-24 blade in a FICON environment
FCIP	When performing multiple cabling changes to the SAN fabric in a FICON Emulating FCIP Tunnel configuration with the Brocade 7800 or FX8-24 blade, either disable all of the FCIP Tunnels or issue the switch disable command on all FCIP interconnected switches to avoid IFCCs in a mainframe environment. Issuing either a switch disable or an FCIP Tunnel disable command will allow the FCIP FICON Emulation processing state-machine to execute an orderly cleanup process and allow normal activation of the new configuration. When all cabling and Traffic Isolation Zone manipulations have been completed, enable the switches or the FCIP Tunnels.
FCIP	A disabled XGE or GE port will be re-enabled after a code upgrade/downgrade. To prevent XGE/GE ports from being re-enabled after a code load they should be persistently disabled.
Firmware Downloads	Firmware upgrades for FICON are only supported from FOS v7.1.0c or FOS v7.2.0d.
Firmware Downloads	Non-disruptive Hot Code Load is only supported on director class switches (DCX, DCX-4S, DCX8510-8, and DCX8510-4). Comprehensive non-disruptive Hot Code Load is not supported on the 7800 or a DCX, DCX-4S, DCX8510-8, or DCX8510-4 with an FX8-24 blade since the FCIP tunnels will go down for 10-15 seconds and all traffic in the tunnels will be disrupted. IFCCs may result if traffic is not stopped while downloading firmware.
Firmware Downloads	The CUP device must be varied offline to all MVS partitions before starting a code load. The CUP device can be varied back online after the code load completes. Failure to vary off the CUP devices may result in missing interrupt.

<table>
<tr><th>Area</th><th>Comments</th></tr>
<tr><td>Firmware Downloads</td><td>When downgrading from v7.2.1d to v7.1.0c, ICL ports might go down with port status In_Sync or Port_Flt when FMS mode is turned on and XISLs are configured.
Contact device support to get a special version of FOS v7.1.0c for downgrading from v7.2.1d to v7.1.0c in this scenario.</td></tr>
<tr><td>Interoperability</td><td>When connecting an 8G or 16G capable port in a Brocade switch to an IBM Virtualization Engine TS7700 with R1.6 or below, the port must be configured to a minimum of 16 buffers to avoid IFCCs at the channel and loss of FICON paths to the control unit. This requires the Extended Fabric license on the Brocade switch.
The recommended best practice is to upgrade the TS7700 to R1.7 or higher and leave the BB credits of the switch port at the default setting of 8.
Contact TS7700 device support to determine proper settings of your device.</td></tr>
<tr><td>Manageability</td><td>It is suggested that Port Fencing be used to avoid taking ports down for normal fabric events. The recommended fencing criteria and settings are:
<table>
<tr><th>Criteria</th><th>Value</th></tr>
<tr><td>ITW (Invalid Transmission Words)</td><td>25 per minute</td></tr>
<tr><td>CRC (Cyclical Redundancy Check)</td><td>3 per hour</td></tr>
<tr><td>Protocol Errors</td><td>2 per minute</td></tr>
<tr><td>State Change</td><td>7 per minute</td></tr>
<tr><td>Link Reset</td><td>3 per minute</td></tr>
</table>
Note: Port fencing should not be set for C3 discards.</td></tr>
<tr><td>Manageability</td><td>As a "Best Practice" for deploying FOS switches/directors into a FICON environment, verify the FOS version shipped with the most current FOS recommendation. It is recommended to update all FOS switch/directors to the same FOS levels for production.</td></tr>
<tr><td>Manageability</td><td>FMS must be enabled on the local switch for the remote CUP to work.</td></tr>
<tr><td>Manageability</td><td>The FICON merge wizard feature in Network Advisor cannot be used to merge a 48000 with a DCX, DCX-4S, DCX8510-8, or a DCX8510-4.</td></tr>
<tr><td>Manageability</td><td>When setting insistent domain ID on a switch using the FICON Configuration Wizard, the switch will always be taken offline and insistent domain ID set, even if insistent domain ID is already set.</td></tr>
<tr><td>Optics</td><td>When configuring inter-switch links (ISLs) between a 16G platform and an 8G platform, the ISL ports must be configured for E-Port only.</td></tr>
<tr><td>Serviceability</td><td>zDAC may not give reliable results. The SIOCA tool run from HMC on System z performs a similar function and therefore may not give reliable results as well.</td></tr>
<tr><td>Traffic Isolation Zones</td><td>Under certain circumstances, enabling multiple Traffic Isolation Zones with failover disabled may cause some frames to be dropped due to the timing of when paths are re-routed while the zones are being implemented. To avoid this, all Traffic Isolation Zones should be enabled with failover enabled first so that all desired routes are established.</td></tr>
<tr><td>Traffic Isolation Zones</td><td>Assistance from service support should be sought before attempting to configure and enable this feature.</td></tr>
</table>

Area	Comments
Virtual Fabrics	Assistance from service support should be sought before attempting to enable Virtual Fabrics or use the XISL (Base Switch ISL) capability.
Virtual Fabrics	If a port gets assigned a port address of 0xFE in an Open System logical switch, an RSCN will be sent by FOS on behalf of port address 0xFE during CP failover or firmware download. This may result in an IFCC for any FCP channel running traffic to port address 0xFE.

Maximum CUP Support

This table indicates the maximum supported number of logical switches that can have FMS (CUP) enabled on the specified platform.

Platform	Maximum Number of CUP Instances
8510-8	4
8510-4	4
6510	2 (no base switch)
DCX	4
DCX-4S	4
5300	4
7800	2 (no base switch)

Interoperability

When cascaded to other switches, referred to as a "fabric," all switches in the fabric must be at FOS v7.1.0c or FOS v7.2.0d before upgrading to v7.2.1d. Interoperability between switches at FOS v6.4.2a, FOS v7.0.0c, FOS v7.0.0d, FOS v7.1.0c, FOS v7.2.0d and FOS v7.2.1d is supported; however, the recommended best practice is to have all switches in the same fabric at the same code level.

The following section indicates supported intra-fabric interoperability between hardware platforms, supported management software levels, and recommended firmware versions.

FICON Hardware/Firmware/Software Interoperability with FOS v7.2.1d

Interoperability is supported with FOS v7.2.1d between the following platforms:

- DCX
- DCX-4S
- DCX8510-8
- DCX8510-4
- 6510
- 5300
- 7800

All platforms operating with FOS v7.2.1d must be managed with Brocade Network Advisor v12.1.3 or later. FICON support for FOS v7.2.1d starts with Brocade Network Advisor v12.1.3 – please check Brocade Network Advisor release notes for latest updates.

The following platforms using **FOS v6.4.2a, FOS v7.0.0c, FOS v7.0.0d, FOS v7.1.0c or FOS v7.2.0d** may also interoperate in a fabric with switches running FOS v7.2.1d:

- DCX
- DCX-4S
- 5300
- 5100
- 7800
- 48000

Platforms operating with FOS v7.1.0c can be managed with Brocade Network Advisor v12.1.3.

The following platforms are NOT supported for interoperability in fabrics with switches using FOS v7.x:

- M6140
- Mi10K
- 7500/7500