Brocade Fabric OS v7.1.1
Release Notes v1.0

May 30, 2013

Document History

Document Title	Summary of Changes	Publication Date
Brocade Fabric OS v7.1.1 Release Notes v1.0	Initial Release	May 30, 2013

Contents

Overview

Fabric OS (FOS) v7.1.1 is a maintenance release based on FOS v7.1.0. All hardware platforms and features supported in FOS v7.1.0 are also supported in FOS v7.1.1. This release also contains fixes for many defects including those from the FOS v7.1.0a, b, and c patch releases.

Warning – Applicable only if upgrading from FOS v7.1.0:

Before upgrading the firmware to FOS v7.1.1 from FOS v7.1.0, you must run the **supportSave** command to save any existing error log information. Once the switch is upgraded to FOS v7.1.1, any previously existing error log entries on the switch will be permanently lost - only new error log entries created while running FOS v7.1.1 will be retained.

Note: This warning is not applicable if the current firmware version is not FOS v7.1.0. For example, if the upgrade is being performed from FOS v7.1.0a, FOS v7.1.0b, FOS v7.1.0c, FOS v7.0.x to FOS v7.1.1, the existing error log entries will be preserved even after upgrading to FOS v7.1.1. Please refer to "FOS Migration Considerations" section of this document for additional considerations.

Resolution of Important Defects

Defect 446858: In a heavily congested fabric, if a HAfailover happens when a backend port is reporting frame timeout, switch falsely identifies stuck VC and performs link reset.

Defect 442080 : Making auto-tuned value persistent across reboot

Defect445644: BES went into low memory state because of "Continuous polling from BNA"

Defect442422: System security card is not being read on BES/FS8-18 card readers

Defect446429: ASIC entries are not being cleared upon 8510 hafailover processing leading to server issues

New Features & Support

In addition to fixes for defects, there is new support in FOS v7.1.1 including:

- Support for SmartOptics 8G CWDM 70km SFP+
    - Supported only on FC8-xx (FC8-16, FC8-32, FC8-48) blades in DCX and DCX-4S
    - Supported only on FC8-xx (FC8-32E, FC8-48E), FC16-xx (FC16-32, FC16-48) blades on DCX 8510-8 and DCX 8510-4
- Support for SmartOptics 8G DWDM 40km SFP+
    - Supported only on FC8-xx (FC8-16, FC8-32, FC8-48), FX8-24 blades in DCX and DCX-4S
    - Supported only on FC8-xx (FC8-32E, FC8-48E), FX8-24, FC16-xx (FC16-32, FC16-48) blades in DCX 8510-8 and DCX 8510-4
    - Supported on 300, 5100, 5300, 6505, 6510, 6520, 7800

Optionally Licensed Software

Fabric OS v7.1 includes all basic switch and fabric support software, as well as optionally licensed software that is enabled via license keys.

Optionally licensed features supported in FOS v7.1 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 Fabric or E_Port or Full Fabric— This license enables a switch to connect to a multi-switch fabric via E_Ports, forming ISL connections.

Note: This license is only required on select embedded switch models and the Brocade 300, and does not apply to other fixed-port switches or chassis-based platforms.

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

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 and provides notification if established limits or thresholds are exceeded. Fabric Watch includes Port Fencing capabilities.

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 license is enabled by default on all 16G FC platforms, and on DCX and DCX-4S platforms that are running Fabric OS v7.0.0 or later.

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 included in this license, and are fully available on all 8Gb and 16Gb platforms.

Note: 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 (SAO) — 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: 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 a dedicated router to a fabric for FCR purposes.

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.

Brocade 8000 FC Ports on Demand — This license enables all eight FC ports on the Brocade 8000.

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 or the 10G FC capability on FC16-xx blade ports. On the Brocade 6510 and Brocade 6520, this license enables 10G FC ports. This license is available on the DCX/DCX-4S/DCX 8510-8/DCX 8510-4 on an individual slot basis.

- **FX8-24:** With this license 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
- **FC16-xx:** Enables 10G FC capability on an FC16-xx blade in a slot that has this license
- **Brocade 6510, Brocade 6520:** Enables 10G FC capability on the switch

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 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 participating in a group of five or more Brocade DCX 8510 chassis connected 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 how many chassis are interconnected via ICLs. This license is only 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.

Fabric Insight License - The new Fabric Vision license is being introduced as part of some software bundles and that it enables new functionality being introduced in FOS v7.2. When installed on a switch operating with FOS v7.1.x, the licenseshow command will display this as the "Fabric Insight license," and it does not enable or affect any functionality on the switch.

Temporary License Support

The following licenses are available in FOS v7.1 as Universal Temporary or regular temporary licenses:

- Fabric (E_Port) license
- Extended Fabric license
- Trunking license
- High Performance Extension license
- Advanced Performance Monitoring license
- Adaptive Networking license
- Fabric Watch license
- Integrated Routing license
- Server Application Optimization license
- Advanced Extension license
- Advanced FICON Acceleration license
- 10GbE FCIP/10G Fibre Channel license
- FICON Management Server (CUP) license
- Enterprise ICL 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.

Other Licensing Changes

- The capabilities associated with the Adaptive Networking and SAO licenses are included by default on the Brocade 6520. Hence these licenses are not applicable to the Brocade 6520 platform.

Supported Switches

- Fabric OS v7.1 supports the Brocade 300, 5410/5424/5430/5450/5460/5470/5480/NC-5480, 5100, 5300, VA-40FC, Brocade Encryption Switch (BES), DCX/DCX-4S, 8000, 7800, 6505, 6510, 6520, DCX 8510-8 and DCX 8510-4.

Access Gateway mode is also supported by Fabric OS v7.1, and is supported on the following switches: the Brocade 300, 5100, VA-40FC, 8000, 5450, 5430, 5460, 5470, 5480, NC-5480, M5424, 6510, 6505.

Standards Compliance

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

The Brocade 8000 and 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 Brocade 8000 and 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:

   ```
   FT00X0054E9
   ```

   AVS0305E012

   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 8000 — On the switch ID pullout tab located inside the chassis on the port side on the left and also on the bottom of the chassis
   - 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 v7.0.x or FOS v7.1.0x can be non-disruptively upgraded to FOS v7.1.1. This upgrade is non-disruptive to both FC and FCoE traffic (when using FCOE10-24 blades).

FR4-18i and FC10-6 blades are not supported on DCX/DCX-4S with FOS v7.1 or later. Hence these blades must be removed from the chassis before upgrading the firmware to FOS v7.1.1.

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.

Disruptive upgrades to Fabric OS v7.1.1 are allowed and supported from FOS 6.4.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.

The Brocade 8000 does not support non-disruptive hot code loads (HCL). Upgrading the Brocade 8000 to FOS v7.1.1 will be disruptive to the I/O through the switch.

Recommended Migration Paths to FOS v7.1.1

Migrating from FOS v7.1.0

Warning

Before upgrading the firmware to FOS v7.1.1 from FOS v7.1.0, you must run the supportSave command to save any existing error log information. Once the switch is upgraded to FOS v7.1.1, any previously existing error log entries on the switch will be permanently lost - only new error log entries created while running FOS v7.1.1 will be retained.

Any 8G or 16G platform running FOS v7.1.0 can be non-disruptively upgraded to FOS v7.1.1. However, any previously existing error log entries with FOS v7.1.0 will be permanently lost once upgraded to FOS v7.1.1.

Migrating from FOS v7.1.0x

Any 8G or 16G platform running any FOS v7.1.0x (FOS v7.1.0a, FOS v7.1.0b, FOS v7.1.0c) firmware can be non-disruptively upgraded to FOS v7.1.1.

Migrating from FOS v7.0.1x or 7.0.2x

Any 8G or 16G platform running any FOS v7.0.1x /FOS v7.0.2x firmware can be non-disruptively upgraded to FOS v7.1.1. However, users must pay close attention to the following before upgrading the DCX 8510 platforms to FOS v7.1.1:

If the upgrade on a DCX 8510 from FOS v7.0.1x/FOS v7.0.2x to FOS v7.1.1 is blocked due to the absence of the EICL license, users must first install the EICL license on the DCX 8510 and then proceed with upgrading the firmware to FOS v7.1.1.

Migrating from FOS v7.0.0x

Any 8G or 16G platform running any FOS v7.0.0x firmware can be non-disruptively upgraded to FOS v7.1.1. However, users must pay close attention to the following before upgrading the DCX 8510 platforms to FOS v7.1.1:

If the upgrade on a DCX 8510 from FOS v7.0.0x to FOS v7.1.1 is blocked due to the absence of the EICL license, users must first upgrade the DCX 8510 to FOS v7.0.1x or later, install the EICL license on the DCX 8510, and then proceed with upgrading the firmware to FOS v7.1.1.

Migrating from FOS v6.4.x

DCX/DCX-4S units running any FOS v6.4.x firmware must be upgraded to FOS v7.0.x before they can be non-disruptively upgraded to FOS v7.1.1.

Any 8G platforms (other than DCX/DCX-4S) that are currently operating at lower than FOS v6.4.1a must be upgraded to FOS v6.4.1a or later, they then must be upgraded to FOS v7.0.x, before non-disruptively upgrading to FOS v7.1.1. Upgrading these platforms from any FOS V6.4.x release **lower than FOS v6.4.1a to FOS v7.0.x will cause disruption to FC traffic**.

Any 8G platform operating at FOS v6.4.1a or later versions of FOS v6.4.x must be upgraded to FOS v7.0.x or later before non-disruptively upgrading to FOS v7.1.1.

Migrating from FOS v6.4.1_fcoe1

Units running FOS v6.4.1_fcoe1 must be upgraded to FOS v7.0.x before non-disruptively upgrading to FOS v7.1.1.

Important Notes

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

Brocade Network Advisor Compatibility

Brocade® Network Advisor provides the industry's first unified network management solution for data, storage, and converged networks. It supports Fibre Channel Storage Area Networks (SANs), Fibre Channel over Ethernet (FCoE) networks, Layer 2/3 IP switching and routing networks, wireless networks, application delivery networks, and Multiprotocol Label Switching (MPLS) networks. In addition, Brocade Network Advisor supports comprehensive lifecycle management capabilities across different networks through a seamless and unified user experience. It is the next-generation successor product to legacy Brocade management products (Brocade Data Center Fabric Manager (DCFM), Brocade Fabric Manager (FM) and Brocade Enterprise Fabric Connectivity Manager (EFCM)).

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 12.0.0 is available in

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

For SAN Management, Network Advisor 12.0 is available in three editions:

- *Network Advisor Professional:* a fabric management application that is ideally suited for small-size businesses that need a lightweight management product to manage their smaller fabrics. It manages 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 12.0 Release Notes, Network Advisor 12.0 User Guide, and Network Advisor 12.0 Installation, Migration, & Transition Guides.

Note:

Brocade Network Advisor 12.0 is required to manage switches running FOS 7.1 or later, and also to manage the Brocade 6520 platform.

DCFM Compatibility

DCFM is not qualified with and does not support the management of switches operating with FOS v7.0 and later firmware versions. **You must first upgrade DCFM to Network Advisor 12.0 if you are planning to upgrade devices to FOS v7.1.0 or later.**

WebTools Compatibility

FOS v7.1.0 is qualified and supported only with Oracle JRE 1.7.0 update 9.

SMI Compatibility

- It is important to note that host SMI-S agents cannot be used to manage switches running FOS v7.1.0

  If users want to manage a switch running FOS v7.1.0 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	
Brocade 2000-series switches	Not supported, end of support (December 2007)
Brocade 3200, 3800	Direct E-port connections are not supported – must use FCR
Brocade 3000	Direct E-port connections are not supported – must use FCR v3.2.1c [3]
Silkworm 3016, 3250, 3850, 3900, 24000	Direct E-port connections are not supported – must use FCR
4100, 4900, 7500, 7500e, 5000, 200E, 48K Brocade 4012, 4016, 4018, 4020, 4024, 4424	v6.2.2 or later[6]
Silkworm 12000	v5.0.x [3] (Direct E_Port connections are not supported – must use FCR)
Brocade 5410, 5480, 5424, 5450, 5460, 5470, NC-5480	v6.2.0 or later[6]
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	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

Supported Products and FOS Interoperability	
Brocade 6505	FOS v7.0.1 or later
Brocade 6520	FOS v7.1 or later
48000 with FA4-18 blade(s), Brocade 7600	V6.2.2 or later [6]
Secure Fabric OS (on any model)	Not Supported
Mi10k, M6140, ED-6064, ES-3232, ES-4300, ES-4400, ES-4500, ES-4700 (McDATA Fabric Mode and Open Fabric Mode) [1]	Direct E_Port connections are not supported – must use FCR running pre-FOS v7.1. M-EOS v9.9.5 or later
McDATA ED-5000 32-port FC director	Not Supported

Multi-Protocol Router Interoperability	
Brocade 7420	Not supported
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.

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.

Blade Support

Fabric OS v7.1.0 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.
Intelligent blade	Up to a total of 8/4 intelligent blades. See below for maximum supported limits of each blade.
6 port 10G FC blade (FC10-6)	Not supported on FOS v7.1 or later
FCIP/FC Router blade (FR4-18i)	Not supported on FOS v7.1 or later
Virtualization/Application Blade (FA4-18)	Not supported on FOS v7.0 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. **Note:** FR4-18i cannot coexist with FX8-24 in FOS v7.0 or later
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	Not supported

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

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

Fabric OS v7.1 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	Supported starting with FOS v7.0
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 Condor3 based 8G blades	Supported starting with FOS v7.0.1[1]
FC10-6	Not supported.
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 maximum of 4 blades of this type.
FCoE/L2 CEE blade FCOE10-24	Not supported

Table 2 Blade Support Matrix for DCX 8510-8 and DCX 8510-4 with FOS v7.1

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[2]	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	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	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	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)	FC16-32, FC16-48, FX8-24, FS8-18 (Two intelligent blades and maximum of four slots populated with FC16-xx/FC8-xxE blades)	Port / Intelligent Blade	4 Power Supplies	2 Power Supplies	200-240VAC: 1+1 Power Supplies 110VAC: 2+2[1] Power Supplies
192 8Gb Ports & max 2 intelligent blades (FX8-24 /FS8-18/ combination)	FC8-32E, FC8-48E, FX8-24, FS8-18 (Two intelligent blades and maximum of four slots populated with FC16-xx/FC8-xxE blades)	Port / Intelligent Blade	4 Power Supplies	2 Power Supplies	200-240VAC: 1+1 Power Supplies 110VAC: 2+2[1] Power Supplies
336 16Gb ports	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

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[2]	Blades	Type of Blade	DCX 8510-8 @110 VAC (Redundant configurations)	DCX 8510-8 @200-240 VAC (Redundant configurations)	Comments
336 8Gb ports	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
384 16Gb ports	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	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	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 (Defect 000349586), which will prevent Fabric Watch from generating notifications when the switch enters the marginal state due to missing power supplies

2. The power draw of ICL ports is taken into account and does not change the listed PS requirements

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[1]	Blades	Type of Blade	DCX 8510-4 @110 VAC (Redundant configurations)	DCX 8510-4 @200-240 VAC (Redundant configurations)	Comments
96 ports max	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	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

1. The power draw of ICL ports is taken into account and does not change the listed PS requirements

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.

Access Gateway

- AG cascading is not supported on Brocade 6510 or Brocade 6505.

- 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:

  o Log in to http://my.brocade.com

- o   Go to Documentation > Tech Notes.

- o   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.

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 FOS v7.0.1 or later.
    - Use of SSKM with the Brocade encryption solution is only supported for SSKM operating in PVM mode. Please see SSKM documentation for operating in PVM mode for details. Operation in HVM mode is not supported.
    - It is recommended to use Tight VNC connection to access the management console for SSKM and LKM key vaults instead of remote desktop. If remote desktop is used, customer may encounter the following errors related to smart card reader:
        - Error communicating with smart card reader.
        - Card reader already in use by default key.
        - Unable to complete TEP/TAP process as window for selecting card and entering password does not appear.
    - Please refer to SafeNet Keysecure install documentation for setting up and initially configuring the SSKM key vaults. There are some changes between setting up the SSKMs and the LKMs. Please refer SafeNet or NetApp documentation for any LKM to SSKM migration procedures. This migration is not tested/supported with FOS v7.0.1 or later.
    - The following is tested and supported with FOS v7.0.1 or later
        - Platform Serial Number: 27CJNQ1
        - Platform FW Version: SSKM-1.0-03
        - Platform Firmware Build ID: 0.5_secure
        - DB version: 166
        - SEP FW ID: SEPLuna TDB
        - SEP HW ID: Luna K6 TBD
        - SEP SW ID: 6.2.0 TBD
        - System Card FW ID: 200.5
        - Management console version: 1.0 build 18.
- 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.

- If the migration to FOS v7.0 or later does not occur from 6.4.1a, 6.4.1b, or 6.4.2, the following will result

    - BES will reboot if auto reboot is enabled otherwise it needs to be rebooted manually for recovery2010/11/08-04:54:35:485488, [FSS-1009], 4424/886, CHASSIS, ERROR, MACE, FSS Error: fcsw0-vs: MISMATCH: component., svc.c, line: 2462, comp:FSSK_TH, ltime:2010/11/08-04:54:35:485484

- 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.

- When host clusters are deployed in an Encryption environment, please note the following recommendations:

    - If two EEs (encryption engines) are part of a HAC (High Availability Cluster), configure the host/target pair such that they form a multipath from both EEs. Avoid connecting both the host/target pairs to the same EE. This connectivity does not give full redundancy in the case of EE failure resulting in HAC failover.

    - Since quorum disk plays a vital role in keeping the cluster in sync, please configure the quorum disk to be outside of the encryption environment.

- The "–key_lifespan" option has no effect for "cryptocfg –add –LUN", and only has an effect for "cryptocfg --create –tapepool" for tape pools declared "-encryption_format native". For all other encryption cases, a new key is generated each time a medium is rewound and block zero is written or overwritten. For the same reason, the "Key Life" field in the output of "cryptocfg --show -container -all –stat" should always be ignored, and the "Key life" field in "cryptocfg --show –tapepool –cfg" is only significant for native-encrypted pools.

- The Quorum Authentication feature requires a compatible DCFM or Brocade Network Advisor release (DCFM 10.3 or later for pre-FOS v7.0 and Network Advisor 11.1 or later for FOS v7.0 or later) that supports this feature. Note, all nodes in the EG must be running FOS v6.3.0 or later for quorum authentication to be properly supported.

- The System Card feature requires a compatible DCFM or Brocade Network Advisor release (DCFM 10.3 or later for pre-FOS v7.0 and Network Advisor 11.1 or later for FOS v7.0 or later) that supports this feature. Note, all nodes in the EG must be running FOS v6.3.0 or later for system verification to be properly supported.

- 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.

- HP SKM & ESKM are supported with Multiple Nodes and Dual SKM/ESKM Key Vaults. Two-way certificate exchange is supported. Please refer to the Encryption Admin Guide for configuration information. If using dual SKMs or ESKMs on BES/FS8-18 Encryption Group, then these SKM / ESKM Appliances must be clustered. Failure to cluster will result in key creation failure. Otherwise, register only one SKM / ESKM on the BES/FS8-18 Encryption Group.

- FOS 7.1.0 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 versions (6.4.x/7.0.x) to FOS 7.1.0 and downgrade from FOS 7.1.0 to FOS versions (6.4.x/7.0.x) would require regeneration and re-registration of CA and signed KAC certificates to restore connectivity to the key vault. Please refer to Encryption AG 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 versions (6.4.x/7.0.x) to FOS7.1.0, 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 AG 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 v6.4.1a to FOS v7.0 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 following key vault types: ESKM, TEKA, TKLM and KMIP. To use disk device decommissioning feature for these KVs, all the nodes in the encryption group must be running FOS v7.1.0 or later. Firmware downgrade will be prevented from FOS v7.1.0 to a lower version if this feature is in use. Disk Device decommissioning for DPM and LKM key vaults will continue to work as with previous firmware versions.

- FOS7.1.0 introduces a new KMIP keyvault type for Safenet KeySecure SW v6.1 KMIP server. Firmware downgrade will be prevented from FOS v7.1.0 to a lower version if key vault type is set to KMIP. Please refer to the KMIP Encryption Admin Guide for more details.

- FOS 7.1.0 mandates regular zones for Hosts and Targets must be defined in the effective configuration before adding an initiator into a crypto container. If crypto commit operation is performed without regular zones for Host and Target, frame redirection zones will not be created. Hosts and targets must be zoned together by worldwide port name (WWPN) rather than worldwide node name (WWNN) in configurations where frame redirection will be used

- In FOS 7.1.0 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.

- Special Notes for HP Data Protector backup/restore application

  - Tape Pool encryption policy specification:

    - On Windows Systems, HP Data Protector can be used with tape pool encryption specification only if the following pool label options are used:

      - Pick from Barcode
      - User Supplied – Only 9 characters or less

    For other options, behavior defaults to Tape LUN encryption policy.

    - On HP-UX systems, HP Data Protector cannot be used with tape pool encryption specification for any of the pool options. The behavior defaults to Tape LUN Encryption Policy.

  - Tape LUN encryption policy specification:

    - No restrictions, tape LUN encryption policy specification can be used with HP Data Protector on HP-UX and Windows systems.

- 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 and therefore VMFS5 with ATS is not supported. It is recommended to use VMFS3.

FCIP (Brocade 7800 and FX8-24)

- Any firmware activation will disrupt I/O traffic on FCIP links.

- Latency measurements supported on FCIP Tunnels:

    o 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 v7.0.0 or later, if any of the following features are enabled in the FCIP configuration, a downgrade operation to pre-FOS v7.0.0 will be blocked until the features are removed from the FCIP configuration:

    o InBand Management

    o Multigigabit Circuit

    o Shared GE among Logical Switches

    o Auto-mode compression option

    o VE as XISL

    o 10GigE lossless failover

    o Modified QoS percentages

    o 10GigE ARL

    o IP Configuration where multiple GigEs have same subnet values

    o For a tunnel configuration on 1GE ports that has more than 4 circuits

    o Teradata emulation enabled

    o Circuits configured explicitly to be listeners or an initiators

FCoE/DCB/CEE (Brocade 8000 and FCOE10-24)

- When upgrading a Brocade 8000 or 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.

- FOS v7.0 or later supports a new optimized model for provisioning FCoE with fewer configuration steps to enable FCoE on DCB ports. These changes do not allow the Brocade 8000 to retain FCoE configuration information following an upgrade to FOS v7.0 or later. After the upgrade to FOS v7.0 or later, all FCoE edge ports will need to be provisioned with the new model before any FIP FLOGIs will take place

- Although including Brocade 8000 in the path of TI (Traffic Isolation) and ETI (Enhanced Traffic Isolation) Zones is not prohibited, it is not supported. Configuring Brocade 8000 in the TI/ETI Zone path is not recommended and will result in undefined behavior.

- Ethernet L2 traffic with xSTP Hello timer set to less than or equal to 3 seconds may experience momentary traffic disruption during HA failover.

- The Brocade 8000 balances the FCoE bandwidth across all six port groups (each port group contains four ports). To get optimum performance for FCoE traffic it is recommended that the user distribute server CNA connections across these six port groups.

- 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 Brocade 8000/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 Brocade 8000 and 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.

- The Brocade 8000 does not support non-disruptive hot code loads (HCL). Upgrading the Brocade 8000 to FOS v7.1 or downgrading from v7.1 is disruptive to the IO through the switch.

- 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.

- Connecting Brocade 8000 to an FCR-capable switch with fcrbcast config enabled will cause a storm of broadcast traffic resulting in termination of iswitchd.

- 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 Brocade 8000 and FCOE10-24 can handle 169 small FCoE frames in bursts. If you are using the Brocade 8000 or 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.

- To allow Hot Code Load on Brocade 5100 when using Integrated Routing, the edge switch connected to the 5100 must be running Fabric OS v6.1 or later code.

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 when using active DWDM links. Hence FEC must be disabled on Condor3 ports when using active DWDM links by using portCfgFec command. Failure to disable FEC on active DWDM links may result in link failure during port bring up.

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.

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.

Licensing

- The new Fabric Vision license is being introduced as part of some software bundles and that it enables new functionality being introduced in FOS v7.2. When installed on a switch operating with FOS v7.1.x, the licenseshow command will display this as the "Fabric Insight license," and it does not enable or affect any functionality on the switch.

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 does not support EX port configuration in Interopmode 2 or Interopmode 3.

- Device sharing between a switch running FOS v7.1 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.

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 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

- **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.

Defects

Closed with Code Change in Fabric OS v7.1.1

This section lists the defects with Critical, High and Medium Technical Severity closed with a code change as of May 30, 2013 in Fabric OS v7.1.1.

Defect ID: DEFECT000404322	Technical Severity: Medium
Summary: Spinfab does not attain saturation of 3.2G throughput over long distance E-port due to reduced size frames	
Symptom: Expected throughput of 3.2G for Long Distance E-Port is not obtained during spinfab test using 16G LWL 10km SFP	
Risk of Fix: Low	
Feature: Diagnostics	Function: Other
Reported In Release: FOS7.0.2	

Defect ID: DEFECT000405095	Technical Severity: Medium
Summary: thconfig not supporting timebase option none for class SFP with SFPTYPE as 16G,10G,QSFP	
Symptom: When set timebase option for class SFP, area PWRONHRS to none, customer gets an error : "Timebase not supported by this class"	
Risk of Fix: Low	Probability: High
Feature: FOS Software	Function: Fabric Services
Reported In Release: FOS7.0.1	Service Request ID: 741483,741497

Defect ID: DEFECT000408703	Technical Severity: Medium
Summary: Updated default serdes value for FC8-48 and new value is effective after hafailover.	
Symptom: CRC with Good EOF Errors detected on Slot 1 port 2 of DCX-4S with FC8-48 installed in Slot 1	
Risk of Fix: Low	
Feature: 8G ASIC Driver	Function: C2 ASIC driver
Reported In Release: FOS6.4.2	Service Request ID: 736755

Defect ID: DEFECT000410381	Technical Severity: Medium
Summary: RPC entries need to be removed from IP filter	
Symptom: ipfilter --show continues to display RPC ports	
Risk of Fix: Low	Probability: High
Feature: FOS Software	Function: Management Embedded
Reported In Release: FOS7.0.0	Service Request ID: 753121,649971,696577

Defect ID: DEFECT000420051	Technical Severity: Medium
Summary: On DCX with FC8-48 in slot 3, CRC with good eof errors are seen.	
Symptom: CRC with good EOF onbserved on DCX with FC8-48 in slot 3 on ports 3/42 <-> 8/139	
Risk of Fix: Medium	Probability: Medium
Feature: FOS Software	Function: System Performance
Reported In Release: FOS6.4.3	Service Request ID: 1035482

Defect ID: DEFECT000420473	Technical Severity: Medium
Summary: HTTP TRACE requests are processed over HTTPS/SSL connections	
Symptom: http trace/track methods are allowed on secure connections.	
Risk of Fix: Low	Probability: Low
Feature: FOS Software	Function: Management Embedded
Reported In Release: FOS7.0.0_pha	Service Request ID: ,1133738

Defect ID: DEFECT000421461	Technical Severity: Medium
Summary: On DCX-4S, backend CRC errors detected on core blade port 3/56 connecting FC8-32 port blade.	
Symptom: RASLog message C2-5825 "Detect CRC error with good EOF" displayed.	
Risk of Fix: Low	Probability: Medium
Feature: FOS Software	Function: OS: Configuration
Reported In Release: FOS6.4.2	Service Request ID: 1035401

Defect ID: DEFECT000421879	Technical Severity: Medium
Summary: When an access control list is configured for SNMP and the list contains a subnet area, that particular subnet will not be able to query the switch	
Symptom: Not able to query SNMP from host on defined access host subnet area.	
Workaround: Yes	
Risk of Fix: Low	Probability: Medium
Feature: FOS Software	Function: SNMP
Reported In Release: FOS7.0.1	Service Request ID: 1087061

Defect ID: DEFECT000422477	Technical Severity: High
Summary: Unstable ICL/other ports can cause switch reboot	
Symptom: This defect has implication on DCX, FX8-24 etc., with unstable ICL/BI ports, it can cause switch to panic.	
Risk of Fix: Low	Probability: Medium
Feature: FOS Software	Function: ASIC Driver
Reported In Release: FOS7.0.2	Service Request ID: 1032557

Defect ID: DEFECT000423875	Technical Severity: Medium
Summary: Race condition during SNMP query of interface statistics caused BR8000 switch to panic.	
Symptom: B8000 switch experienced nsm panic and subsequent switch reboot	
Risk of Fix: Low	Probability: Low
Feature: CEE-Protocol	Function: NSM
Reported In Release: FOS6.4.2	Service Request ID: 1094688,1143458

Defect ID: DEFECT000425570	Technical Severity: Medium
Summary: FabricWatch trap 5 is not sending to 3rd party tool in FOS v7.0.1	
Symptom: Customer is unable to capture fabric watch trap(Specific-trap: 5) using 3rd party tool with FOS v7.0.1, but FOS v6.4.2x was able to capture. Raslog and email communication are able to receive these traps.	
Risk of Fix: Low	Probability: High
Feature: FOS Software	Function: Fabric Services
Reported In Release: FOS7.0.1	Service Request ID: 1098326,1122983

Defect ID: DEFECT000427535	Technical Severity: Medium
Summary: After setting a low threshold for SFP temperature on BR6505, The temperature is shown as above instead of Below.	
Symptom: After a custom setting for SFP temperature of HIGH =85 and Low - 75, even if the temperature is below 75, it is shown as above and not below.	
Risk of Fix: Low	
Feature: FOS Software	Function: EM / Hil / Sysctrl
Reported In Release: FOS7.0.2	Service Request ID: 1103272

Defect ID: DEFECT000428368	Technical Severity: Medium
Summary: turboramtest output is differenet dependent on switch platform	
Symptom: Inconsistent output from turboramtest on BR8510 and BR6510	
Risk of Fix: Low	**Probability:** Low
Feature: Diagnostics	**Function:** Other
Reported In Release: FOS7.0.2	**Service Request ID:** 1102971

Defect ID: DEFECT000428605	Technical Severity: Medium
Summary: Enhance to allow FPGA upgrade on FS8-18 and BES.	
Symptom: Cannot upgrade FPGA image sperately from FOS on FS8-18 and BES	
Risk of Fix: Low	**Probability:** Low
Feature: Data Security	**Function:** Platform
Reported In Release: FOS7.0.2	

Defect ID: DEFECT000428780	Technical Severity: High
Summary: When running full bandwidth bi-directional traffic in recommended 16G ICL topology configuration, some traffic flows may experience a performance throughput degradation.	
Symptom: Observed performance throughput degradation for some ICL traffic flows in a 8 flow ICL topology.	
Risk of Fix: Low	**Probability:** Medium
Feature: 16G ASIC Driver	**Function:** Routing
Reported In Release: FOS7.1.0	

Defect ID: DEFECT000429115	Technical Severity: High
Summary: After diag test, switch route table (RTE) is not being updated properly.	
Symptom: LUN disappeared after "portloopbacktest" and "turboramtest" diagnostic tests were performed on single chip low port count pizza box switches such as BR5100, 4100, 5000, 300 and embedded switches.	
Workaround: cold reboot	
Risk of Fix: Low	**Probability:** High
Feature: 16G Platform Services	**Function:** FOS Kernel Drivers
Reported In Release: FOS7.1.0_blv	

Defect ID: DEFECT000429695	Technical Severity: High
Summary: Name Server loses FC4 type in routed environment.	
Symptom: Some hosts that make FC-4 type based Name Server queries won't be able to establish paths to storage.	
Risk of Fix: Low	**Probability:** High
Feature: 8G FCR	**Function:** FCR Daemon
Reported In Release: FOS7.0.1	**Service Request ID:** 1102900,1123307

Defect ID: DEFECT000429712	Technical Severity: Medium
Summary: BR5100 does not transmit SNMP trap as chassis instance after user configured sysmonitor.	
Symptom: SNMP trap and errdump indicates error with FID:128 even though sysmonitor is a chassis-wide command.	
Risk of Fix: Low	**Probability:** Medium
Feature: Mgmt Embedded - SNMP	**Function:** Other
Reported In Release: FOS7.0.2	**Service Request ID:** 1106710

Defect ID: DEFECT000429815	Technical Severity: High
Summary: 5480 switch under management by BNA exhibits snmpd crash and switch reboot	
Symptom: 5480 switches running in AG mode and managed by BNA exhibit snmpd crash and switch reboot.	
Workaround: avoid manaing the AG switch by BNA or have all ports connected to either N_Port or F_port or have AG in auto policy disabled state.	
Risk of Fix: Low	**Probability:** High
Feature: FOS Software	**Function:** Management Services
Reported In Release: FOS6.4.2	**Service Request ID:** 1102791

Defect ID: DEFECT000430083	Technical Severity: Medium
Summary: Unable to delete user account in VF environment created using AD settings	
Symptom: After modifying a user account with "userconfig --addad lsadmin -a 1-128" command, deleting the user account fails with the following error message: "Cannot manage the target account due to conflicting LF permissions"	
Risk of Fix: Low	**Probability:** Medium
Feature: FOS Software	**Function:** Fabric Services
Reported In Release: FOS7.0.2	**Service Request ID:** 1092980

Defect ID: DEFECT000431095	Technical Severity: High
Summary: diagshow command in interactive mode hangs and leads to high CPU utilization when telnet session is killed	
Symptom: High CPU utilization when telnet session with diagshow command in interactive mode is killed	
Risk of Fix: Low	**Probability:** Low
Feature: FOS Software	**Function:** Diagnostics
Reported In Release: FOS6.4.2	**Service Request ID:** 1104381

Defect ID: DEFECT000431101	Technical Severity: Medium
Summary: Fibre Channel loop even is not completed when disk is removed from Loop storage connected to Brocade 300	
Symptom: When pull out a disk from a 3rd party vendor storage, access to the whole storage is lost.	
Workaround: Bounce port by portdisable and portenable.	
Risk of Fix: Low	**Probability:** Low
Feature: 8G ASIC Driver	**Function:** C2 ASIC driver
Reported In Release: FOS7.0.0	**Service Request ID:** 1106546

Defect ID: DEFECT000431369	Technical Severity: High
Summary: Brocade switch mib browser displays misinterperated fcportflag	
Symptom: Mib browser displays ascii-hex of populated fcportflag value such as 30 for 0 and 31 for 1. But expected value is 0 and 1.	
Risk of Fix: Low	**Probability:** High
Feature: FOS Software	**Function:** SNMP
Reported In Release: FOS7.0.2	**Service Request ID:** 1106614

Defect ID: DEFECT000431529	Technical Severity: High
Summary: Restore job failing after partial restore.	
Symptom: Restore job runs up to a point and then tries to access the first dirve the restore started with. Host is getting incorrect block and the job is terminating.	
Workaround: Disable FCIP Open Systems Tape Pipelining	
Risk of Fix: Low	**Probability:** Low
Feature: FCIP	**Function:** Emulation
Reported In Release: FOS7.0.0	**Service Request ID:** 1110201

Defect ID: DEFECT000431920	Technical Severity: High
Summary: Support the documneted BRCD-FCIP-Ext MIB in MIB reference.	

Symptom: User will always see 0 for the below measures
        fcipExtendedLinkTcpDroppedPackets
        fcipExtendedLinkTcpSmoothedRTT
        fcipExtendedLinkRtxRtxTO
        fcipExtendedLinkRtxDupAck
        fcipExtendedLinkDupAck	

Risk of Fix: Low	Probability: High
Feature: Port Statistics	Function: Other
Reported In Release: FOS7.0.1	

Defect ID: DEFECT000432470	Technical Severity: High
Summary: Standby CP panics every time two port blades are moved into a new logical switch	
Symptom: On a switch with devices neither cut light nor come on line, using lscfg to move ports around logical switch, standby CP could panic.	
Risk of Fix: Low	Probability: Low
Feature: 16G Platform Services	Function: FOS Kernel Drivers
Reported In Release: FOS7.1.0	

Defect ID: DEFECT000432514	Technical Severity: Medium
Summary: FC8-64 port blade installed in 8510 incorrectly faults during POST after powercycle	
Symptom: FC8-64 port blade incorrectly faults (51) during POST. A slotpoweroff/on or reboot clears the condition.	
Risk of Fix: Low	
Feature: Diagnostics	Function: Post Diags
Reported In Release: FOS7.0.1	Service Request ID: EMC TL 8058

Defect ID: DEFECT000432654	Technical Severity: High
Summary: Setting strict mode with DCC policy from disabled switch can cause dual CP panic	
Symptom: When having a DCC policy of a disabled switch and then setting strict mode on the fabric may cause a verify error that results in a dual CP panic.	
Workaround: Found the misconfigured DCC policy, remove that particular DCC Policy and use the fabric.	
Risk of Fix: Low	Probability: Medium
Feature: FOS Security	Function: ACL
Reported In Release: FOS7.1.0	

Defect ID: DEFECT000433313	Technical Severity: Medium
Summary: CP Faulty reason is not persistent over a reboort	
Symptom: CP which is indicating Faulty(53) - Possible RRD does not persist the failing reason over a reboort	
Risk of Fix: Low	Probability: Low
Feature: System Controls/EM	Function: Infrastructure
Reported In Release: FOS7.1.0	

Defect ID: DEFECT000433562	Technical Severity: Medium
Summary: For all 16G platforms and FC8-32E/FC8-48E blades, error message is shown when Web Tools port admin wizard is used to configure long distance with VC_Link INIT set to Arbitrary(1)	
Symptom: An error message is displayed when trying to configure long distance in the Web Tools port configuration wizard "Valid configurations are :vc_translation_link_init=0, fillword = IDLE_IDLE or vc_translation_link_init=1, fillword = ARB_ARB,IDLE_ARB,AA_THEN_IA"	
Risk of Fix: Low	**Probability:** Medium
Feature: WebMgmt	**Function:** Ports Admin
Reported In Release: FOS7.1.0	

Defect ID: DEFECT000433644	Technical Severity: High
Summary: 8510-8 in reboot loop with POST failing for all 16G blades where the default FID of the default switch was changed to something other than 128	
Symptom: After a physical power failure, DCX8510-8 went into a reboot loop with all 16G port baldes failing POST.	
Risk of Fix: Low	**Probability:** Medium
Feature: Diagnostics	**Function:** Post Diags
Reported In Release: FOS7.1.0	

Defect ID: DEFECT000433727	Technical Severity: High
Summary: Logical Fabric Addressing Modes unexpectly modified	
Symptom: Logical Fabric Addressing Modes: Once customer configures for mode 1 or 2, can never go back to mode 0.	
Risk of Fix: Low	**Probability:** Medium
Feature: 16G Platform Services	**Function:** Partition Management
Reported In Release: FOS7.1.0	

Defect ID: DEFECT000433865	Technical Severity: High
Summary: 7800 panics when host writes data to tape drive via FCIP tunnel with fastwrite and tape pipelining enabled	
Symptom: Write I/Os failed after a few write I/Os were completed, 7800 panics.	
Workaround: Disable FCIP Fastwrite and tape pipelining	
Risk of Fix: Low	**Probability:** Medium
Feature: FOS Software	**Function:** FCIP
Reported In Release: FOS7.0.1	**Service Request ID:** 1118991

Defect ID: DEFECT000434032	Technical Severity: Medium
Summary: Remote mirroring is not working when fastwrite is enabled	
Symptom: Replication may fail when fastwrite is enabled.	
Workaround: Disable FCIP Fastwrite on the tunnel.	
Risk of Fix: Low	**Probability:** Medium
Feature: FCIP	**Function:** Emulation
Reported In Release: FOS7.0.0	**Service Request ID:** 1117702

Defect ID: DEFECT000434293	Technical Severity: High
Summary: HTTP status queried from BNA returned as FAILED even for Successfully download in Device	
Symptom: FirmwareDownload finished successfully in device but HTTP status returned as FAILED to BNA	
Risk of Fix: Low	
Feature: Mgmt Embedded - CAL	**Function:** Other
Reported In Release: FOS7.1.0	

Defect ID: DEFECT000434819	Technical Severity: Medium
Summary: Continuous decrease in free memory on blade processor when polling container stat every 30 seconds	
Symptom: Continuous decrease in free memory is observed on blade processor when polling container stat every 30 seconds.	
Workaround: rebooting lance blade or mace	
Risk of Fix: Low	**Probability:** Medium
Feature: Data Security	**Function:** Disk Encryption
Reported In Release: FOS7.0.2	**Service Request ID:** 1102253

Defect ID: DEFECT000435074	Technical Severity: High
Summary: FX8-24 blade DP panics with FCIP tape pipelining enabled	
Symptom: FCIP tunnels go down and become not available.	
Workaround: Disable FCIP Open Systems Tape Pipelining	
Risk of Fix: Low	**Probability:** Medium
Feature: FOS Software	**Function:** FCIP
Reported In Release: FOS7.0.1	**Service Request ID:** 1123356

Defect ID: DEFECT000435397	Technical Severity: Medium
Summary: IPv6 links are not presented in Fabric Tree when connecting to switch via IPv6	
Symptom: When connecting to a switch configured with both IPv4 and IPv6 addresses from a host configured with only IPv6, the links within the "Fabric Tree" for remote switches are presented only as IPv4. Also, in the "Switch Information" it will not display any IPv6 information.	
Risk of Fix: Low	**Probability:** High
Feature: FOS Software	**Function:** Management Embedded
Reported In Release: FOS7.0.2	**Service Request ID:** 1122346

Defect ID: DEFECT000435414	Technical Severity: Medium
Summary: Error log content is getting cleared of prior messages when migrating to FOS 7.1.0	
Symptom: After successful firmwaredownload upgrade to FOS 7.1.0, errdump results will not include any messages that were in the error log prior to the firmwaredownload. Only the latest messages appear.	
Workaround: No workaround however supportsave can be used to save and retain error log contents if the supportsave is successfully executed prior to the firmwaredownload upgrade to FOS 7.1.0.	
Risk of Fix: Low	**Probability:** Medium
Feature: FIRMWARE DOWNLOAD	**Function:** Firmware Download
Reported In Release: FOS7.1.0	**Service Request ID:** 1124793/P1124623

Defect ID: DEFECT000435619	Technical Severity: Medium
Summary: Webtool Search function errors.	
Symptom: Webtool search function of 'Switch Throughput Utilization' could not search trunk port, also after a user did search of a port once, the same port could not be searched again.	
Risk of Fix: Low	**Probability:** High
Feature: FOS Software	**Function:** Web Management
Reported In Release: FOS7.0.2	**Service Request ID:** 1118431

Defect ID: DEFECT000435983	Technical Severity: High
Summary: A negative value is displayed for the number of host side paths in command display	
Symptom: Portshow xtun <slot/>vePort -ficon -stats output displays a negative for the number of FICON Host side Paths.	
Workaround: Disable FCIP FICON Tape Pipelining or XRC emulation	
Risk of Fix: Low	**Probability:** Medium
Feature: FCIP	**Function:** Emulation
Reported In Release: FOS7.0.0	**Service Request ID:** 11112161

Defect ID: DEFECT000436215	Technical Severity: Medium
Summary: The thconfig command will not properly monitor a port that has SFP swapped from 8G to 16G	
Symptom: The thconfig command incorrectly reports the state of a port that has SFP swapped from 8G to 16G is Above range.	
Risk of Fix: Medium	Probability: High
Feature: FOS Software	Function: Fabric Services
Reported In Release: FOS7.0.2	Service Request ID: 1116355

Defect ID: DEFECT000436879	Technical Severity: Medium
Summary: thconfig -sfptype configuration gets applied without running --apply option	
Symptom: With 16GSWL SFP, the custom configuration gets applied as soon as the custom value is manually changed by --set option before --apply option. 8G SFP does not show that problem.	
Risk of Fix: Low	Probability: Medium
Feature: FABRIC WATCH	Function: Performance Monitor
Reported In Release: FOS7.0.2	Service Request ID: 1125131

Defect ID: DEFECT000437078	Technical Severity: High
Summary: Incompatible FDMI attribute between different FOS releases caused kernel panic	
Symptom: In a mixed FOS fabric with FOS v6.4.x and FOS v7.1, switch running v7.1.0 could panic when there are FDMI queries.	
Workaround: Do not use pre-v7.0 switches as BNA seed switch.	
Risk of Fix: Low	Probability: Low
Feature: FC Services	Function: FDMI
Reported In Release: FOS7.1.0	

Defect ID: DEFECT000437186	Technical Severity: Medium
Summary: On trunk master EX-port disable, parameters are copied from the old master port to the neighbor pwwn	
Symptom: On trunk master EX-port disable, all the parameters from the old master port are erroneously copied the neighbor pwwn.	
Workaround: Need to disable and enable the invalid port	
Risk of Fix: Low	Probability: High
Feature: 8G FCR	Function: FCR Daemon
Reported In Release: FOS7.1.0	

Defect ID: DEFECT000437463	Technical Severity: High
Summary: #rd party device failing writes to tape drives when appending	
Symptom: IO Errors when tape jobs are started against a newly installed tape Drive: An I/O error occurred while accessing drive xxx (/dev/hmt_xxx) for RDBLKID operation, errno = 78, rc = 1.	
Workaround: Disable open systems tape pipelining or limit tunnel vtn to 1	
Risk of Fix: Low	Probability: Medium
Feature: FCIP	Function: Emulation
Reported In Release: FOS7.0.0	Service Request ID: 1108847

Defect ID: DEFECT000437467	Technical Severity: High
Summary: During LSAN activation, some event sequences can cause GE_PT query to fail	
Symptom: Hosts do not discover targets after LSAN zone activation.	
Workaround: Bounce any of the host ports and all targets are discovered by host.	
Risk of Fix: Low	**Probability:** Low
Feature: FC Services	**Function:** Zoning
Reported In Release: FOS7.1.0	

Defect ID: DEFECT000437555	Technical Severity: High
Summary: Sfpshow CLI does not provide data	
Symptom: Sfpshow CLI will show "Not Available" on some fields, and polling has not started: Temperature : Not Available Current : Not Available Voltage : Not Available RX Power : Not Available TX Power : Not Available Last poll time : Polling has not started	
Workaround: sfpshow -f	
Risk of Fix: Low	**Probability:** High
Feature: 16G Platform Services	**Function:** FOS Kernel Drivers
Reported In Release: FOS7.1.0	

Defect ID: DEFECT000437875	Technical Severity: High
Summary: Kernel Panic while attempting to correct ASIC memory Parity error.	
Symptom: Kernel Panic resulted in network outage on Brocade 8000	
Risk of Fix: Low	**Probability:** Low
Feature: FOS Software	**Function:** ASIC Driver
Reported In Release: FOS6.3.2	**Service Request ID:** 1128822

Defect ID: DEFECT000437958	Technical Severity: Medium
Summary: Remove excessive internal I2C reset raslog message	
Symptom: i2c reset message on recoverable errors causing unnecessary concerns	
Risk of Fix: Low	**Probability:** Low
Feature: 8G Platform Services	**Function:** Other
Reported In Release: FOS7.0.1	

Defect ID: DEFECT000438017	Technical Severity: Medium
Summary: SNMP configuration replication overwrites AAA LDAP Settings.	
Symptom: When trying to replicate SNMP settings alone from one switch to another switch using BNA, CLI, AAA settings also getting replaced.	
Risk of Fix: Low	**Probability:** High
Feature: FOS Software	**Function:** OS: Configuration
Reported In Release: FOS7.1.0	**Service Request ID:** FromPM

Defect ID: DEFECT000438388	Technical Severity: High
Summary: XTUN-1007 errors logged during systemverification tests on a DCX/8510 with an installed FX8-24 blade is installed	
Symptom: Message [XTUN-1007], 2114714, SLOT 6 | CHASSIS, ERROR, Brocade_DCX, FCIP FC frame drop due to truncated receive on slot=1 DP=2 BLS=0 DR=0 Frames Dropped=1068703 appears numerous times	
Risk of Fix: Low	**Probability:** Low
Feature: FCIP	**Function:** FCIP Port
Reported In Release: FOS7.1.0	**Service Request ID:** 1131027

Defect ID: DEFECT000438901	Technical Severity: High
Summary: kernel panic while running portcfgspeed command on internal port of an embedded switch.	
Symptom: BR5470 embedded switch panic'd while running portcfgspeed command, causing momentary outage.	
Risk of Fix: Low	**Probability:** Low
Feature: FOS Software	**Function:** ASIC Driver
Reported In Release: FOS6.4.2	**Service Request ID:** 1132056

Defect ID: DEFECT000439119	Technical Severity: Medium
Summary: Misleading (DPort + DWDM) instructions to "enable the port" to remove DWDM upon proper firmwaredownload failure.	
Symptom: Firmwaredownload is properly blocked but the instructions of "Portcfgdport --disable" command does not rectify the situation.	
Risk of Fix: Low	**Probability:** Medium
Feature: FIRMWARE DOWNLOAD	**Function:** FirmwareInstall
Reported In Release: FOS7.0.1	

Defect ID: DEFECT000439725	Technical Severity: High
Summary: The command IpAddrSet --delete is unsuccessful at removing an IPv6 switch address	
Symptom: Switch operations were not affected as the IPv6 address was not being used however, the IPv6 address could not be removed.	
Risk of Fix: Low	**Probability:** Low
Feature: OS Services	**Function:** IP Admin
Reported In Release: FOS7.1.0	

Defect ID: DEFECT000440137	Technical Severity: High
Summary: Update Serdes values for FC8-16 port blades in slot 1,2 of DCX-4s	
Symptom: Enhanced serdes tuning value to address CRC with good EOF	
Risk of Fix: Low	**Probability:** Low
Feature: FOS Software	**Function:** ASIC Driver
Reported In Release: FOS7.0.0	**Service Request ID:** 1131911

Defect ID: DEFECT000440420	Technical Severity: Medium
Summary: Power supply reports faulty(EM-1034) message on alternate power supplies in 6520 switches	
Symptom: Power supply faulty EM-1034 messages displayed on 6520 switches	
Risk of Fix: Low	**Probability:** Medium
Feature: System Controls/EM	**Function:** Other
Reported In Release: FOS7.1.0	**Service Request ID:** 1130981

Defect ID: DEFECT000440716	Technical Severity: High
Summary: TSM experiencing errors when OXID re-use is encountered and operation is dropped on PI side when FCIP OSTP is enabled.	
Symptom: Failed OSTP sequences and TSM Logs include the following types of errors: ANR8311E An I/O error occurred while accessing drive "driveName and mount point" for LOCATE or WRITE operation, errno = 5 or 16.	
Workaround: Disable FCIP Open Systems Tape Pipelining	
Risk of Fix: Low	**Probability:** Low
Feature: FCIP	**Function:** Emulation
Reported In Release: FOS7.0.0	**Service Request ID:** 1134539

Defect ID: DEFECT000440760	Technical Severity: High
Summary: FCIP 7800/FX8-24 DP panic when Ethernet jumbo frames are forwarded to the CP	
Symptom: Frequent core panics on DP.	
Workaround: Disable jumbo frame support in IP connected infrastructure where 7800/FX8-24 is connected	
Risk of Fix: Low	**Probability:** Medium
Feature: FCIP	**Function:** FCP TCP/IP Stack
Reported In Release: FOS7.0.2	**Service Request ID:** 1125980

Defect ID: DEFECT000440839	Technical Severity: High
Summary: Incorrect route removed when switching TIzone from failover-enabled to failover-disabled	
Symptom: Change a TIzone from failover enabled to disabled will cause traffic to stop and loose access to the targets.	
Risk of Fix: Low	**Probability:** Medium
Feature: FC Services	**Function:** Name Server
Reported In Release: FOS7.1.0	

Defect ID: DEFECT000440968	Technical Severity: High
Summary: Switch panic due to media pointer access failure.	
Symptom: Switch could panic if remove or power down FC and DCE blades during HAfailover.	
Risk of Fix: Low	**Probability:** Low
Feature: FOS Software	**Function:** Panic / OOM
Reported In Release: FOS6.4.2	**Service Request ID:** 1136223

Defect ID: DEFECT000440989	Technical Severity: High
Summary: Network Adivisor experiences out of memory error when obtaining or polling for encrypted LUN level info from two encryption groups that each have 4,000 defined LUNs	
Symptom: Network Advisor restarts after hitting an out of memory error.	
Workaround: rebooting lance blade or mace	
Risk of Fix: Low	**Probability:** Low
Feature: CEE-MANAGEABILITY	**Function:** CAL INTERFACE
Reported In Release: FOS7.1.0	**Service Request ID:** 1102253

Defect ID: DEFECT000440993	Technical Severity: Medium
Summary: Deskew value of last online port of a trunk group may be different	
Symptom: If FEC is enabled, the deskew value of the last online port of the trunk group may show a difference of up to 36.	
Risk of Fix: Low	**Probability:** Medium
Feature: 8G ASIC Driver	**Function:** ASIC Driver
Reported In Release: FOS7.1.0	

Defect ID: DEFECT000441306	Technical Severity: Medium
Summary: Firmwaredownload failed due to a missing or invalid firmware signature.	
Symptom: Firmwaredownload may fail with the message "missing or invalid firmware signature"	
Risk of Fix: Low	Probability: Medium
Feature: FOS-Infrastructure	Function: Firmware Download
Reported In Release: FOS7.0.1	

Defect ID: DEFECT000441913	Technical Severity: High
Summary: A 16Gbit switch may panic when an ICL port enters soft fault state. This is very unlikely but may also occur with Backend Internal or Backend External port.	
Symptom: During switch install, slot power cycle test, observed 16G switch panic.	
Risk of Fix: Low	Probability: Medium
Feature: 16G Platform Services	Function: FOS Kernel Drivers
Reported In Release: FOS7.0.2	Service Request ID: 1032557

Defect ID: DEFECT000441966	Technical Severity: High
Summary: Stale socket connection causes key retrival failure on encryption switches.	
Symptom: Key retrieval fails after Key vault connectivity errrors found	
Risk of Fix: Low	Probability: Low
Feature: Data Security	Function: Key Vault
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000442070	Technical Severity: Medium
Summary: When transfering a CSR using IPv6, the status message says failed when it actually succeded.	
Symptom: After a successful transfer of a CSR, the switch reports "Failed to export CSR to remote host:".	
Risk of Fix: Low	Probability: High
Feature: FOS Software	Function: Security
Reported In Release: FOS7.0.2	Service Request ID: 1137829

Defect ID: DEFECT000442080	Technical Severity: Medium
Summary: Making auto-tuned value persistent across reboot	
Symptom: Values from serds auto/manual tuning session are lost after poweroff/on blade or cold reboot of switch.	
Risk of Fix: Low	Probability: Low
Feature: 8G ASIC Driver	Function: C2 ASIC driver
Reported In Release: FOS7.0.2	

Defect ID: DEFECT000442112	Technical Severity: High
Summary: With OSTP enabled, 3rd party device write errors are encountered during backup processing	
Symptom: 3rd party device write errors during backup processing similar to: mm/dd/yy hh:mm:ss An I/O error occurred while accessing drive xxx (/dev/rmtyy) for WRITE operation, errno = 78, rc = 1.	
Workaround: Disable FCIP Open Systems Tape Pipelining	
Risk of Fix: Low	Probability: Medium
Feature: FCIP	Function: Emulation
Reported In Release: FOS7.0.0	Service Request ID: 1132526

Defect ID:	DEFECT000442422	Technical Severity:	High
Summary:	System security card is not being read on BES/FS8-18 card readers.		
Symptom:	Authentication for crypto operations on BES/FS8-24 fails. In this case, BES/FS8-24 functions as an ordinary FC switch or blade when it is powered up, but use of the encryption engine is denied as a result.		
Workaround:	Disable the systemcard feature, issue cryptocfg -- set -systemcard disable from the encryption group leader.		
Risk of Fix: Low		**Probability:** Medium	
Feature: FOS-Infrastructure		**Function:** Other	
Reported In Release: FOS7.1.0			

Defect ID:	DEFECT000442467	Technical Severity:	High
Summary:	Network Advisor initiated supportsave times out when collecting data		
Symptom:	Observed the following from the Network Advisor masterlog. "One or more modules timed out during supportsave. retry supportsave with -t option to collect all logs."		
Risk of Fix: Low		**Probability:** Medium	
Feature: Mgmt Embedded - CAL		**Function:** Other	
Reported In Release: FOS7.1.0			

Defect ID:	DEFECT000442919	Technical Severity:	Medium
Summary:	Switch panic while plugging in cables to ISL ports with one of the trunk port.		
Symptom:	Switch panics in RTE route module and hafailover. It occurred once just at the same time as customer was plugging in cables to ISL port of a trunk and it was not reproducible.		
Risk of Fix: Low		**Probability:** Low	
Feature: 4G Platform Services		**Function:** FOS Kernel Drivers	
Reported In Release: FOS6.4.2		**Service Request ID:** 1140381	

Defect ID:	DEFECT000443541	Technical Severity:	Medium
Summary:	Continuous FSS-1001 messages after firmware upgrade from FOR v6.4.2a to v6.4.3c		
Symptom:	Continuous FSS-1001 messages after firmware upgrade due to inconsistent Access Gateway State Synchronization		
Risk of Fix: Low		**Probability:** Low	
Feature: FOS Software		**Function:** High Availability	
Reported In Release: FOS6.4.3		**Service Request ID:** 1143366	

Defect ID:	DEFECT000444029	Technical Severity:	Medium
Summary:	FICON aborts during FCIP read emulation while running VTS		
Symptom:	Aborts during read emulation while running IBM VTS.		
Workaround:	Disable all FCIP FICON Tape Emulation Features.		
Risk of Fix: Low		**Probability:** Medium	
Feature: FCIP		**Function:** Emulation	
Reported In Release: FOS6.4.2		**Service Request ID:** 1143795	

Defect ID:	DEFECT000444171	Technical Severity:	High
Summary:	Data buffer is too small for holding frames header in error condition		
Symptom:	Kernel panic on BR8000 switch with FCOE when sending several iterations of maximum number of FDISCs continually.		
Risk of Fix: Low		**Probability:** Low	
Feature: CEE-FCOE		**Function:** FCOE DRIVER	
Reported In Release: FOS6.4.3		**Service Request ID:** 1111262	

Defect ID: DEFECT000444288	Technical Severity: Medium
Summary: Generate an alert if timeout frame discards and congestion are detected at the same time	
Symptom: No bottleneck alert is generated even if frames are already being discarded due to timeout.	
Risk of Fix: Medium	Probability: High
Feature: Bottleneck detection	Function: Other
Reported In Release: FOS7.1.0	

Defect ID: DEFECT000445644	Technical Severity: High
Summary: BES went into low memory state because of "Continuous polling from BNA"	
Symptom: BES CLI Commands are failing - Operation failed: BES/FS8-18 blade is not present or up	
Risk of Fix: Low	Probability: Medium
Feature: FOS Software	Function: Encryption
Reported In Release: FOS7.0.2	Service Request ID: 1145987

Defect ID: DEFECT000445729	Technical Severity: High
Summary: QSFP LED state inconsistent with port state on the 4 channels (ports)	

Symptom: Two sympthoms observed:
   1. QSFP's LED light is OFF while all four of the ICL based E-Ports on that single QSFP are online.
   2. QSFP's LED light is blinking Amber when no QSFP installed.	

Risk of Fix: Low	Probability: Medium
Feature: 16G Platform Services	Function: Other
Reported In Release: FOS7.1.0	

Defect ID: DEFECT000445814	Technical Severity: Medium
Summary: Configuration download failure when downloading fabric watch settings	
Symptom: After configure download from CLI or use BNA to do partial fabric watch data replication, Bottleneck configurations were removing from the switch.	
Risk of Fix: Low	Probability: Medium
Feature: FOS Software	Function: Management Services
Reported In Release: FOS7.0.0	Service Request ID: 1137933

Defect ID: DEFECT000446004	Technical Severity: High
Summary: 7800 Tunnel in DwnPend state after making change to committed rate	
Symptom: 7800 Tunnel enters DwnPend state after configuration change is made. An IPC error is reported during subsequent attempts to delete the tunnel.	
Risk of Fix: Low	Probability: Medium
Feature: FOS Software	Function: FCIP
Reported In Release: FOS7.0.1	Service Request ID: 1147343

Defect ID: DEFECT000446429	Technical Severity: High
Summary: ASIC entries are not being cleared upon 8510 hafailover processing leading to server issues.	
Symptom: On 8510, observed non-responsive host paths on an AIX server with server eventually crashing.	
Risk of Fix: Low	Probability: Low
Feature: FOS Software	Function: Fabric Services
Reported In Release: FOS7.1.0	Service Request ID: 1143385

Defect ID: DEFECT000446834	Technical Severity: Medium
Summary: When ICL Port Fencing is enabled, port enable/disable button in WT displays UI anomalies.	
Symptom: WT presents incorrect options for enable/disable of ports.	
Risk of Fix: Low	**Probability:** Medium
Feature: WebMgmt	**Function:** Other
Reported In Release: FOS7.1.0	

Defect ID: DEFECT000446858	Technical Severity: Medium
Summary: In a heavily congested fabric, if a HAfailover happens during backend port reporting timeout frame, switch falsely identifies stuck VC and performs link reset.	
Symptom: Switch continuously reports of RASLOG "C2-1014, Link Reset" on backend port, and under rare occasion, observed switch panic.	
Risk of Fix: Medium	**Probability:** Medium
Feature: 4G Platform Services	**Function:** FOS Kernel Drivers
Reported In Release: FOS7.0.2	**Service Request ID:** 1148619,1132068

Defect ID: DEFECT000447192	Technical Severity: Medium
Summary: D-Port test between AG and the HBA is stuck and is in IN PROGRESS status.	
Symptom: D-Port test between AG and the HBA is stuck in the "IN PROGRESS" state. It passed the Electrical Loopback but it never started the Optical and the rest of test.	
Risk of Fix: Low	**Probability:** Low
Feature: Access Gateway Services	**Function:** Other
Reported In Release: FOS7.1.0	

Defect ID: DEFECT000447216	Technical Severity: High
Summary: Access Gateway does not respond to FLOGI from host	
Symptom: Access gateway does not respond to the FLOGI issued by the host adapter with ExtLinkRply Accept	
Risk of Fix: Low	**Probability:** Medium
Feature: Access Gateway Services	**Function:** Other
Reported In Release: FOS7.1.0	

Defect ID: DEFECT000447611	Technical Severity: High
Summary: Disable auto tuning for 8G blades in 16G chassis and only manual tuning will be supported for these combination.	
Symptom: After enabling auto tuning, FC8-64 blades faulted in a 16G chassis and the blade had to be power cycled to be recovered.	
Workaround: Disable auto tuning	
Risk of Fix: Medium	**Probability:** Medium
Feature: FOS Software	**Function:** ASIC Driver
Reported In Release: FOS7.0.2	**Service Request ID:** 1149900

Defect ID: DEFECT000447848	Technical Severity: High
Summary: Network Advisor failed to get VF details for the switch when FMS mode is enabled.	
Symptom: Unable to open VF dialog in Network Advisor for a switch with FMS mode enabled.	
Risk of Fix: Low	**Probability:** Low
Feature: FICON	**Function:** Ficud
Reported In Release: FOS7.1.0	

Defect ID: DEFECT000448174	Technical Severity: High
Summary: Director may panic with termination of process fabricd	
Symptom: Director experienced panic after ICL un-plugin/re-plugin or disabling ICL's master	
Workaround: Need to reboot the standby every time ICL master fails and slave turns to new master	
Risk of Fix: Low	Probability: Medium
Feature: FC Services	Function: Fabric
Reported In Release: FOS7.1.0	

Defect ID: DEFECT000448364	Technical Severity: Medium
Summary: Port Admin table does not get updated within the expected refresh interval	
Symptom: Port admin table may show stale data since it is not getting updated as expected.	
Risk of Fix: Low	Probability: Medium
Feature: WebMgmt	Function: Other
Reported In Release: FOS7.1.0	

Defect ID: DEFECT000448534	Technical Severity: High
Summary: NS stops responding to CT commands such as GID_FT, GPN_FT, and RPN_ID.	
Symptom: 3rd party storage ports stop responding which results in I/O stopping. The devices ports must be manually reset to force a relogin with the nameserver again.This issue occurs intermittently at customer setup.	
Risk of Fix: Low	Probability: Low
Feature: FOS Software	Function: Fabric Services
Reported In Release: FOS7.0.1	Service Request ID: 1104327

Defect ID: DEFECT000448752	Technical Severity: Medium
Summary: Web Tools does not show Standby CP firmware level	
Symptom: Web Tools "Switch Admin	Fware Download panel" shows "none" for Standby CP level	
Risk of Fix: Low	Probability: High
Feature: WebMgmt	Function: Firmware Download
Reported In Release: FOS7.1.0	

Defect ID: DEFECT000448983	Technical Severity: High
Summary: FICON DASD CHPID activation fails through FCIP emulating tunnel.	
Symptom: CHPID activation fails	
Workaround: Disable FCIP and all FICON emulation on a tunnel	
Risk of Fix: Low	Probability: High
Feature: FCIP	Function: Emulation
Reported In Release: FOS7.1.0	

Defect ID: DEFECT000448985	Technical Severity: Medium
Summary: Removing AN license key does not remove QoS functionality until link is dropped, need message added to AN license remove and AN license add functionality	
Symptom: If customer removes (or adds) the Adaptive Networking License Key, QoS functionality will not be active until the link is dropped; there is no message indicating this functionality. This could leave the customer with a false sense that they still have or don't have QoS functionality. If the link is dropped unexpectedly this will be a cause for concern.	
Risk of Fix: Low	Probability: Medium
Feature: License	Function: Other
Reported In Release: FOS7.1.0	

Defect ID: DEFECT000450480	Technical Severity: High
Summary: Firmware downgrade from v7.1.0 to v7.0.0d is erroneously blocked (FMS + Allow XISL) when logical switch does not have Allow XISL enabled.	
Symptom: Firmwaredownload is erroneously blocked.	
Risk of Fix: Low	Probability: Low
Feature: Mgmt Embedded - CAL	Function: VF
Reported In Release: FOS7.1.0	

Defect ID: DEFECT000451112	Technical Severity: High
Summary: SNMP daemon exits on FCIP setup	
Symptom: Switch hafailover/hareboot during SNMP daemon retrieves statics on FCIP circuit.	
Risk of Fix: Low	Probability: Medium
Feature: Mgmt Embedded - SNMP	Function: Other
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000451330	Technical Severity: Medium
Summary: Webtools unable to enter a D,I zone	
Symptom: WebTools is not accepting a D,I zone. The window opens for zoning and using 'add other' button opens the box with 'Enter WWN or Domain, Port Index value' but when a D,I were entered and click on enter the box disappears but the zone was not added. WWN zones were able to be added with the same steps.	
Risk of Fix: Low	Probability: Medium
Feature: WebMgmt	Function: Zone Admin
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000451617	Technical Severity: Medium
Summary: Unstable link caused switch to internally reset port, and generated link level errors.	
Symptom: On embedded switch, after upgraded FOS, observed high count of LOSSYNC, link failure errors during server boot.There is no impact to port come online time, but the counters triggered fabric watch warnings.	
Risk of Fix: Low	
Feature: 4G ASIC Driver	Function: PORT
Reported In Release: FOS6.3.2	Service Request ID: TR000369703

Defect ID: DEFECT000451632	Technical Severity: Medium
Summary: weblinkercfgd crashes with BNA scheduled backup of the switch	
Symptom: weblinkercfgd is a restart-able daemon. Most time no ill effect is observed by customer.	
Risk of Fix: Low	Probability: Low
Feature: UNDETERMINED	Function: Other
Reported In Release: FOS7.0.0	Service Request ID: 1157646

Defect ID: DEFECT000451666	Technical Severity: High
Summary: Overall FCIP Tunnel performance degradation between FOS v7.0.2 and v7.1.0x	
Symptom: Tunnel performance difference in a 10 gig tunnel configuration with uncompressed traffic. FOS v7.1.0, v7.1.0a, v7.1.0b seems to max out at 860 MB/sec where as FOS v7.0.x runs at almost line speed (1 Giga-Byte/sec)	
Risk of Fix: Low	Probability: High
Feature: FCIP	Function: FCIP I/O
Reported In Release: FOS7.1.0	

Defect ID: DEFECT000452033	Technical Severity: Medium
Summary: CRC with good EOF on backend ports	
Symptom: CRC with good EOF on backend ports of FC8-64 blade in a DCX-8510. The following ports were observed to see CRCs with good EOF: 1/114, 10/154, and 11/154	
Risk of Fix: Low	Probability: High
Feature: FOS Software	Function: ASIC Driver
Reported In Release: FOS7.0.1	Service Request ID: 1158004

Defect ID: DEFECT000452556	Technical Severity: Medium
Summary: portaddress --bind <slot>/<port> <16-bit address> --auto not working, no error message on failure.	
Symptom: When attempting to bind a specific 8bit area to a port using "portaddress --bind <slot>/<port> <16-bit address> --auto" the command is not recognized and returns the command usage. (no error message for failure)	
Risk of Fix: Low	Probability: High
Feature: FOS Software	Function: Virtual Fabric
Reported In Release: FOS7.0.2	Service Request ID: 1159663

Defect ID: DEFECT000452558	Technical Severity: Medium
Summary: Remove deprecated MIB from FOS v7.1.1 onwards	
Symptom: Remove MIBs that has been deprecated in FOS v7.0 and obsolete in FOS v7.1	
Risk of Fix: Low	Probability: High
Feature: Tech Pubs	Function: Others
Reported In Release: FOS7.1.0	

Defect ID: DEFECT000454123	Technical Severity: High
Summary: Unable to launch EZManager.	
Symptom: EZManager status bar stops at 53% and throws an exception halting the launch	
Risk of Fix: Low	Probability: Medium
Feature: WebMgmt	Function: Web Tools EZ
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000454312	Technical Severity: Critical
Summary: CP panic while taking over active CP role leads to cold recovery	
Symptom: With FX8-18, FR4-18i, when the blade is having sudden access problem, switch recovery may turn cold.	
Risk of Fix: Low	Probability: Low
Feature: FOS Software	Function: Striker
Reported In Release: FOS7.0.0	Service Request ID: 1166323