Brocade Fabric OS v7.0.2e

Release Notes v1.0

May 29, 2014

Document History

Document Title	Summary of Changes	Publication Date
Brocade Fabric OS v7.0.2e Release Notes v1.0	Initial Release	May 29, 2014

Contents

Overview

Fabric OS (FOS) v7.0.2e is a patch release based on FOS v7.0.2d. All hardware platforms and features supported in FOS v7.0.2d are also supported in FOS v7.0.2e. In addition FOS v7.0.2e includes support for all of the features supported in FOS v7.0.1.

Resolution of Important Defects

- DEFECT000454312
  With FX8-18, FR4-18i blades, CP may panic while taking over active CP role, resulting in cold recovery.

- DEFECT000471333
  Switch goes into a rolling reboot. After rolling reboot is stopped by RRD, any subsequent command is responded to with "fabos not yet initialized". Further investigation revealed that certain Vendor Version Level (VVL) bits, in the device FLogi message, were set unexpectedly.

- DEFECT000430239
  FCIP tunnel bounces due to DRAM2 memory allocation failures or BLS-5024 event.

- DEFECT000468549
  3rd party cluster application fails after device gets name server query rejected with reason NSRJT_EXPL_NO_PORTID.

- DEFECT000484414
  Under rare conditions, Access Gateway(AG) entries stay in management server (MS) database even after removing them from the fabric. FOS firmware is expected to remove these stale entries during execution of agshow CLI command. However, due to a timing issue the stale entries may not be removed from the database when agshow CLI command is run.

- DEFECT000476762
  User sees unwanted warning messages while launching Web Tool or Network Advisor.

- DEFECT000481199
  With JRE 1.7.0 update 45, users will see a warning message when WebTools is launched through HTTPS and will not be able to launch WebTools from Brocade Network Advisor versions prior to v12.1.4.

- DEFECT000432406
  Customer observes multiple supportsave processes on switch without actively initiating a recent supportsave. These processes consume memory and may lead to switch panic when an additional supportsave is initiated.

- DEFECT000457373
  BR5480 embedded switch displays invalid message without functional impact.

- DEFECT000485708
  3rd party application fails when connected to a BR8470 FCoE switch running FOS v6.4.3_dcb in Access Gateway mode. Device re-FDISC on one of its logins is incorrectly rejected by the Access Gateway.

- DEFECT000490754
  Switch ports connected to storage controller become unresponsive.

Features

FOS v7.0.2 is a maintenance release that contains fixes for defects including those from FOS v7.0.1a and FOS v7.0.1b patch releases. In addition this release includes the following features and enhancements implemented in FOS v7.0.2:

- D_Port Enhancements
    - D_Port link saturation capability – ability to drive test traffic to saturate link utilization close to line rate as part of D_Port test
- Ability to assign individual ports of an optical ICL to logical switches
    - Prior to FOS v7.0.2, in Virtual Fabrics enabled environment, an entire ICL port (which includes four individual ports as part of a single QSFP) has to be associated with a single logical switch. Starting with FOS v7.0.2, the individual ports within an optical ICL can be assigned to different logical switches. This feature is applicable to the DCX8510 platforms.

      Note: Please note that if any individual port of a QSFP is part of the Base Switch, the remaining ports of that QSFP cannot be assigned to any other logical switch.
- Bottleneck detection enhancements - Decoupling of latency and congestion alerts

  In FOS v7.x releases prior to FOS v7.0.2, when users enabled bottleneck alerts, it would enable alerting for both congestion and latency bottleneck conditions. Starting with FOS v7.0.2 users can choose to enable alerts only for latency bottleneck while not enabling alerts for congestion bottleneck or vice versa. Users still have the option to enable alerts for both congestion and latency bottleneck conditions.

FOS v7.0.1 Feature Descriptions

New Hardware Support

- Brocade 6505 entry level 16G FC switch
- FC8-32E and FC8-48E Condor3 based 8G blades for DCX 8510-8 and DCX 8510-4

Enhanced Optical ICL Topology Support for DCX 8510

FOS v7.0.1 supports the following enhanced topologies using optical ICLs:

- Support for up to nine DCX 8510 chassis in full mesh configuration using optical ICLs
- Support for ICL connectivity with up to ten DCX 8510 chassis in core-edge topology

This increased support delivers massive scalability, significantly reduces cabling complexity, and also makes more ports available for device connectivity.

FOS v7.0.1 also adds support for Enterprise ICL license on DCX 8510 platforms. Description of this license can be found in the "Optionally Licensed Software" section of this document.

Support for Dynamic Fabric Provisioning: Fabric Assigned World Wide Name

In order to simplify and accelerate server deployment and improve operational efficiency, FOS v7.0.1 provides Fabric Assigned WWN or FA-PWWN capability. This feature allows users to create a virtual WWN for a server instead of using the server's physical port WWN (PWWN) to create zoning and LUN mapping/masking. When a FA-PWWN capable server is attached to the SAN, this feature allows the fabric to assign this virtual WWN to that server. This feature requires servers to be using Brocade HBAs/Adapters. Please consult Brocade HBA/Adapter driver documentation and Release Notes to confirm minimum requirements for this feature. For Brocade Network Advisor support, please consult Brocade Network Advisor documentation and Release Notes.

VCS/VDX6730 to FC SAN Connectivity

This feature enables connectivity between hosts (using FCoE) connected to VCS/VDX platforms and FC storage connected to FC SAN via FCR. An E-port on a VDX6730 platform running NOS v2.1.1 is connected to an EX_port on an FCR running FOS v7.0.1 to enable this functionality.

Note:

- Integrated Routing license is not required to share devices between VDX/VCS Ethernet fabric and FC SAN fabric.
- It is recommended to use 5300, DCX/DCX-4S, DCX 8510-8, DCX 8510-4 for FCR functionality for higher scalability.
- A new FCR EX_port mode 5 is used to connect VCS/VDX6730 to FCR

FCIP Enhancements

FOS v7.0.1 enables ESCON and Bus/Tag printer emulation support on FCIP platforms.

This feature provides near native performance for FICON Extended paths to remote ESCON or Bus and Tag printers. Enabling FICON Printer emulation requires the Advanced FICON Acceleration license. This feature is supported on 7800 and FX8-24.

D-port (Diagnostic Port) Support between Brocade 16G Fabric Adapter and Brocade 16G FC switch

D-port functionality is supported between a Brocade 16G Fabric Adapter with adapter firmware version 3.1 or later, and a Brocade 16G FC switch running FOS v7.0.1 or later. This feature requires usage of 16G SFP+ at

both the adapter and the switch. For additional information please consult the Brocade Adapter Release Notes for firmware version 3.1 or later, and the Brocade Adapter Administrator's Guide.

Optionally Licensed Software

Fabric OS v7.0.2 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 v7.0.2 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 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 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.

High Performance Extension over FCIP/FC (formerly known as "FCIP Services") (For the FR4-18i blade) — This license key also includes the FC-FastWrite feature and IPsec capabilities.

Note: The FC-FastWrite feature is not supported on FR4-18i in FOS v7.0 or later.

Brocade Accelerator for FICON – This license enables unique FICON emulation support for IBM's Global Mirror (formerly XRC) application (including Hitachi Data Systems HXRC and EMC's XRC) as well as Tape Pipelining for all FICON tape and virtual tape systems to significantly improve XRC and tape backup/recovery performance over virtually unlimited distance for FR4-18i.

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.

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.

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

Integrated Routing— This license allows any port in a DCX 8510-8, DCX 8510-4, Brocade 6510, 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, 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**: 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 and later.

Temporary License Support

The following licenses are available in FOS v7.0.2 as Universal Temporary or regular temporary licenses:

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

Supported Switches

Fabric OS v7.0.2 supports the Brocade 300, 5410/5424/5450/5460/5470/5480/NC-5480, 5100, 5300, VA-40FC, Brocade Encryption Switch (BES), DCX/DCX-4S, 8000, 7800, 6505, 6510, DCX 8510-8 and DCX 8510-4.

Access Gateway mode is also supported by Fabric OS v7.0.2, and is supported on the following switches: the Brocade 300, 5100, VA-40FC, 8000, 5450, 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:

   

   The serial number label is located as follows:

   - Brocade Encryption Switch, VA-40FC, 300, 5100, 5300, 6510, 6505 — 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 **licenseId** command to display the License Identifier.

FOS Migration Considerations

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

Recommended Migration Paths to FOS v7.0.2e

Migrating from FOS v7.0

Any 8G or 16G platforms running any FOS v7.0.0x release can be non-disruptively upgraded to FOS v7.0.2e.

Migrating from FOS v6.4.x

DCX/DCX-4S units running any FOS v6.4.x release can be non-disruptively upgraded to FOS v7.0.2e.

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 before non-disruptively upgrading to FOS v7.0.2e. Upgrading these platforms from any FOS V6.4.x release **lower than FOS v6.4.1a to FOS v7.0.2e will cause disruption to FC traffic**.

Upgrading any 8G platform operating at FOS v6.4.1a or later to FOS v7.0.2e is non-disruptive to FC traffic.

Migrating from FOS v6.4.1_fcoe1

The upgrade from FOS v6.4.1_fcoe1 to FOS v7.0.2e is non-disruptive to both FC and FCoE traffic on DCX and DCX-4S.

Note: Upgrading from FOS v6.4.1_fcoe or FOS v6.4.x releases other than v6.4.1_fcoe1 to FOS v7.0.2e will be disruptive to FCoE traffic going through FCOE10-24 blades in DCX/DCX-4S. When loading FOS v7.0.2e with Brocade Network Advisor v11.1.1/11.1.1a, there is no warning flagging this FCoE traffic disruption.

Migrating from FOS v6.3.x

To non-disruptively migrate from FOS v6.3.x to v7.0.2e, units should first load FOS v6.4.1a or later (v6.4.1b should be used for encryption platforms, units operating in Access Gateway mode, or units with ports configured as EX or VEX for FCR), and then migrate to FOS v7.0.2e.

FOS Upgrade and Downgrade Special Considerations

The DCX/DCX-4S units running any FOS v6.4.x can be non-disruptively upgraded to FOS v7.0.2e. This upgrade is non-disruptive to FC traffic only. When loading FOS v7.0.2e to a DCX chassis with FCOE10-24 blades with Brocade Network Advisor v11.1.1/11.1.1a, there is no warning flagging FCoE traffic disruption.

The DCX/DCX-4S units running FOS v6.4.1_fcoe1 can be non-disruptively upgraded to FOS v7.0.2e. This upgrade is non-disruptive to both FCoE traffic through FCOE10-24 blades and FC traffic.

Non-disruptive upgrade to FOS v7.0.2e on 8G switches is allowed from **FOSv6.4.1a** or later.

Disruptive upgrades to Fabric OS 7.0.2e are allowed and supported from FOS 6.3 (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 v7.0 .2e will be disruptive to the I/O through the switch.

FC FastWrite , EX_Ports, and TCP byte streaming on FR4-18i must be disabled prior to upgrading to FOS v7.0.2e. Failure to do so will cause the upgrade to be blocked.
Upgrading a switch currently operating in interopmode 2 or 3 to FOS v7.0.2e is disruptive. The interopmode must be changed to 0 prior to upgrading to FOS v7.0.2e, as interopmodes 2 and 3 are not supported on FOS v7.0.2e. Changing the interopmode is an offline operation.

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 11.1.0 is available in

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

For SAN Management, Network Advisor 11.1 is available in three editions:

- ***Network Advisor Professional***: a fabric management application that is ideally suited for small-size businesses that need a lightweight management product to manage their smaller fabrics. It manages 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 four physical or virtual fabrics (FOS, M-EOS and Mixed fabrics) 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 24 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 11.1 Release Notes, Network Advisor 11.1 User Guide, and Network Advisor 11.1 Installation, Migration, & Transition Guides.

Note:

Brocade Network Advisor 11.0 and DCFM 10.4 cannot manage switches running FOS v7.0 or later.

Brocade Network Advisor 11.1.3 is required to manage Brocade 6505 platform.

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

DCFM Compatibility

DCFM is not qualified or support the management of switches operating with FOS v7.0 and later firmware versions. **You must first upgrade DCFM to Network Advisor 11.1 or later if you are planning to upgrade devices to FOS v7.0 or you risk losing management connectivity.**

WebTools Compatibility

FOS v7.0.2e is qualified and supported with Oracle JRE 1.7.0 update 25, update 45, update 51, and update 55. Launching WebTools with Oracle JRE 1.7.0 update 51 and update 55 through Brocade Network Advisor is only supported on version 12.1.5 or later. With JRE 1.7.0 update 51 to update 55, users could see some browser warning messages that can be ignored. WebTools is supported with Google Chrome browser with FOS v7.0.2e.

- When launching WebTools on a computer without Internet access, it could take upto 5 minutes to complete because the certicate revocation check performed for the WebTools application takes time to timeout. Users can turn off the certification revocation check on the Java control panel as a workaround.
- Launching WebTools with Oracle JRE 1.7.0 update 51 and update 55 through Brocade Network Advisor is only supported on version 12.1.5 or later. With JRE 1.7.0 update 51 and update 55, users could see browser warning messages that the WebTools application requires unrestricted access or the certificate signing the application is not recognized. These messages can be ignored. In addition, users must check the "Enable Java content in the browser" box under the Security tab of Java Control Console to allow launching WebTools from BNA server clients.

SMI Compatibility

- It is important to note that host SMI-S agents cannot be used to manage switches running FOS v7.0.2
- If users want to manage a switch running FOS v7.0.2 using SMI-S interface, they must use Brocade Network Advisor's integrated SMI agent.

Fabric OS Compatibility

The following table lists the earliest versions of Brocade software supported in this release, that is, the *earliest* supported software versions that interoperate. Brocade recommends using the *latest* software versions to get the greatest benefit from the SAN.

To ensure that a configuration is fully supported, always check the appropriate SAN, storage or blade server product support page to verify support of specific code levels on specific switch platforms prior to installing on your switch. Use only FOS versions that are supported by the provider.

For a list of the effective end-of-life dates for all versions of Fabric OS, visit the following Brocade Web site:

http://www.brocade.com/support/end_of_life.jsp

Supported Products and FOS Interoperability	
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)

Supported Products and FOS Interoperability	
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]
VA-40FC	v6.2.1_vfc [6], v6.2.2 or later [6]
Brocade DCX-4S	v6.2.0 or later [6]
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
Brocade 6505	FOS v7.0.1 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. 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]
McDATA SANRouters 1620 and 2640	Not Supported

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

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. For higher FCR backbone scalability (refer to separate "Brocade SAN Scalability Guidelines" documentation for details), please use 5300, DCX, DCX-4S, DCX 8510-8, DCX 8510-4.

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 v7.0.2 software is fully qualified and supports the blades for the DCX/DCX-4S noted in the following table:

DCX/DCX-4S Blade Support Matrix	
16-, 32-, 48- and 64-port 8Gbit port blades (FC8-16, FC8-32, FC8-48, FC8-64) and the 6-port 10G FC blade (FC10-6)	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.
FCIP/FC Router blade (FR4-18i)	Up to a maximum of 4 blades of this type. This can be extended under special circumstances, but must be approved by Brocade's Product Team. Up to 8 FR4-18i blades can be installed in a DCX if they are used only for FCIP without routing. **Note**: FR4-18i cannot coexist with FX8-24 in FOS v7.0 or later FR4-18i does not support EX-ports, FC FastWrite and WAN optimization features in FOS v7.0 or later FR4-18i supports VEX ports on FOS v7.0 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 v7.0.2

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

Fabric OS v7.0.2 software is fully qualified and supports the blades for the DCX 8510-8 and DCX 8510-4 noted in the table below.

DCX 8510-8/DCX 8510-4 Blade Support Matrix	
FC16-32, FC16-48 16G FC blades	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 v7.0.2

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

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

Power Supply Requirements for Blades in DCX/DCX-4S				
Blades	**Type of Blade**	**DCX/DCX-4S** @110 VAC (Redundant configurations)	**DCX/DCX-4S** @200-240 VAC (Redundant configurations)	**Comments**
FC10-6, 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	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

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 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, Brocade 6505 in FOS v7.0.1 or later.
- Users who want to utilize Access Gateway's Device-based mapping feature in the ESX environments are encouraged to refer to the SAN TechNote GA-TN-276-00 for best implementation practices. Please follow these instructions to access this technote:
  - Log in to http://my.brocade.com

- Go to Documentation > Tech Notes.
- Look for the Tech Note on Access Gateway Device-Based Mapping in VMware ESX Server.

Brocade HBA/Adapter Compatibility

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

D-Port

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

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.
- The "*cryptocfg –manual_rekey –all*" command should not be used in environments with multiple encryption engines (FS8-18 blades) installed in a DCX/DCX-4S/DCX 8510 chassis with more than one encryption engine has access to the same LUN. In such situations, use the "*cryptocfg –manual_rekey <CTC> <LUN Num> <Initiator PWWN>"* command to manually rekey these LUNs.
- 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.
- The RSA RKM Appliance A1.6, SW v2.7.1.1 is supported. The procedure for setting up the RKM Appliance with BES or a DCX/DCX-4S/DCX 8510 with FS8-18 blades is located in the Encryption Admin Guide.
- Support for registering a 2nd RKM Appliance on BES/FS8-18 is blocked. If the RKM Appliances are clustered, then the virtual IP address hosted by a 3rd party IP load balancer for the RKM 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.
- For new features added to encryption in FOS v6.4.0, such as, disk device decommissioning, combined disk-tape encryption support on the same encryption engine, and redundant key ID metadata option for replication environments, all the nodes in the encryption group must be running FOS v6.4.0 or higher versions of FOS. Firmware downgrade will be prevented from FOS v6.4.0 to a lower version if one or more of these features are in use.
- 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 and EXTENDED COPY, which are related to VAAI (vStorage APIs for Array Integration) hardware acceleration in vSphere 4.1. This will result in non-VAAI methods of data transfer for the underlying arrays, and may affect the performance of VM related operations.

FCIP (FR4-18i, Brocade 7800 and FX8-24)

- Any firmware activation will disrupt I/O traffic on FCIP links.
- Latency measurements supported on FCIP Tunnels:
    - 1GbE & 10GbE - 200ms round trip time and 1% loss.
- After inserting a 4G SFP in GE ports of an FX8-24 blade or 7800 switch, sometimes "sfpshow" output might display "Cannot read serial data!" . Removing and re-inserting the SFP should resolve this issue. It is recommended that users perform sfpshow immediately after inserting the SFP and ensure SFP is seated properly before connecting the cables.
- When running FOS v7.0.0 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:
    - InBand Management
    - Multigigabit Circuit
    - Shared GE among Logical Switches
    - Auto-mode compression option

- VE as XISL
- 10GigE lossless failover
- Modified QoS percentages
- 10GigE ARL
- IP Configuration where multiple GigEs have same subnet values
- For a tunnel configuration on 1GE ports that has more than 4 circuits
- Teradata emulation enabled
- 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 v7.0.2d or downgrading from v7.0.2d 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.
- When using FC Routing in a backbone to edge configuration with an Mi10K in the edge fabric, users may experience slow throughput for hosts attached to the Mi10K. Users may encounter this following a bounced IFL connection between the backbone and edge fabric. This slowdown can be resolved by disabling/enabling the Mi10K ports for the hosts that are impacted.
- Mi10K Directors operating with firmware prior to M-EOSn v9.9.5 may experience repeated system faults when attached as an FCR edge switch to a Brocade 7800 EX Port. To avoid this, ensure that the Mi10K is operating with M-EOSn v9.9.5 or later when in an edge fabric that will be attached to a Brocade 7800 FCR Backbone.
- 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.
- EX ports may transition to a faulty state after trunking is enabled.
    - When EX port trunking is set to "1" on the same ASIC, port states toggle between "Mod_val", "No_Module", and "Port_Flt" followed by raslog PORT-1003 messages.
    - If this behavior is encountered, upgrade to FOS 7.1.x code or higher with the fix for defect 510027.

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, and Brocade 6505.
- 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.

Native Connectivity (M-EOS interoperability)

- A switch running FOS v7.0 or later cannot form E-port connectivity with any M-EOS platform. A switch running FOS v7.0 or later can only operate in Brocade native mode (interopmode 0). Connectivity between M-EOS platforms and a switch running FOS v7.0 or later is supported via FCR.

Port Mirroring

- On the Brocade 5300, the port mirroring feature has a limitation where all port mirror resources must stay within the same ASIC port group. The resources are the configured mirror port, Source Device, and Destination Device or ISL, if the Destination Device is located on another switch. The ASIC port groups are 0-15, 16-31, 32-47, 48-63, and 64-79. The routes will be broken if the port mirror resources are spread across multiple port groups.
- Port Mirroring is not supported on the Brocade 7800.

Port Statistics

- On Condor3-based (16G FC) 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.

SNMP

- Though below OIDs are present in Brocade MIBs, they are not functional in FOS v7.0.2a or later . Below are the OIDs that are not functional in FOS v7.0.2a or later:
  - swDeviceStatusTrap
  - swConnUnitPCSErrorCounter in swConnUnitPortStatExtensionTable
  - swDeviceStatus in swSystemTable.
  - Addition of swConnUnitPortCapableSpeeds

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

- The maximum zone database size supported in FOS v7.x is limited to 1MB, even though the cfgsize CLI on some platforms (DCX, DCX-4S, DCX 8510-8, DCX 8510-4) show the maximum zone database capacity to be 2MB. Users should not exceed the 1MB zone database capacity to operate within the supported limits. Please note that there is no enforcement by FOS 7.0.x to restrict users to operate within 1MB 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

- 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.
- For the configure command, in FOS v6.4, or later the default value that displays for Maximum Logins per switch is different than the value that displays in FOS v6.3.x. The default value has not changed; it was displayed incorrectly in FOS v6.3.x, and is now corrected.
- The Brocade Network Advisor seed switch should always have the highest FOS version used in the fabric.
- For login authentication through RADIUS, Brocade switch should be able to reach RADIUS servers through TCP authentication port (default 1812) and accounting port (default 1813). Both of these ports must be kept open in any firewall settings.

Defects

Closed with Code Change in Fabric OS v7.0.2e

This section lists the defects with Critical, High, and Medium Technical Severity closed with a code change as of May 29, 2014 in FOS v7.0.2e.

Defect ID: DEFECT000361971	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Other
Reported In Release: FOS7.0.0	**Technology Area:** Other
Symptom: F-Port was logged out of switch due to laser fault during media access.	
Condition: This is an unlikely situation that may be encountered under heavy CPU load and rare timing race condition. i2c read of smart data has been enhanced to address this for impacted CPU type.	

Defect ID: DEFECT000408703	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS6.4.2	**Technology Area:** BB Credits
Symptom: "CRC with Good EOF Errors detected" may cause buffer credit loss.	
Condition: DCX-4S platform with FC8-48 installed in Slot 1; Slot 1 port 2	
Recovery: Manual tuning or auto tuning	

Defect ID: DEFECT000411138	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Other
Reported In Release: FOS7.0.0	**Technology Area:** Other
Symptom: DCX family could experience a hafailover during core blade failure.	
Condition: In an unlikely event of handling hardware error interrupts on core blade, CP paniced due to race condition attempting to bring core blade down gracefully.	

Defect ID: DEFECT000417440	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.0.0	**Technology Area:** CLI
Symptom: Detected termination of name server daemon (NSD) during the execution of the CLI command "nodefind".	
Condition: The CLI command "nodefind" triggers switch panic when name server shows two devices present for the same WWN.	
Workaround: Do not execute the CLI command "nodefind".	

Defect ID: DEFECT000418392	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.1.0	**Technology Area:** Web Tools
Symptom: Weblinker crash while the fabric is being monitored by Brocade Network Advisor.	
Condition: This may be encountered in a large fabric with security policy activated.	

Defect ID: DEFECT000430239	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.0.0	**Technology Area:** FCIP
Symptom: FCIP tunnel bounces due to DRAM2 memory allocation failures or BLS-5024 event.	
Condition: Memory allocation failures lead to VE ports down with circuits InProg.	
Recovery: FX8-24 requires reset to recover.	

Defect ID: DEFECT000431101	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Other
Reported In Release: FOS7.0.0	**Technology Area:** Other
Symptom: When pulling out a disk from a 3rd party vendor storage, access to the whole storage is lost.	
Condition: After hareboot, loop enable bit is not set. If a disk is removed from a loop storage connected to switch fabric loop (FL) port, then access to storage is lost.	
Recovery: Bounce port by portdisable and portenable	

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

Defect ID: DEFECT000433200	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.0.2	**Technology Area:** Web Tools
Symptom: Under rare condition Weblinker/HTTPD are terminated and restarted but still cannot service the HTTP requests. All subsequent Webtools/BNA requests encounter the error "Chassis is not ready for management". Note: This fix does not fully resolve this issue but it provides a non-disruptive workaround for the interim period. With this fix customer may workaround/recover from this condition with hafailover/hareboot, or may contact support for manual HTTPD restart workaround. This issue is fully resolved via Defect 477596 fix in FOS 7.0.2e/7.1.1b/v7.1.2/7.2.1.	
Condition: This may be encountered on very rare occasions when switches are managed by Webtools/Brocade Network Advisor.	
Workaround: NONE without this fix. Use reboot to recover.	

Defect ID: DEFECT000440137	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.0.0	**Technology Area:** BB Credits
Symptom: "CRC with good EOF errors" observed and may cause buffer credit loss.	
Condition: This may occur on DCX-4S with FC8-16 port blades installed in slot 1, 2	
Recovery: Manual tuning or auto tuning.	

Defect ID: DEFECT000453711	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Security
Reported In Release: FOS7.1.0	**Technology Area:** Fabric Authentication
Symptom: Following certificate deletion, the certificate file size is truncated to zero, causing reboot loop on standby CP with weblinker panic. Console logs message with: SSLCertificateFile: file '/etc/fabos/certs/sw0/x.x.x.x.crt' does not exist or is empty.	
Condition: Delete certificate from the non-default VF context using seccertutil CLI command.	
Recovery: Remove the zero sized certificate file on standby CP. Active CP will sync the new file.	

Defect ID: DEFECT000454312	
Technical Severity: Critical	**Probability:** Low
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.0.0	**Technology Area:** FCIP
Symptom: With FX8-18, FR4-18i blades, CP may panic while taking over active CP role, resulting in cold recovery.	
Condition: This is a very unlikely scenario, where the new active CP may panic while accessing a faulted/disabled blade, on the heels of a reset of the original active CP.	

Defect ID: DEFECT000454580	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Security
Reported In Release: FOS6.4.2	**Technology Area:** Fabric Authentication
Symptom: On director, with SSL configured on Active CP, a newly inserted Standby CP may panic. On switch, hot code load may result in cold recovery due to CP Panic if Time Server becomes unreachable during hareboot.	
Condition: On Directors, a new/replacement standby CP may panic upon insertion. This may happen if: 1. The clock on the new standby CP is configured to a later time than on the active CP and 2. Weblinker is auto restarted to pick up a configuration change such as SSL configured on the active CP, but not configured on the new standby CP. On Switches, hareboot may result in cold recovery, due to CP Panic, if Time Server becomes unreachable during hareboot and the internal clock is configured to an earlier time than the Time Server clock.	
Workaround: For director CP replacement case: Perform hadisabled before inserting standby CP. Then login to standby CP, change the date/time on standby CP to earlier than on the active CP using the command "/bin/date" and then execute haEnable. For Switch hot code case: Configure the switch to use local time (instead of NTP) and then revert back to NTP upon successful completion of warm recovery.	
Recovery: No action required. Previous switch reboot will fix the issue.	

Defect ID: DEFECT000454926	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Other
Reported In Release: FOS7.0.0	**Technology Area:** Other
Symptom: On Brocade 300, observed CRC errors on 8G ISL ports when there are 4G ports in the same chip in a specific customer configuration.	
Condition: Problems stems from 4G data and 8G ISLs are run in physically adjacent ports.	
Workaround: Physically separating 4G and 8G channels on the system,	

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

Defect ID: DEFECT000459102	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.0.2	**Technology Area:** FC-FC routing
Symptom: Domain change caused proxy devices to be stuck in "initializing" state.	
Condition: If a domain ID was previously changed, proxy devices could get stuck in "initializing" state after adding a new switch to an edge fabric.	
Recovery: Deleting and re-adding an LSAN zone will permit the devices to recover.	

Defect ID: DEFECT000461189	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.2.0	**Technology Area:** Web Tools
Symptom: Unable to launch WebTools using Google Chrome browser and IE11 with Java update 45 or 51.	
Condition: This happens when using the latest Java update revision 45 or 51.	
Workaround: Use another browser or older Java update.	

Defect ID: DEFECT000462116	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.0.0	**Technology Area:** Platform Services
Symptom: After director reboot, CPs lost heartbeat and active CP was reset. Standby CP panicked while taking over the Active role.	
Condition: Port blade hardware failure may trigger loss of heartbeat (between two CPs).	
Recovery: Switch is recovered after reboot; replace bad port blade to prevent re-occurrence.	

Defect ID: DEFECT000467263	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.0.2	**Technology Area:** Frame Monitoring
Symptom: The fwd daemon may crash and result in a switch panic while repeatedly performing addition and deletion of frame monitors.	
Condition: This may be encountered when frame monitor deletion coincides with fabric watch polls (that occurs periodically every 6 sec) to get the threshold values.	

Defect ID: DEFECT000468549	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.0.2	**Technology Area:** FC-FC routing
Symptom: 3rd party cluster application fails after device gets name server query rejected with reason NSRJT_EXPL_NO_PORTID.	
Condition: This is a timing issue that occurs rarely for a node device that sends back to back FLOGIs within a short time span on the same port.	
Workaround: Disable and enable ports manually to complete site swap.	
Recovery: Toggle affected ports.	

Defect ID: DEFECT000469915	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS6.4.2	**Technology Area:** Platform Services
Symptom: CLI nscamshow reported "state is unknown" for Port IDs of remote switches, and impacted devices cannot communicate with each other.	
Condition: This may occur in a setup with Long distance E port due to a rare name server query frame time out condition.	
Recovery: hafailover to recover.	

Defect ID: DEFECT000470123	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Virtualization
Reported In Release: FOS7.0.0	**Technology Area:** Access Gateway
Symptom: Immediately after a port bounce with AG or while running “agshow” CLI command, Brocade Network Advisor seed switch may panic.	
Condition: Following a bounce of the port connecting AG to the switch, before fabric management server and name server data bases have stabilized, polling from Brocade Network Advisor may cause seed switch to panic. Likewise, running agshow on switch may also cause the switch to panic. The timing window for triggering the panic is very small.	
Workaround: Do not poll switch immediately following disruptive events.	

Defect ID: DEFECT000471333	
Technical Severity: Critical	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.0.0	**Technology Area:** FC-FC routing
Symptom: Switch goes into a rolling reboot. After rolling reboot is stopped by RRD, any subsequent command is responded to with "fabos not yet initialized". Further investigation revealed that certain Vendor Version Level (VVL) bits, in the device FLogi message, were set unexpectedly.	
Condition: This may be observed while 3rd party vendor performs firmware upgrade.	
Workaround: Keep the port(s) connected to the conflicting device in a disabled state or reboot the conflicting device(s). 3rd party vendor has also released new firmware to correct the Flogi bits setting. Please contact support to obtain details.	
Recovery: Disable switch port(s) connected to device(s) in question and reboot to bring up the switch.	

Defect ID: DEFECT000472121	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Security
Reported In Release: FOS7.0.2	**Technology Area:** Encryption
Symptom: SCSI errors are logged on host during an encrypted tape backup.	
Condition: GCS_ID query from host with Virtual Target PID is responded with 0x0 (No class of Service) from Name Server.	
Recovery: No recovery is needed. Tape backup is actually completed but host logs errors without impacting the backup itself.	

Defect ID: DEFECT000473087	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.2.0	**Technology Area:** FC-FC routing
Symptom: Customer could see different symptoms, such as: 1. RTWR error due to frame drop on 16G FCR 2. Fabric domains are inconsistent between fabric module and routing module, which cause Fport cannot come online.	
Condition: If non-trunked EX-port is configured, when remote side of the EX-port goes down (i.e E-port disabled), in a multiple 16G FCR Backbone-to-Edge configuration, iswitchd will not remove the LE domain. It will retain the LE domain even though its proxies are removed. During this time, all the domain controller frames to the LE domain are dropped. This does not impact 4G/8G FCR switches. However, SCN is not sent and could impact fabric rebuild.	

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

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

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

Defect ID: DEFECT000476762	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Management
Reported In Release: FOS7.2.0	**Technology Area:** Web Tools
Symptom: User sees unwanted warning messages while launching Web Tool or Network Advisor.	
Condition: When a server uses a later revision of JAVA update JRE1.7u45 and JRE1.7u51.	
Workaround: Launch Web Tools through Network Advisor running version 12.1.4 or higher.	

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

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

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

Defect ID: DEFECT000480765	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Management
Reported In Release: FOS7.2.0	**Technology Area:** Web Tools
Symptom: "Application Blocked by Security Settings" is displayed and fails to launch EZ Manager	
Condition: This issue will be seen only with older JRE updates (40 and below).	
Workaround: Use latest JRE	

Defect ID: DEFECT000481199	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Management
Reported In Release: FOS7.2.0	**Technology Area:** Web Tools
Symptom: With JRE 1.7.0 update 45, users will see a warning message when WebTools is launched through HTTPS and will not be able to launch WebTools from Brocade Network Advisor versions prior to v12.1.4.	
Condition: Web Tools will be blocked when it is launched through a version of Brocade Network Advisor prior to 12.1.4 on a system running JRE 1.7u45. Web Tools will encounter error messages when it is launched directly through HTTPs on a system running JRE 1.7u45.	
Workaround: Launch Web Tools through Brocade Network Advisor running version 12.1.4 or higher.	
Recovery: JRE must be downgraded to 1.7u25.	

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

Defect ID: DEFECT000485708	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Virtualization
Reported In Release: FOS6.4.3_dcb	**Technology Area:** NPIV
Symptom: 3rd party application fails when connected to a BR8470 FCoE switch running FOS v6.4.3_dcb in Access Gateway mode. Device re-FDISC on one of its logins is incorrectly rejected by the Access Gateway.	
Condition: This issue occurs under the following conditions: 1. Switch is in Access Gateway mode 2. Device has already logged into a NPIV port on Access Gateway 3. NPIV device has also already logged in (with FDISC) to the same port 4. NPIV device logs in again (with FDISC) on the same port	
Recovery: Bounce (offline, then online) the Access Gateway port.	

Defect ID: DEFECT000489829	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.1.0	**Technology Area:** End-to-end Performance Monitoring
Symptom: RX /Tx performance values higher than 100% on a couple of ports.	
Condition: These may be seen only when link goes down and comes back up.	

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

Defect ID: DEFECT000492340	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.3.0	**Technology Area:** BB Credits
Symptom: User may notice frame drops on the back end edge and core ports with FS8-18 and FX8-24 in the chassis.	
Condition: This may be seen when FS8-18 and FX8-24 blades are used in a 8510-4 or 8510-8 chassis.	
Recovery: Upgrade code with fix and perform a power cycle of port blade to have the new credit buffer allocation scheme to take effect.	

Defect ID: DEFECT000498907	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Management
Reported In Release: FOS7.0.2	**Technology Area:** Web Tools
Symptom: After resetting switch to factory defaults with AMM Web interface on BR5470, switch goes through a limited cycle of rolling reboots.	
Condition: It happens when using AMM Web Interface to reset switch back to Factory defaults. It deleted /etc/fabos/rbac/dynamic file.	
Recovery: Need to copy dynamic.default to dynamic in /etc/fabos/rbac/ to recover	

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

Defect ID: DEFECT000505359	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.0.0	**Technology Area:** CLI
Symptom: Switch panics intermittently after Supportsave command is started.	
Condition: This may occur when supportsave is issued with 4G blades in switch.	
Recovery: Switch recovers on its own.	

Closed with Code Change in Fabric OS v7.0.2d

This section lists the defects with Critical, High, and Medium Technical Severity closed with a code change as of June 25, 2013 in FOS v7.0.2d.

Defect ID: DEFECT000389303	**Technical Severity:** Medium
Summary: Switch finds inconsistency in domain count and E-port count during HAfailover	
Symptom: After FOS upgrade, multiple ports report "Not ready for F or L ports"	
Workaround: Manual fabric rebuild by bouncing E_port or switch disable/enable.	
Probability: Medium	
Feature: FOS Software	**Function:** Fabric Services
Reported In Release: FOS6.4.2	**Service Request ID:** 710297

Defect ID: DEFECT000404322	**Technical Severity:** Medium
Summary: Diagnostics do 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	
Feature: Diagnostics	**Function:** Other
Reported In Release: FOS7.0.2	

Defect ID: DEFECT000409350	**Technical Severity:** Medium
Summary: Observed SCSI "Clear ACA" dropped during boot over SAN	
Symptom: Boot over SAN may have an 8 second delay when target device is not on the local switch.	
Probability: Medium	
Feature: FOS Software	**Function:** ASIC Driver
Reported In Release: FOS7.0.0	**Service Request ID:** 746453

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.	
Probability: Medium	
Feature: FOS Software	**Function:** SNMP
Reported In Release: FOS7.0.1	**Service Request ID:** 1087061

Defect ID: DEFECT000423389	**Technical Severity:** High
Summary: Switch panic while running suppotsave with 4G blades.	
Symptom: When RTE portion of supportsave is run on a 4G blade, it may trigger a switch panic.	
Probability: Low	
Feature: FOS Software	**Function:** Panic / OOM
Reported In Release: FOS7.0.0	**Service Request ID:** 1094952

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.	
Probability: High	
Feature: 8G FCR	**Function:** FCR Daemon
Reported In Release: FOS7.0.1	**Service Request ID:** 1102900,1123307

Defect ID: DEFECT000429815	**Technical Severity:** High
Summary: BR5480 exhibits snmpd crash and switch reboot when being managed by BNA.	
Symptom: BR5480 switches running in AG mode and managed by BNA exhibit snmpd crash and switch reboot.	
Workaround: Avoid managing an AG switch with BNA or have all ports connected to either N_Port or F_port or have AG in auto policy disabled state.	
Probability: High	
Feature: FOS Software	**Function:** Management Services
Reported In Release: FOS6.4.2	**Service Request ID:** 1102791

Defect ID: DEFECT000432514	**Technical Severity:** Medium
Summary: After power cycle, FC8-64 port blade that is installed incorrectly in BR8510 faults during POST	
Symptom: FC8-64 port blade faults (51) during POST. A slotpoweroff/on or reboot clears the condition.	
Feature: Diagnostics	**Function:** Post Diags
Reported In Release: FOS7.0.1	

Defect ID: DEFECT000434819	**Technical Severity:** Medium
Summary: Polling container stats every 30 seconds caused free memory decrease on blade processor.	
Symptom: Continuous decrease in free memory is observed on blade processor when polling container stat every 30 seconds.	
Workaround: Reboot FS8-18 blade or BES switch	
Probability: Medium	
Feature: Data Security	**Function:** Disk Encryption
Reported In Release: FOS7.0.2	**Service Request ID:** 1102253

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.	
Probability: High	
Feature: FOS Software	**Function:** Fabric Services
Reported In Release: FOS7.0.2	**Service Request ID:** 1116355

Defect ID: DEFECT000436921	**Technical Severity:** High
Summary: Console print hung and caused other process to unable to complete	
Symptom: In general customer observes switch panic, unable to access switch.	
Workaround: Check console port and make sure the settings are correct	
Probability: Low	
Feature: FOS	**Function:** KERNEL
Reported In Release: FOS6.3.1_dcb	**Service Request ID:** 1112726

Defect ID: DEFECT000440989	**Technical Severity:** High
Summary: BNA 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: BNA restarts after hitting an out of memory error.	
Workaround: Reboot FS8-18 blade or BES switch	
Probability: Low	
Feature: CEE-MANAGEABILITY	**Function:** CAL INTERFACE
Reported In Release: FOS7.1.0	**Service Request ID:** 1102253

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.	
Probability: Low	
Feature: 8G ASIC Driver	**Function:** C2 ASIC driver
Reported In Release: FOS7.0.2	

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/FS8-18 fails. In this case, BES/FS8-18 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.	
Probability: Medium	
Feature: FOS-Infrastructure	**Function:** Other
Reported In Release: FOS7.1.0	

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

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	
Probability: Medium	
Feature: FOS Software	**Function:** Encryption
Reported In Release: FOS7.0.2	**Service Request ID:** 1145987

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.	
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 HA processing leading to server issues.	
Symptom: Observer non-responsive host paths on an server with server eventually crashing. Switch does not forward any SCSI task management commands	
Probability: Low	
Feature: FOS Software	**Function:** Fabric Services
Reported In Release: FOS7.1.0	**Service Request ID:** 1143385

Defect ID: DEFECT000446858	**Technical Severity:** Medium
Summary: 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.	
Symptom: Switch continuously reports RASLOG “C2-1014, Link Reset” on backend port, and under rare occasion, observed switch panic.	
Probability: Medium	
Feature: 4G Platform Services	**Function:** FOS Kernel Drivers
Reported In Release: FOS7.0.2	**Service Request ID:** 1148619,1132068

Defect ID: DEFECT000447611	**Technical Severity:** High
Summary: Disable auto tuning for 8G blades in 16G chassis. Only manual tuning will be supported for this 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	
Probability: Medium	
Feature: FOS Software	**Function:** ASIC Driver
Reported In Release: FOS7.0.2	**Service Request ID:** 1149900

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

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 upgrading FOS, observed high count of LOSSYNC, link failure errors during server boot.There is no impact to the time for port to come online, but the counters triggered fabric watch warnings.	
Feature: 4G ASIC Driver	**Function:** PORT
Reported In Release: FOS6.3.2	

Defect ID: DEFECT000460768	**Technical Severity:** High

Summary: Blade fault unnecessarily on rare parity errors.	
Symptom: Customer experienced frequent blade fault upon detecting transient self-correctable ASIC errors	
Feature: FOS Software	**Function:** ASIC Driver
Reported In Release: FOS7.1.0	**Service Request ID:** 1184138

Defect ID: DEFECT000461019	**Technical Severity:** Medium
Summary: Report the back end link CRC with good EOF errors separately from the current asic error monitoring scheme	
Symptom: Unable to decide when to tune serdes value for link optimal performance: Added new raslog C2-1020 and C2-1030, C3-1020 and C3-1030 to separately track backend CRC with good EOF	
Probability: Low	
Feature: FOS Software	**Function:** ASIC Driver
Reported In Release: FOS6.4.3	

Defect ID: DEFECT000418918	**Technical Severity:** Medium
Summary: Bit errors in lookup memory may cause incorrect decryption.	
Symptom: If the read only memory (ROM) inside the FPGA used by the AES engine for memory lookups encounters a bit error, data frames may then be wrongly decrypted.	
Risk of Fix: Medium	**Probability:** High
Feature: Data Security	**Function:** Encryption Group
Reported In Release: FOS7.1.0	

Closed with Code Change in Fabric OS v7.0.2c

This section lists the defects with Critical, High, and Medium Technical Severity closed with a code change as of February 22, 2013 in FOS v7.0.2c

Defect ID: DEFECT000431588	**Technical Severity:** Medium
Summary: FC8-64 in Slot 1 of DCX+ Faulting During Serdes Auto Tuning. The change also applies to DCX.	
Symptom: FC8-64 running in slot 1 of a DCX+ experienced blade fault due to excessive CRC w/good EOF errors. Autotuning was attempted but blade fault occurred before an alternate value could be derived to resolve the errors.	
Probability: Low	
Feature: 8G ASIC Driver	**Function:** C2 ASIC driver
Reported In Release: FOS7.0.2	**Service Request ID:** 1087861

Defect ID: DEFECT000441030	**Technical Severity:** Medium
Summary: SNMPv3 read/write USM user do not work in Fabric OS v7.0.2b	
Symptom: Unable to query any OID from a read/write snmpv3 user, but read only users are successful.	
Workaround: Use SNMPv1/V2. Also, SNMPv3 with users having Read Only (RO) permission can ontinue to discover the switch and perform CAL/HTTP query and SNMP get operations.	
Probability: High	
Feature: FOS Software	**Function:** SNMP
Reported In Release: FOS7.0.2	**Service Request ID:** 1135189

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.	
Probability: Medium	
Feature: 16G Platform Services	**Function:** FOS Kernel Drivers
Reported In Release: FOS7.0.2	**Service Request ID:** 1032557

Closed with Code Change in Fabric OS v7.0.2b

This section lists the defects with Critical, High, and Medium Technical Severity closed with a code change as of March 18, 2013 in FOS v7.0.2b

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	
Probability: Medium	
Feature: 16G ASIC driver	**Function:** Routing
Reported In Release: FOS7.0.2	

Defect ID: DEFECT000409897	**Technical Severity:** High
Summary: Switches running FOS v7.0.x firmware may have an issue bringing F ports online when multiple ports attempt to login to the switch at the same time	
Symptom: F-ports cannot come on line and CLI “switchshow” has the ports as "Disabled (Switch not ready for F or L ports)”.	
Probability: Medium	
Feature: 16G Platform Services	**Function:** FOS kernel drivers
Reported In Release: FOS7.0.2	

Defect ID: DEFECT000358156	**Technical Severity:** High
Summary: FCIP Tunnel bounce caused by chip reset on FX8-24	
Symptom: Chip reset due to PCIe errors with raslog BLS-5023. The chip reset can cause tunnel bounce and IO halt	
Probability: Low	
Feature: Striker/Spike Platform Services	**Function:** Blade Driver
Reported In Release: FOS7.0.0	

Defect ID: DEFECT000387013	**Technical Severity:** Medium
Summary: Stale AG entry remains present in management server database after the removal of AG.	
Symptom: Switch stays in manageability view even after it is physically removed from fabric.	
Probability: Low	
Feature: FOS Software	**Function:** Access Gateway
Reported In Release: FOS6.2.2	**Service Request ID:** 699581

Defect ID:	DEFECT000410236	**Technical Severity:**	Medium
Summary:	EE monitors in VF environment with duplicate PID/SID on same ASIC do not function		
Symptom:	Create a logical switch and install EE monitors on the ports (same asic) of both default and logical switch having same sid/pid, then run traffic and the EE monitor counters do not increament as expected.		
Probability:	Low		
Feature:	FOS Software	**Function:**	Virtual Fabric
Reported In Release:	FOS6.3.2	**Service Request ID:**	752195

Defect ID:	DEFECT000411644	**Technical Severity:**	Medium
Summary:	When executed on BR6510/BR06505, portloopbacktest command always uses 16G mode, regardless of port speed specified.		
Symptom:	On BR6510/BR6505, "portloopbacktest -spd_mode 8" does not indicate the test is run in 8G speed. Same is true for 4G and other valid "spd_mode" options		
Probability:	High		
Feature:	16G Platform Services	**Function:**	FOS Kernel Drivers
Reported In Release:	FOS7.0.1	**Service Request ID:**	754811

Defect ID:	DEFECT000412938	**Technical Severity:**	Medium
Summary:	Fabric Watch erroneously reporting a "build fabric"		
Symptom:	On a busy switch, Fabric Watch falsely reports "build fabric" event.		
Probability:	Low		
Feature:	FOS Software	**Function:**	System Performance
Reported In Release:	FOS6.4.1	**Service Request ID:**	756411

Defect ID:	DEFECT000414360	**Technical Severity:**	High
Summary:	"Redirect zone update failed" when issuing 'cryptocfg --commit'		
Symptom:	After adding initiator to target container is performed, executing the 'cryptocfg --commit' command results in the following failure: "Operation succeeded. Commit operation completed successfully, Redirect zone update failed. Please retry commit operation." Additional attempts at commit do not result in redirect zone creation success, and container remains offline.		
Probability:	Medium		
Feature:	Data Security	**Function:**	Disk Encryption
Reported In Release:	FOS7.1.0		

Defect ID:	DEFECT000419620	**Technical Severity:**	High
Summary:	An hafailover, hareboot or firmwaredownload may cause unused ports with a ASIC register being zeroed out		
Symptom:	If frames are queued to the unused ports, credit is permanently lost and observe busy buffer condition on the port		
Probability:	Low		
Feature:	8G ASIC Driver	**Function:**	C2 ASIC driver
Reported In Release:	FOS7.0.0	**Service Request ID:**	1033850

Defect ID:	DEFECT000419937	**Technical Severity:**	High
Summary:	Fabric LOGO is not clearing out the stale FCID logins on Brocade Access Gateway. Customer is seeing "duplicate Alpa" error messages from fabric.		
Symptom:	Duplicate Alpa error message is being seen on Brocade AG when LPAR move is executed. This move re-assigns virtual WWPNs to another physical host.		
Probability:	High		
Feature:	FOS Software	**Function:**	Access Gateway
Reported In Release:	FOS6.4.2	**Service Request ID:**	1087072,1087072

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	
Probability: Medium	
Feature: FOS Software	**Function:** System Performance
Reported In Release: FOS6.4.3	**Service Request ID:** 1035482

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.	
Probability: Medium	
Feature: FOS Software	**Function:** OS: Configuration
Reported In Release: FOS6.4.2	**Service Request ID:** 1035401

Defect ID: DEFECT000422259	**Technical Severity:** High
Summary: Fabric watch daemon (fwd) triggered switch panic.	
Symptom: Switch panic after monitor of a particular frame type is installed to a larger number of ports.	
Probability: Low	
Feature: FABRIC WATCH	**Function:** Other
Reported In Release: FOS7.1.0	**Service Request ID:** ,1102396

Defect ID: DEFECT000422455	**Technical Severity:** Medium
Summary: During DWDM link failover, OLS is experienced with LOS_TOV enabled.	
Symptom: A port connected to a third party DWDM goes into 'no module' mode during DWDM failover.	
Probability: Medium	
Feature: 16G ASIC Driver	**Function:** General
Reported In Release: FOS7.0.1	

Defect ID: DEFECT000422477	**Technical Severity:** High
Summary: HBA on 5460 embedded port does not login correctly after the host is rebooted	
Symptom: Embedded switch port must be disabled/enabled once the host is fully booted to support successful HBA login.	
Probability: Medium	
Feature: FOS Software	**Function:** ASIC Driver
Reported In Release: FOS7.0.2	**Service Request ID:** 1032557

Defect ID: DEFECT000422523	**Technical Severity:** Medium
Summary: Switch in reboot loop after loading config with SSL certificate file entry and no certificate on the switch	
Symptom: Loading a configuration with an invalid ssl.certfile entry may cause the switch to reboot repeatedly.	
Workaround: Delete the csr file in /etc/fabos/certs/sw0 then reboot the switch.	
Probability: Medium	
Feature: FOS Software	**Function:** Web Management
Reported In Release: FOS7.0.2	**Service Request ID:** 1093229

Defect ID: DEFECT000423054	**Technical Severity:** High
Summary: Specifying 32 character usernames in snmpconfig causes unexpected termination of snmpd and rolling reboot	
Symptom: Termination of snmpd occurs, message [KSWD-1002] is displayed.	
Workaround: Specify usernames less than 15 characters in length.	
Probability: High	
Feature: FOS Software	**Function:** SNMP
Reported In Release: FOS6.3.2	**Service Request ID:** 1092977

Defect ID: DEFECT000424701	**Technical Severity:** Medium
Summary: portloopbacktest -nframes option does not work correctly	
Symptom: The portloobacktest -nframes option currently sends one frame at a time whereas burst capabilities are required.	
Feature: Diagnostics	**Function:** Other
Reported In Release: FOS7.1.0	

Defect ID: DEFECT000425581	**Technical Severity:** High
Summary: CRC w/ good EOF observed on ports 1/24 and 1/74 on FC8-64 in BR8510	
Symptom: CRC w/ good EOF and enc errors occurring on ports 1/34 and 1/74. FOS auto-tuning cycles through first 6 tuning value, but then blade is faulted before it can try other settings.	
Probability: Medium	
Feature: FOS Software	**Function:** ASIC Driver
Reported In Release: FOS7.0.2	**Service Request ID:** Case#1099691,Case#10

Defect ID: DEFECT000426728	**Technical Severity:** Medium
Summary: Experiencing CRC w/Good EOF errors C2-5825 on BR48000 port 5/45 with FC8-32 installed in slot 3	
Symptom: CRC with Good EOF Errors is reported on slot 5/45 when FC8-32 card is installed in slot 3 of a BR48000 system.	
Probability: Medium	
Feature: FOS Software	**Function:** ASIC Driver
Reported In Release: FOS6.4.3	**Service Request ID:** 1084752

Defect ID: DEFECT000427117	**Technical Severity:** Medium
Summary: Frimwaredownload on BR6505 is not blocked from FOSv7.0.2x to FOSv7.0.0x	
Symptom: Brocade 6505 switch is supported with FOS v7.0.1 or above. Loading pre-v7.0.1 firmware will render 6505 switch inoperable.	
Probability: High	
Feature: FIRMWARE DOWNLOAD	**Function:** Firmware Download
Reported In Release: FOS7.0.2	**Service Request ID:** ,1110373/1110326

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

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”	
Probability: Medium	
Feature: FOS Software	**Function:** Fabric Services
Reported In Release: FOS7.0.2	**Service Request ID:** 1092980

Defect ID: DEFECT000430349	**Technical Severity:** High
Summary: Due to busy BES blade processor, LUN discovery is failing	
Symptom: Host access to LUNs is lost after initiator WWNs are added to the crypto target container (CTC)	
Probability: Medium	
Feature: FOS Software	**Function:** Encryption
Reported In Release: FOS6.4.2	**Service Request ID:** 1106719