BROCADE

Software Release 12.5.02y for Brocade ServerIron ADX Series Application Delivery Controllers

Release Notes v1.0

Jul 17, 2020

Document History

Document Title	Summary of Changes	Publication Date
Software Release 12.5.02y for Brocade ServerIron ADX Application Switches v1.0	New document	Jul 10, 2020

Copyright © 2017, Brocade Communications Systems, Inc. All Rights Reserved.

Brocade, the B-wing symbol, Brocade Assurance, ADX, AnyIO, DCX, Fabric OS, FastIron, HyperEdge, ICX, MLX, MyBrocade, NetIron, OpenScript, VCS, VDX, and Vyatta are registered trademarks, and The Effortless Network and the On-Demand Data Center are trademarks of Brocade Communications Systems, Inc., in the United States and in other countries. Other brands and product names mentioned may be trademarks of others.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

The authors and Brocade Communications Systems, Inc. assume no liability or responsibility to any person or entity with respect to the accuracy of this document or any loss, cost, liability, or damages arising from the information contained herein or the computer programs that accompany it.

The product described by this document may contain open source software covered by the GNU General Public License or other open source license agreements. To find out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit https://support.hcladx.com

Contents

Summary of enhancements for 12.5.02y **8**

Treck TCP/IP Stack upgrade **8**

Summary of enhancements for 12.5.02x **9**

Enhancement in SSL rate limit **9**

Summary of enhancements for 12.5.02v **10**

Enhancement in SSH for CTR cipher support 10

Enhancement in SSL Offload **10**

Summary of enhancements for 12.5.02q **11**

Configuring the maximum connection for a virtual server and virtual port **11**

Summary of enhancements for 12.5.02n **12**

Enhancement in timeout for half-close connections **12**

Configuring the maximum connection rate for a virtual server Port **12**

Brocade ServerIron ADX Series Documentation Update **12**

Summary of enhancements for 12.5.02m **13**

Signature algorithm extension **13**

Disable weak ciphers for SSL health check **13**

License-based default system resources for tenants in Multitenancy **14**

Brocade ServerIron ADX Series Documentation Update **14**

Summary of enhancements for 12.5.02h **15**

Support of loopback as a source-interface for traffic that originates from MP for supported protocols (router code only) **15**

Brocade ServerIron ADX Series Documentation Update **15**

Summary of enhancements for 12.5.02g **16**

IPv6 support for VRRP-E pools and non-preempt mode **16**

Memory Utilization **16**

Configuring a threshold for BP heap memory utilization 16

Configuring a threshold for MP heap memory utilization 16

Hardware forwarding of pass-through traffic in DSR SLB configuration 16

Brocade ServerIron ADX Series Documentation Update 17

Summary of enhancements for 12.5.02f 18

New CLI command "show ip vrrp-e mac" 18

Using VIP IP as NAT IP 18

Brocade ServerIron ADX Series Documentation Update 18

Summary of enhancements for 12.5.02e 19

MP SSL health check stack upgrade 19

Event log file enhancements 19

GSLB XML APIs 19

Server reselection during a UDP connection in case of health check failure 19

Stateless/Fast-Stateless SLB performance optimization 20

IPv6 cache improvements 21

GSLB Cross-Controller Site Stickiness 21

Keep a sticky session on even if a health check is down. 21

Improved IPv6 traffic processing 21

Supportability feature enhancement 21

Brocade ServerIron ADX Series Documentation Update 22

Summary of enhancements for 12.5.02d 23

Perfect-Forward-Secrecy and additional SSL cipher-suite support 23

TLS Server Name Indication 23

Brocade ServerIron ADX Series Documentation Update 23

Summary of enhancements for 12.5.02c **24**

TRL (Transaction Rate Limit) enhancements **24**

Delayed VRRP-e failover **24**

Management Processor CPU traffic rate limiting enhancement **24**

Source-interface support for DNS and SNTP traffic originated from MP (Management Processor) **24**

Auto-clearing of GSLB selection counters **25**

Displaying order numbers and metric statistics for domain IP addresses **25**

CLI history enhancement **25**

Summary of enhancements for 12.5.02a **26**

SSL protocol version selection **26**

Summary of enhancements for 12.5.02 ..... **27**

GSLB Enhancements **27**

OpenScript Enhancements **28**

High Availability (HA) enhancements **28**

Other enhancements **28**

Software image files for ServerIron ADX release 12.5.02y **29**

Embedded Boot Image **29**

Notes **29**

Factory Pre-Loaded Software **30**

Additional information **31**

Requirements for Running the ServerIron ADX WEB GUI Interface **31**

Qualified USB Drives with the Release **31**

Supporting Documentation for ServerIron ADX release 12.5.02 ..... **31**

Technical Support **32**

Upgrading an ADX system with a single management module **33**

Upgrading an ADX System with dual management modules **34**

Defects closed with code in ServerIron ADX 12.5.02y **35**

Defects closed with code in ServerIron ADX 12.5.02x **36**

Defects closed with code in ServerIron ADX 12.5.02w **37**

Defects closed with code in ServerIron ADX 12.5.02v **38**

Defects closed with code in ServerIron ADX 12.5.02u **39**

Defects closed with code in ServerIron ADX 12.5.02t **41**

Defects closed with code in ServerIron ADX 12.5.02s **42**

Defects closed with code in ServerIron ADX 12.5.02r **44**

Defects closed with code in ServerIron ADX 12.5.02q **46**

Defects closed with code in ServerIron ADX 12.5.02p **48**

Defects closed with code in ServerIron ADX 12.5.02n **50**

Defects closed with code in ServerIron ADX 12.5.02m **55**

Defects closed with code in ServerIron ADX 12.5.02k **61**

Defects closed with code in ServerIron ADX 12.5.02j **62**

Defects closed with code in ServerIron ADX 12.5.02h **67**

Defects closed with code in ServerIron ADX 12.5.02g **70**

Defects closed with code in ServerIron ADX 12.5.02f **76**

Defects closed with code in ServerIron ADX 12.5.02e **82**

Defects closed with code in ServerIron ADX 12.5.02d **86**

Defects closed with code in ServerIron ADX 12.5.02c **91**

Defects closed with code in ServerIron ADX 12.5.02b **103**

Defects closed with code in ServerIron ADX 12.5.02a **105**

Defects closed with code in ServerIron ADX 12.5.02 ..... **106**

Defects closed without code in ServerIron ADX 12.5.02 ..... **111**

Open Defects in ServerIron ADX 12.5.02 ..... **113**

Summary of enhancements for 12.5.02y

The Brocade ServerIron ADX software release 12.5.02y includes the following new feature and several defect fixes.

Treck TCP/IP Stack upgrade

The ServerIron ADX 12.5.02y patch release provides fixes for the following latest reported Treck CVE's.

CVE ID
CVE-2020-11899
CVE-2020-11900
CVE-2020-11902
CVE-2020-11904
CVE-2020-11906
CVE-2020-11909
CVE-2020-11910
CVE-2020-11911
CVE-2020-11912
CVE-2020-11913
CVE-2020-11914

The below mentioned CVE's are already fixed in prior release from 12502y.

CVE ID
CVE-2020-11896
CVE-2020-11897
CVE-2020-11898
CVE-2020-11907
CVE-2020-11908

The below mentioned CVE's are not applicable to ADX products.

CVE ID
CVE-2020-11901
CVE-2020-11903
CVE-2020-11905

Summary of enhancements for 12.5.02x

The Brocade ServerIron ADX software release 12.5.02x includes the following new feature and several defect fixes.

Enhancement in SSL rate limit

The ServerIron ADX 12.5.02x patch release provides support for rate limit the SSL traffic. The feature was introduced to control SSL traffic which is measured by Cavium pending count.

This feature is disabled by default. Once it is enabled and average cavium pending count is continuously greater than "rate-limit" for 5 seconds, new SSL session will start dropping; however already established SSL session will continue to handle traffic. Once Cavium pending count comes below rate-limit, device will accept all new sessions.

A new CLI commands, as below, is introduced in this enhancement.

```
ServerIronADX(config)# ssl rate-limit enable <Cavium max drop count [1-30]>
```

Syntax: [no] ssl rate-limit enable *<Cavium max drop count [1-30]>*

The *<Cavium max drop count [1-30]>* parameter specifies the maximum drop count for cavium core. The value ranges from 1 through 30.

Summary of enhancements for 12.5.02v

The Brocade ServerIron ADX software release 12.5.02v includes the following new features and several defect fixes.

Enhancement in SSH for CTR cipher support

The ServerIron ADX 12.5.02v patch release provides support for CTR cipher in SSH. A new CLI commands, as below, is introduced in this enhancement.

```
ServerIronADX(config)# ip ssh encryption aes-only
```

Syntax: [no] ip ssh encryption aes-only

The above command is used for enable the AES based encryption ciphers and disable the 3DES-CBC cipher.

```
ServerIronADX(config)# ip ssh encryption
```

Syntax: [no] ip ssh encryption disable-aes-cbc

The above command is used for enable the strong CTR cipher and disable all other weak encryption ciphers.

NOTE: This feature is not supported for webgui.

Enhancement in SSL Offload

The ServerIron ADX 12.5.02v patch release provides support for offload ECC cipher traffic from cavium to openssl. A new CLI commands, as below, is introduced in this enhancement.

```
ServerIronADX(config)# ssl ecc-offload-ratio 19 19
```

Syntax: [no] ssl ecc-offload-ratio *<ECC CAVIUM ratio> <ECC BP ratio>*

The *<ECC CAVIUM ratio>* parameter specifies the offload ratio of cavium. The value ranges from 0 through 90. The *<ECC BP ratio>* parameter specifies the offload ratio of BP. The value ranges from 0 through 90. Device reload required to take effect in ServerIronADX.

Summary of enhancements for 12.5.02q

The Brocade ServerIron ADX software release 12.5.02q includes the following new features and several defect fixes.

Configuring the maximum connection for a virtual server and virtual port

The ServerIron ADX 12.5.02q patch release allows you to specify the maximum number of TCP connections allowed for virtual server and virtual server port.
The ServerIron ADX monitors the traffic conditions and rejects new connections to a specific TCP server or port when the connection exceeds the limit specified.

Use the **max-conn** command, to limit the number of new TCP connections that a virtual server can receive.
The below example shows how to limit new TCP connections to the server to 3000 connections.

```
ServerIronADX 1000(config)# server virtual-name-or-ip vs1 x.x.x.x
ServerIronADX 1000(config-vs-vs1)# max-conn 3000
```

Syntax: max-conn *num*

The <*num*> parameter specifies the maximum number of connections. The value ranges from 1 through 2000000.

Use the **show server virtual** command to display the VIP TCP connection.

Use the **port** <*num*|*name*> **max-conn** command, to limit the number of new TCP connections that a virtual server port can receive.
The below example shows how to limit new TCP connections to the specific application port to 3000 connections.

```
ServerIronADX 1000(config)# server virtual-name-or-ip vs1 x.x.x.x
ServerIronADX 1000(config-vs-vs1)# port http max-conn 3000
```

Syntax: port <*num*|*name*> **max-conn** *num*

The <*num*|*name*> parameter specifies the port number or the port name.
The <*num*> parameter specifies the maximum number of connections. The value ranges from 1 through 2000000.

Summary of enhancements for 12.5.02n

The Brocade ServerIron ADX software release 12.5.02n includes the following new features and several defect fixes.

Enhancement in timeout for half-close connections

The ServerIron ADX 12.5.02n patch release provides support to remove the half-closed connections in a specified time (seconds). A new CLI command, as below, is introduced to support this enhancement.

```
ServerIronADX(config)# ip tcp half-close-conn-timeout 10
```

Syntax: [no] ip tcp half-close-conn-timeout *value*

The <*value*> parameter specifies the timeout for the half-close connections. The value ranges from 1 through 300 seconds. The default timeout is 300 seconds.

Configuring the maximum connection rate for a virtual server Port

The ServerIron ADX 12.5.02n patch release allows you to specify the maximum rate of TCP connection allowed for virtual server port.

The ServerIron ADX monitors the traffic conditions and rejects new connections to a specific TCP port when the connection rate exceeds the limit.

Use the **port** <*num*|*name*> **max-tcp-conn-rate** command, to limit the number of new TCP connections that a virtual server port can receive per second.

The below example shows how to limit new TCP connections to the server to 2000 per second.

```
Virtual ADX(config)# server virtual-name-or-ip vs2 x.x.x.x

Virtual ADX(config-vs-vs2)# port http max-tcp-conn-rate 2000
```

Syntax: port <*num*|*name*> **max-tcp-conn-rate** *num*

The **port** <*num*|*name*> parameter specifies the port number or the port name.

The <*num*> parameter specifies the maximum number of connections per second. The value ranges from 1 through 4294967295.

Brocade ServerIron ADX Series Documentation Update

This documentation guide contains the updates for the various feature enhancements made in the Brocade ServerIron ADX releases all the way to 12.5.02n. The information regarding these updates will be added to the documentation guides and made available with the next major release of the Brocade ServerIron ADX. The documentation guide with Brocade ServerIron ADX release 12.5.02n update is the:

- Brocade ServerIron ADX Server Load Balancing Guide

Summary of enhancements for 12.5.02m

The Brocade ServerIron ADX software release 12.5.02m includes the following new features and several defect fixes.

Signature algorithm extension

The ServerIron ADX 12.5.02m patch release provides support for signature algorithm extension in SSL Client Hello for data traffic, simple health check, and complete health check.

Below is a snapshot of the signature algorithm.

```
⊟ Extension: signature_algorithms
    Type: signature_algorithms (0x000d)
    Length: 32
    Signature Hash Algorithms Length: 30
  ⊟ Signature Hash Algorithms (15 algorithms)
    ⊟ Signature Hash Algorithm: 0x0601
        Signature Hash Algorithm Hash: SHA512 (6)
        Signature Hash Algorithm Signature: RSA (1)
    ⊞ Signature Hash Algorithm: 0x0602
    ⊞ Signature Hash Algorithm: 0x0603
    ⊞ Signature Hash Algorithm: 0x0501
    ⊟ Signature Hash Algorithm: 0x0502
        Signature Hash Algorithm Hash: SHA384 (5)
        Signature Hash Algorithm Signature: DSA (2)
    ⊞ Signature Hash Algorithm: 0x0503
    ⊞ Signature Hash Algorithm: 0x0401
    ⊞ Signature Hash Algorithm: 0x0402
    ⊟ Signature Hash Algorithm: 0x0403
        Signature Hash Algorithm Hash: SHA256 (4)
        Signature Hash Algorithm Signature: ECDSA (3)
    ⊟ Signature Hash Algorithm: 0x0301
        Signature Hash Algorithm Hash: SHA224 (3)
        Signature Hash Algorithm Signature: RSA (1)
    ⊞ Signature Hash Algorithm: 0x0302
    ⊞ Signature Hash Algorithm: 0x0303
    ⊞ Signature Hash Algorithm: 0x0201
    ⊟ Signature Hash Algorithm: 0x0202
        Signature Hash Algorithm Hash: SHA1 (2)
        Signature Hash Algorithm Signature: DSA (2)
    ⊞ Signature Hash Algorithm: 0x0203
```

Disable weak ciphers for SSL health check

The ServerIron ADX 12.5.02m patch release provides support to disable weaker ciphers while performing simple and complete SSL health check. A new CLI command, as below, is introduced to support this enhancement.

Syntax: server ssl disable-weak-ciphers-ssl-hc

It is not desirable, to disable the above command to have strong ciphers but in case you need to enable weak-ciphers, the below command can be used.

Syntax: [no] server ssl disable-weak-ciphers-ssl-hc (default)

License-based default system resource:es for tenants in Multitenancy:

The ServerIron ADX 12.5.02m patch release assigns the default value of the system resource for the CLI parameter *source-ip* based on the license type instead of chassis type. ServerIron ADX 10000 supports two types of licenses, Tier1 and Tier2. ServerIron ADX 4000 supports the Tier1 license. Following are the new default values for the CLI parameter *source-ip*.

Network Limit	CLI Parameter	Description	ServerIron ADX 1000	ServerIron ADX 4000	ServerIron ADX 10000
Source IPs	source-ip	The maximum number of source IP addresses supported.	Valid range: 0 – 128. Default value: 8	Valid range: 0 – 128. Default value: 8 with Tier1 license	Valid range: 0 – 128. Default value: 8 with Tier1 license. 4 with Tier2 license

Brocade ServerIron ADX Series Documentation Update

This documentation guide contains the updates for the various feature enhancements made in the Brocade ServerIron ADX releases all the way to 12.5.02m. The information regarding these updates will be added to the documentation guides and made available with the next major release of the Brocade ServerIron ADX. The documentation guide with Brocade ServerIron ADX release 12.5.02m update is the:

- Brocade ServerIron ADX Multitenancy Guide

Summary of enhancements for 12.5.02h

The Brocade ServerIron ADX software release 12.5.02h includes the following new feature, useful enhancement and several defect fixes.

Support of loopback as a source-interface for traffic that originates from MP for supported protocols (router code only)

Starting with the ServerIron ADX 12.5.02h patch release, users can select loopback as a source-interface for traffic that originates from Management Processor (MP) by using the following CLI command. DNS, RADIUS, TACACS, TFTP, Telnet, SNTP, SSH, and SYSLOG traffic support the loopback source interface.

The syntax of the command follows:

ip <*protocol*> source-interface [loopback <x>|Ethernet <x/x>|mgmt1|ve <x>]

logging source-interface [loopback <x>|Ethernet <x/x>|mgmt1|ve <x>]

Note: Support for loopback as a source-interface was removed starting with 12.5.02d patch release.

Brocade ServerIron ADX Series Documentation Update

This documentation guide contains the updates for the various feature enhancements made in the Brocade ServerIron ADX releases all the way to 12.5.02h. The information regarding these updates will be added to the documentation guides and made available with the next major release of the Brocade ServerIron ADX. The documentation guide with Brocade ServerIron ADX release 12.5.02h update is the:

- Brocade ServerIron ADX Administration Guide

Summary of enhancements for 12.5.02g

The Brocade ServerIron ADX software release 12.5.02g includes the following new feature, useful enhancement and several defect fixes.

IPv6 support for VRRP-E pools and non-preempt mode

A VRRP backup device with a higher priority can preempt a VRRP master with a lower priority and assume the role of the master. This behavior can be avoided by disabling preemption. Preemption applies only to backup devices and takes effect only when the master fails; the backup assumes ownership of the VRID.

Pools are defined to attach dependent VRRP instances. You can add VRRP instances for each container. Adding VRIDs to a container ensures that all VRIDs within the container track all other ports that are tracked by a VRID in the container. A container also ensures that if a VRID in the container has non- preempt mode configured, all the VRRP instances in the container are in +-preempt mode.

Memory Utilization

This section describes the monitoring of heap memory utilization for barrel processors (BP) and management processors (MP).

Configuring a threshold for BP heap memory utilization

In this release, the **bp-memory-util-threshold** command is introduced that allows you to configure the threshold, expressed as a percentage, for BP heap memory utilization.

```
ServerIronADX(config)# bp-memory-util-threshold 80
```

Syntax: bp-memory-util-threshold <integer>

The <integer> parameter specifies the threshold percentage that ranges from 1 through

100.

Configuring a threshold for MP heap memory utilization

In this release, the **mp-memory-util-threshold** command is introduced that allows you to configure the threshold, expressed as a percentage, for MP heap memory utilization.

```
ServerIronADX(config)# mp-memory-util-threshold 80
```

Syntax: mp-memory-util-threshold <integer>

The <integer> parameter specifies the threshold percentage that ranges from 1 through 100.

Hardware forwarding of pass-through traffic in DSR SLB configuration

Traffic originating from an interface IP address of a Direct Server Return (DSR) that flows through ServerIron ADX is processed by application CPUs. With the existing hardware-forwarding feature (server hw-fwd-pass-through-traffic), traffic with an L4 source port-matching SLB real port is forwarded by application CPUs and other traffic is hardware-forwarded. As reverse SLB traffic always originates from loopback (ServerIron ADX's virtual server) IPs in a DSR SLB configuration, it is not necessary to process traffic from interface IPs of servers by application CPUs. This behavior can cause inefficient use of CPUs when such traffic is high.

Starting with the ServerIron ADX 12.5.02g patch release, traffic distribution rules on ServerIron ADX are enhanced such that any traffic originating from an interface IP address of a DSR server is hardware forwarded instead of CPU processed. This enhancement ensures efficient use of application CPUs when traffic from interface IPs of DSR servers is high.

To enable this enhancement, use the following command at the global configuration level:

```
ServerIronADX(config)# server dsr-cam-optimization
```

Syntax: [no] server dsr-cam-optimization

NOTE: This enhancement can be used only when all the SLB virtual servers and ports are enabled with DSR and is supported in both L2 and L3 DSR configurations.

Brocade ServerIron ADX Series Documentation Update

This documentation guide contains the updates for the various feature enhancements made in the Brocade ServerIron ADX releases all the way to 12.5.02g. The information regarding these updates will be added to the documentation guides and made available with the next major release of the Brocade ServerIron ADX. The documentation guide with Brocade ServerIron ADX release 12.5.02g update is the:

- ServerIron ADX SLB Guide
- ServerIron ADX Security Guide
- ServerIron ADX Switch and Router Guide

Summary of enhancements for 12.5.02f

The Brocade ServerIron ADX software release 12.5.02f includes the following new feature, useful enhancement and several defect fixes.

New CLI command "show ip vrrp-e mac"

In this release, the **show ip vrrp-e mac** command is introduced that will display the VRRP-e flags in the Brocade ServerIron ADX MP and BP modules. The command also displays the static and Layer-3 flags from each Line card. The following use and syntax of the command is shown below:

```
ServerIronADX# show ip vrrp-e mac
```

Syntax: show ip vrrp-e mac

The fields in the output display includes: Interface = Interface ID; VRID = VRID; State = MP state (Master/Backup); MAC = interface MAC address; MP flag = vrrp flag on the MP (Vrrp/Partner_vrrp); BP Flag = vrrp flag on the BP (Vrrp/Partner_vrrp); and the HW flags: STATIC = static bit on the Line card (Static/Dynamic) and L3 = the L3 bit on the Line card (L3/None).

Using VIP IP as NAT IP

IP NAT is not supported for clients other than real or remote servers when using the same IP address for NAT Pool and virtual server. If you need to enable the IP NAT for clients other than real or remote servers, you will need to define different NAT pool names and different pool IP addresses.

Brocade ServerIron ADX Series Documentation Update

This documentation guide contains the updates for the various feature enhancements made in the Brocade ServerIron ADX releases all the way to 12.5.02f. The information regarding these updates will be added to the documentation guides and made available with the next major release of the Brocade ServerIron ADX. The documentation guide with Brocade ServerIron ADX release 12.5.02f update is the:

- ServerIron ADX SLB Guide
- ServerIron ADX Security Guide

Summary of enhancements for 12.5.02e

The Brocade ServerIron ADX software release 12.5.02e includes the following new features, useful enhancements and several defect fixes.

MP SSL health check stack upgrade

The SSL health check stack on the Brocade ServerIron ADX Management Processor (MP) has been upgraded to allow support for the new stronger SSL cipher suites, the protocol TLS 1.2, and all other available security feature enhancements.

Then upgrade to the ServerIron ADX MP will have no impact on other MP modules (like the certificate management, OCSP and other modules) which are dependent and/or are using the MP SSL health check stack.

Event log file enhancements

Previous to this release, the Brocade ServerIron ADX event log file has a set default maximum size of 32MB and the user could change it within ranges 32MB and 256MB. With the release of 12.5.02e, the user can now change the event log file size with valid ranges of 16MB to 256MB, with the default maximum size being 256MB.

To configure the event log file size, use the following command:

```
ServerIronADX(config)# eventlog size 64
```

Syntax: [no] eventlog size <value in MB>

In addition, the event log has been enhanced to allow storing the event log files in multiples of 16MB sizes instead of storing in one big eventlog.txt file.

GSLB XML APIs

Starting with release 12.5.02e, the Brocade ServerIron ADX supports the GSLB XML APIs that are grouped as follows:

- Secure GSLB API
- Affinity APIs
- ActiveRTT APIs

The GSLB XML APIs supported contains all the methods and data structures used to create and configure GSLB.

Server reselection during a UDP connection in case of health check failure

Prior to this release, the Brocade ServerIron ADX drops packets on an existing UDP connection with port sticky configuration in SLB optimized mode, if the original server failed Layer2 or Layer3 health checks. In case of SLB non-optimized mode, the ServerIron ADX drops packets if the original server failed Layer2 or Layer3 or Layer4 or Layer7 health checks. In both these cases, sticky sessions will be preserved and flow sessions will be deleted.

With the 12.5.02e release, the ServerIron ADX has a configuration option to select a new server for an existing UDP connection in case of Layer2 or Layer3 health check failure in SLB optimized mode, and Layer2 or Layer3 or Layer4 or Layer7 health check failure in SLB non-optimized mode. Once a new healthy server is selected, the ServerIron ADX will update the flow and sticky sessions with the new server. The incoming packet is forwarded to the new server rather than it being dropped. This enhancement is enabled using the global command "**server switch-on-failure**".

The server reselection enhancement is applicable only with the ServerIron ADX port sticky configuration and is not applicable with other sticky features like client-subnet-sticky, group-sticky etc. This enhancement is only applicable for UDP traffic and has no effect on TCP traffic.

Stateless/Fast-Stateless SLB performance optimization

Stateless/Fast-Stateless SLB has been optimized for performance by a factor of three (3). Performance improvement on existing Brocade ServerIron ADX hardware:

- Up to 3x improvement in IPv6 DNS query rate.

IPv6 cache improvements

The software release 12.5.02e enables the Brocade ServerIron ADX to cache IPv6 destination information more intelligently. With this release, IPv6 cache entries are either retained or deleted based on the cache-hit and cache-miss parameters.

GSLB Cross-Controller Site Stickiness

The global server load balancing (GSLB) feature set on the ServerIron ADX devices helps you manage traffic efficiently across geographically dispersed data centers. The software release 12.5.02e introduces a new capability that enables site-based stickiness across a cluster of GSLB controllers. This feature is enabled using the following command:

```
ServerIronADX(config-gslb-policy)# site-sticky
CL1 Syntax: [no] site-sticky <cluster-name>
```

After you execute the site-sticky command on a cluster, every DNS request directed to domains with site sticky enabled from a client will always be checked. This is to see if a similar DNS request from the same client has previously returned an IP from any of the GSLB sites. If the check finds a match, the IP from the same GSLB sites will be returned to the new DNS request regardless of the requested domain name. If no match, the IP returned to the DNS request will be based on the other configured GSLB policies. Once the new DNS request is handled by a controller, the information (which includes the client IP, requested domain name, returned best IP, and site information for the returned best IP) will be captured and shared across the controllers to make sure that all subsequent DNS requests from the same client are returned an IP from the same GSLB site the DNS request was initiated.

For scenarios where the ServerIron ADX devices are deployed behind NAT devices, then the mapping of ServerIron ADX cluster IP addresses and NAT IP addresses are maintained by using the following command:

```
ServerIronADX(config-cluster-CL1)# ip ADX-1 192.168.10.25 use
192.168.10.35 Syntax: [no] ip [<device-name>] <ip> [use <nat ip>]
```

Keep a sticky session on even if a health check is down.

The addition of a new command allows you to keep a sticky session on in a session table even if a health check is down. To do so, enter the following command. This is useful when you have HA configurations and you want to maintain the session with another available real server.

```
ServerIronADX(config)# server allow-sticky health-check-
down Syntax: [no] server allow-sticky health-check-down
```

After you execute the command, when the ServerIron ADX receives a pac10ket which matches the sticky session, the sticky session will be updated to the next available real server at that time due to health check being down. By default, the ServerIron ADX ages out the session within one minute (it depends on a configuration of sticky multiplier) after a health check is down. When a health check goes down on only a standby ServerIron ADX, the standby ServerIron ADX ages out the session within one minute while the active ServerIron ADX keeps the session. When an HA failover occurs, a new Active ServerIron ADX may not have the sticky session and may forward the packet to a different real server even after the health check is up again. The command takes effect immediately.

Improved IPv6 traffic processing

The release 12.5.02e allows for seamless processing of IPv6 traffic while attack prevention is enabled on the ServerIron ADX against several Denial of Service attacks.

Supportability feature enhancement

Starting with release 12.5.02e, a new command has been added to enhance the supportability of the Brocade ServerIron ADX.

Users can use this single command along with a file comprising the desired CLI commands listed in a given format in order to collect and gather the outputs and save in a file. This command internally works similar to the **save tech-support** command which allows users to easily collect and save specific and relevant information in the diagnosis of a problem. The save process customization involves the user providing the command file that allows a maximum of 100 CLI commands to be executed and saved on the file. The commands supported are mainly **show** commands.

To use this enhancement, the following CLI command is used:

```
Syntax: save use-cmd-file <cmd-file-path> text|html <output-file-path>
```

The <cmd-file-path> parameter specifies the path and name of the command file.
The text|html parameter specifies the path and name of the command file.
The <output-file-path> is an optional parameter specifies the path and name of the output file.

Each line in the input file will fall into one of the following categories:

- a comment line: if the line starts with “#” or “//”

a command line: if it doesn’t qualify as a comment line

A command line is either for the Management CPU (MP) or the Application CPU (BP). If the command is for the BP, it should start with "bps: "or "bp <asm#> <bp#>:" Otherwise it is considered an MP command, and the entire line is the command. Examples are given below:

```
bps: show server virtual      ➔ applies to all BPs
bp 1 1: show server virtual   ➔ applies to only BP 1/1
```

Note: (As usual, the index of asm# and bp# starts from 1.)
An example command file is shown below:

```
show clock
show version
bps: show cpu
#bp 1 3:asm show ver
//bp 1 2:asm show ver
bp 1 1:asm show ver
bps:show cpu
bps:show cpu
bp 1 3:asm dm cput sh util-s
bp 1 2:asm dm cput sh util-s
bp 1 1:asm dm cput sh util-s
#bp 1 1:show cpu
```

This command is mainly for Brocade TAC use and will most likely be advised by them to ServerIron ADX users. This allows the collection of certain CLI command outputs and the saving of the outputs in a single file during the time of the issue in order to resolve critical and complex problem. The output file generated with this command can be used to give additional outputs needed on top of the output file generated with "save tech-support" command.

Note: It is recommended and advised that the command syntax be tested on respective CLI such as Application CPU and Management CPU console before using it in the cmd-file.

Brocade ServerIron ADX Series Documentation Update

This documentation guide contains the updates for the various feature enhancements made in the Brocade ServerIron ADX releases all the way to 12.5.02e. The information regarding these updates will be added to the documentation guides and made available with the next major release of the Brocade ServerIron ADX. The documentation guide with Brocade ServerIron ADX release 12.5.02e updates is the:

- ServerIron ADX Security Guide
- XML API Programmer's Guide

Summary of enhancements for 12.5.02d

The Brocade ServerIron ADX software release 12.5.02d includes these useful enhancements and several defect fixes.

Perfect-Forward-Secrecy and additional SSL cipher-suite support

Before this 12.5.02d release, the SSL feature of the Brocade ServerIron ADX supported only RSA public-key infrastructure in which the same key is used for both authentication and encryption. A single key can be used for many SSL sessions; however, compromise of one SSL session could, in turn, lead to the compromise of other SSL sessions. To prevent compromise of SSL sessions from occurring, the ServerIron ADX provides Perfect Forward Secrecy (PFS) for SSL by adding multiple stronger cipher suites under the SSL profile configuration.

The Brocade ServerIron ADX 12.5.02d release supports new cipher suites in SSL-Terminate and SSL-Proxy modes with key sizes of 512, 1024, and 2048 bytes. These cipher-suites can be selectively enabled/disabled in the SSL profile configuration.

TLS Server Name Indication

Previous to the 12.5.02d release, there was no provision in the SSL protocol supported by the Brocade ServerIron ADX to pass the server's domain information prior to the secure connection establishment. Using the same certificate across multiple domains could result in client browsers warning users of certificate mismatch, or blocked SSL connections (as part of the web browser security measures) against Man-In-The-Middle attacks.

Starting with the 12.5.02d release, SSL protocol on the ServerIron ADX application traffic supports Server-Name-Indication (SNI) to eliminate this from occurring.

Brocade ServerIron ADX Series Documentation Update

This documentation guide contains the updates for the various feature enhancements made in the Brocade ServerIron ADX releases all the way to 12.5.02d. The information regarding these updates will be added to the documentation guides and made available with the next major release of the Brocade ServerIron ADX. The documentation guide with Brocade ServerIron ADX release 12.5.02d updates is the:

- ServerIron ADX Security Guide

Summary of enhancements for 12.5.02c

The Brocade ServerIron ADX software release 12.5.02c includes these useful enhancements and several defect fixes.

TRL (Transaction Rate Limit) enhancements

Starting with release 12.5.02c, Client and Global TRL features are supported for IPv6 ICMP traffic.

With the release 12.5.02c, configuration of Client TRL on Virtual Servers is simplified in such a way that users no longer need to provide protocol and port information on the ingress interfaces (example: “ip tcp/udp trans-rate <port>, “ip icmp trans-rate”). This enhancement is not applicable for Client TRL for pass through traffic and Global TRL features, and users still need to provide IP protocol and L4 port information on ingress interfaces.

Delayed VRRP-e failover

With this release, users of the Brocade ServerIron ADX can configure an option to delay VRRP-e failover by a certain period (in seconds) under VRRP-e configuration using the command **delayed-failover <x>**. The delayed failover will be applicable only when the ServerIron ADX running VRRP-e is transitioning from Backup to Master, as a result of VRRP-e interface/track-port UP event. In all other cases where a ServerIron ADX transitions from VRRP-e backup to master, delayed failover will be ignored, for example, when VRRP-e backup priority is increased manually or when a disabled VRRP-e VRID is enabled. This feature is configured using the following example and syntax:

```
ADX(config)# interface ve 12
ADX(config-vif-12)# ip vrrp-extended vrid 1
ADX(config-vif-12-vrid-1)# delayed-failover 10
Syntax: [no] delayed-failover <x>
```

The <x> variable is the delayed failover time in seconds. By default, this feature is disabled, i.e. VRRP-e failover will happen in the normal way.

NOTE: Users need to configure the VRRP-e backup priority value to greater than 20 in order to use this feature.

Management Processor CPU traffic rate limiting enhancement

Starting with release 12.5.02c, when users enable MP CPU traffic rate limiting feature for ICMP traffic, ServerIron ADX will rate limit ICMP Echo Requests only and all other ICMP traffic including Echo Replies will be excluded from rate limiting. With this enhancement, customers can use traffic rate limiting feature for ICMP without affecting ICMP health check (Echo Replies) traffic from real/remote servers.

Source-interface support for DNS and SNTP traffic originated from MP (Management Processor)

Starting with release 12.5.02c, users can select a source-interface (Ethernet or VE or Management) for DNS and SNTP traffic originated from MP using the following CLI. Prior to 12.5.02c release, source-interface support was only available for RADIUS, TACACS, TFTP, SNMP, Telnet, SSH and SYSLOG traffic.

Auto-clearing of GSLB selection counters

With this enhancement, when a previously-failed GSLB site is recovered or a new GSLB site is added, the internal counters for GSLB site selection are automatically cleared. This protects newly available site from receiving all traffic when any one of the weighted GSLB metrics are in use.

Displaying order numbers and metric statistics for domain IP addresses

The release 12.5.02c adds these useful enhancements to the ServerIron ADX **show gslb dns detail** command:

- New GSLB 'Order' metric: The new 'Order' metric helps achieve two objectives -
  1. Simple specification of site priority order: The administrators managing large infrastructures involving multiple GSLB sites can easily define primary, secondary, tertiary and follow-on site priorities using 'Order' metric.
  2. Easy shut down of site for maintenance purposes: If 'Order' metric is followed right after 'health check' metric in GSLB metric-order configuration, then a site can be brought down simply by setting its Order value to zero. The GSLB site with order value of zero will not get selected for any subsequent traffic requests.
- Enriched GSLB show command: Displays selection metric counter for sites that are hosted on non-Brocade application delivery controllers.

CLI history enhancement

Prior to software release 12.5.02c, CLI history on the Brocade ServerIron ADX displayed all commands entered by the user including the incomplete commands. Starting with release 12.5.02c, users can configure the ServerIron ADX to display CLI history with only complete and executed commands.

The command to enable the CLI history enhancement is:

```
Syntax: [no] cli-validate-cmd-history
```

Summary of enhancements for 12.5.02a

The Brocade ServerIron ADX software release 12.5.02a includes the following important feature enhancement:

SSL protocol version selection

With this release, users of the Brocade ServerIron ADX can enable and disable specific versions of SSL protocol as part of the SSL offloading functionality. Additionally, this release provides the users access to the version-specific incoming and denied SSL connection statistics for further analysis. The following command is introduced under the SSL profile configuration for this enhancement:

To disable an SSL protocol version:

```
ServerIronADX(config)# ssl profile test
ServerIronADX(config-ssl-profile-test)# disable tls1
```

Syntax: [no] disable < ssl2 | ssl3 | tls1 | tls1_1 | tls1_2 >

Additional notes about the **SSL protocol version selection** in this release:

- SSL2.0 and SSL3.0 is disabled by default when SSL profile is created. In previous releases, only SSL2.0 was disabled by default.
- The legacy “enable-ssl-v2” command is now obsolete. Existing configuration with this command will be translated to the new command “no disable ssl2” after upgrade.

Summary of enhancements for 12.5.02

The Brocade ServerIron ADX software release 12.5.02 is based on the software release 12.5.01e and includes the following important feature enhancements:

GSLB Enhancements

The Brocade ServerIron ADX global server load balancing (GSLB) functionality enables customers to optimally distribute traffic and provide disaster recovery and business continuity mechanisms to applications hosted across multiple data centers. The software release 12.5.02 adds these two useful enhancements to the GSLB functionality:

- **Secure GSLB using OpenSSL**: The release now supports a maximum of 2048-bit SSL key size from the previous maximum of 1024-bit key size.
- **Increasing GSLB zones from 1000 to 4000**: The release now supports up to 4000 DNS zones, hosts, and applications; and up to 8000 DNS IP addresses. If there is a mismatch between site ServerIron ADX and GSLB Controller software releases, there will be no impact on these features, however, the scalability numbers would be driven by the software release running on the GSLB controller.

OpenScript Enhancements

The OpenScript functionality on the ServerIron ADX provides additional set of APIs to programmatically define policies. The software release 12.5.02 comes with the following new OpenScript module capabilities:

- **OpenScript APIs for parsing SSL certificates**: The OpenScript module comes with new set of APIs that provides insights into an SSL certificate used in establishing a secure connection between a client and the ServerIron ADX. These APIs enable users to define actions based on the SSL certificate fields. For example, a user can define OpenScript-based policy to trigger certain actions, such as logging or resetting of a connection, based on the "OU" field in the certificate. This release supports the SSL certificate fields – Common Name (CN), LocalityName (L), StateorProvinceName (SR), OrganizationName (O), OrganizationUnitName (OU), CountryName ©, StreetAddress (STREET), DomainComponent (DC), and Userid (UID).

- **OpenScript load balancing based on HTTP payload:** Users can define specific actions, such as forward, log, and reset, based on specific information available in the HTTP payload. Since the payload can be encapsulated across multiple packets, the overall latency of the connection is impacted and it can reside anywhere in the payload. To optimize the feature performance, the following options are provided as part of this enhancement:
    - Wait till the whole payload is received,
    - Wait for certain number of packets is received, or
    - Wait for no content to be received

High Availability (HA) enhancements

Many of the mission critical applications rely on load balancers to provide continuous availability of the applications to their end users. The Brocade ServerIron ADX fulfills this responsibility through high availability (HA) functionality. The software release 12.5.02 adds the following important enhancements to the Brocade ServerIron ADX HA capabilities:

- **Increase the number of symmetric HA groups to 255**

- **Simplified symmetric HA failover:** Prior to 12.5.02 release, the Brocade ServerIron ADX deployed in a symmetric HA mode, cannot be upgraded without configuration changes or disabling of ports. This process is very inconvenient, cumbersome and in some instances tricky to manage without causing any network disruptions. With the release of 12.5.02, the user can force an active Brocade ServerIron ADX to failover to its backup node in a symmetric setup using a single command. This forced failover effectively frees up the device for upgrade or maintenance purposes. This command is available both at the CLI exec and config level, however, if the command is executed at the exec level, then it is not saved. To save the command before reload, execute the command at the config level followed by a "write mem".

Other enhancements

The Brocade ServerIron ADX software release 12.5.02 includes the following important feature enhancements:

- **SSL feature includes support for protocol versions TLS 1.1 and TLS 1.2**

- **IPv6 Clients support for maximum concurrent connection feature**: IPv6 clients are now supported for the maximum concurrent connection per client feature of the Brocade ServerIron ADX.

- **L7 health check for RADIUS accounting**: This release adds support to RADIUS accounting health check on the Brocade ServerIron ADX. Now the user can configure RADUIS accounting health check or both RADIUS authentication and RADIUS accounting health checks.

- **SSL Health check Enhancements:** This release enables Brocade ServerIron ADX to support new cipher algorithms as part of the SSL health checks. Similar to client-server SSL traffic, health checks based on SSL tunnel provide additional security between the ServerIron ADX and back end real server. With this release, ServerIron ADX would be able to successfully establish SSL health checks using following AES ciphers, configured both in simple and complete SSL health check modes.

  TLS_RSA_WITH_AES_256_CBC_SHA' - AES cipher algorithm using 256 bit key size
  'TLS_RSA_WITH_AES_128_CBC_SHA' - AES cipher algorithm using 128 bit key size

- **Decoupling the name of VIP from the IP address of VIP:** With the release of 12.5.02, users of the ServerIron ADX can now edit the name of a virtual server without having to delete the complete virtual server configuration.

Software image files for ServerIron ADX release 12.5.02y

The ServerIron ADX Series of application delivery controllers are upgraded using a single software image. This image is downloaded to the ServerIron ADX switch as either a Primary or Secondary. The default image is the Primary while the ServerIron ADX switch can be configured to boot from the Secondary. The signature file must be copied to flash prior to copying the image in order to perform a FIPS upgrade on ServerIron ADX devices.

Device	Layer 2 (switch image)	Layer 3 (router image)	Boot Image File
ServerIron ADX Series All Models	ASM12502y.bin	ASR12502y.bin	Included inside system Image

Note: Brocade recommends using the latest software version to get the greatest benefit from the ServerIron Application Delivery Controller. Check the HCL ADX Support page for the latest software versions that are available.

Embedded Boot Images

The Brocade ServerIron ADX Software comprises multiple image files that are bundled together to form a single image. In simplistic terms, you could say that it consists of two parts:

1. **The application image:** This is the software that controls most of the ServerIron ADX operation and features. It changes with every software release.
2. **The Embedded Boot image:** This image includes various firmware images. These individual images may or may not change with every release. The table below summarizes the changes to these images with every release

ServerIron ADX Software Release	Embedded Boot Image	Embedded boot image change description
12.0.00	First Release (12.0.00)	
12.1.00	Updated (boot ver 12.1.00 Oct 29, 2009)	Code flash RevF support Boot upgrader {flash | tftp} {primary | secondary | tftp } Support
12.1.00c	Updated (boot ver 12.1.00ba Feb 26, 2010)	Changed both MP and BP DIMM setting
12.1.00e	Updated (boot ver 12.1.00a Jul 9, 2010)	CPU version 2.1 support and bug fixes
12.2.00	Boot ver 12.1.00ba Feb 26, 2010, same as 12.1.0c	
12.2.00a	Updated (boot ver 12.1.00a Jul 9, 2010)	
12.2.01	Boot ver 12.1.00a Jul 9, 2010, same as 12.2.0a	

12.3.00	Boot ver 12.1.00a Jul 9, 2010, same as 12.2.0a	
12.3.01	Boot ver 12.1.00a Jul 9, 2010, same as 12.2.0a	
12.3.03	Boot ver 12.3.03a Aug 18, 2011	CPU version 2.2.1
12.4.00	Updated (Boot ver 12.04.00T405, Nov 21 2011)	Bug fixes
12.5.00	Updated (Boot ver 12.5.00T405, Aug 14 2012)	
12.5.01	Updated (Boot ver 12.5.00T405, Aug 14 2012)	
12.5.02 –12.5.02y	Updated (Boot ver 12.5.00T405, Aug 14 2012)	

Notes

1. The ServerIron ADX boot code has backward compatibility for any previous application release as long as the platform supports that application release. As an example, the ServerIron ADX 1000F platform requires a minimum application and boot image version of release 12.3.03.
2. If you upgrade a ServerIron ADX application switch to a later software image, then it upgrades the embedded boot image too. If for some reason, you need to downgrade the software image to older version, then the embedded boot code may not get downgraded. This is not a problem however because the boot code images are backward compatible to all earlier versions of the system image.
3. In a High Availability setup, Brocade recommends running the same software release on both peer application switches. However, if the boot code images are not matching between the two application switches, then as long as application software image files are matching, such setups are supported by Brocade.
4. Downgrading boot code from a newer version to an older version is not necessary or recommended.
5. When installing software image files for release 12.5.00 on ServerIron ADX chassis-based products, an ASM module must be in the chassis to avoid any potential anomalies.

Factory Pre-loaded Software

Starting June, 2013, the ServerIron ADX application delivery switches ship with router code (Layer 3) and switch code (Layer 2) from Brocade's factory. The primary and secondary flash memory on the ServerIron ADX platform is loaded with software images as shown below:

ServerIron ADX	Software on Primary Flash	Software on Secondary Flash
PREM bundle SKUs (including ADX 4000 bundles)	Router	Switch
Non-PREM SKUs	Switch	Router
Individual management modules	Switch	Router

Note that the presence of 'PREM' license is *mandatory* for running router software. The units that are purchased without PREM license will not be able to execute router code.

Note: All ServerIron ADX shipments prior to the date mentioned above were shipped from Brocade factory with Layer 2 switch code only.

Additional information

Requirements for Running the ServerIron ADX WEB GUI Interface

To access the web interface for all the ServerIron ADX platforms, your device requires the following software:

Supported application:

- Adobe Flash Player 10.2 or later must be installed

Supported browsers:

Internet Explorer (8.0 or later) Mozilla

Firefox (9.0 or later)

Google Chrome (16.0 or later) - to access the ServerIon ADX Web GUI using the Chrome browser with https, SSL false start needs to be disabled in Chrome. It can be done by specifying -disable-ssl-false-start when launching Chrome as shown in the following.

```
chrome.exe -disable-ssl-false-start
```

NOTE: Other browsers that support Adobe Flash Player 10.2 may also work but have not been validated with this system.

Qualified USB Drives with the Release

Brocade has qualified USB sticks that use SmartModular or Unigen chip for use with Brocade ServerIron ADX. The USB sticks from other vendors may work as well, but they are not explicitly verified by Brocade. Note that USB sticks with hard drives are not supported with Brocade ServerIron ADX.

Supporting Documentation for ServerIron ADX release 12.5.02

This release note includes a list of supported features in Brocade ServerIron ADX software release 12.5.02. For specific details of the features, and all other information required to operate the devices, refer to the following manuals.

- Brocade ServerIron ADX Server Load Balancing Guide
- Brocade ServerIron ADX Advanced Server Load Balancing Guide
- Brocade ServerIron ADX Global Server Load Balancing Guide
- Brocade ServerIron ADX OpenScript Programmer's Guide
- Brocade ServerIron ADX OpenScript API Guide
- Brocade ServerIron ADX XML API Programmer's Guide
- Brocade ServerIron ADX Security Guide
- Brocade ServerIron ADX Administration Guide
- Brocade ServerIron ADX Switching and Routing Guide
- Brocade ServerIron ADX Firewall Load Balancing Guide

- Brocade ServerIron ADX Graphical User Interface Guide
- Brocade ServerIron ADX NAT64 Configuration Guide
- Brocade ServerIron ADX Multitenancy Guide
- Brocade ServerIron ADX Hardware installation
- Guide Brocade ServerIron ADX MIB Reference

HCL ADX Support page contains the latest versions of these guides.

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:

General Information

- Technical Support contract number, if applicable
- Switch model
- Switch operating system version
- Error numbers and messages received
- Detailed description of the problem, including the switch or network behavior immediately following the problem and specific questions
- Switch Serial Number

Upgrading an ADX system with a single management module

(From release 12.1.00x, 12.2.x, 12.3.x or 12.4.00 to release 12.5.02y)

Use the following steps to upgrade all codes on a Brocade ServerIron ADX.

1. Copy the correct Brocade ServerIron ADX software image to a TFTP server.
2. Use the **copy tftp flash** command to download the software image to the ServerIron ADX from the TFTP server.

   ```
   ServerIronADX# copy tftp flash 192.168.1.10 ASM12502y.bin primary
   ```

   In the example above the software image is downloaded to flash as "primary". When the ServerIron ADX reloads, it will boot using the primary image. Optionally, you can download the image as secondary.
3. Reload the system and the following will automatically occur.
   - The upgraded application image comes up and automatically checks for boot codes and FPGA microcode to determine if they are up-to-date.
   - If boot codes or FPGA microcode are not up-to-date, the images are automatically upgraded and the ServerIron ADX is automatically reloaded. The upgrade will take somewhere between 2 to 3 minutes depending on your system configuration. Do not reset or power cycle the ServerIron ADX during this time because doing so may cause the ServerIron ADX be unbootable next time.
   - The ServerIron ADX will then come up with all correct images.

NOTE: We recommend that customers use the upgrade procedure described above. For debugging purposes, TAC may want you to disable this operation by entering "ctrl-c" during the upgrade process when the following message is printed on the console:

```
ALERT: The version checker found that one or more embedded
images require upgrade. These files are identified using (*).
The system will automatically reload and perform auto-upgrade in
the next 5 seconds… To terminate this auto-upgrade, enter ctrl-c
now (not recommended)
```

Upgrading an ADX System with dual management modules

Note: Use this procedure to upgrade from release 12.1.00x, 12.2.x or 12.3.x or12.4.00 to release 12.5.02y.

Use the following steps to upgrade all codes on a Brocade ServerIron ADX.

1. Copy the correct Brocade ServerIron ADX software image to a TFTP server.
2. Use the following steps to upgrade all codes on a Brocade ServerIron ADX.
3. At the active management module, use the **copy tftp flash** command to download the software image to the primary and secondary on the ServerIron ADX from the TFTP server.

   ```
   ServerIronADX# copy tftp flash 192.168.1.10 ASM12502y.bin primary
   ServerIronADX# copy tftp flash 192.168.1.10 ASM12502y.bin secondary
   ```

   Wait for the new images on the active management module to be synced over to the standby management module. The following message will be displayed when the management modules are synced:

   ```
   ServerIronADX# sync secondary image: not same
   sync version info: done
   sync_file_ctrl_rt_done 0
   ```

   It may take several minutes for this message to display. Do not proceed to the next step until it does.
4. Reload the system and the following will automatically occur.
   - The upgraded application image comes up and automatically checks for boot codes and FPGA microcode to determine if they are up-to-date.
   - If boot codes or FPGA microcode are not up-to-date, the images are automatically upgraded and the ServerIron ADX is automatically reloaded. The upgrade will take somewhere between 2 to 3 minutes depending on your system configuration. Do not reset or power cycle the ServerIron ADX during this time because doing so may cause the ServerIron ADX be unbootable next time.
   - The ServerIron ADX will then come up with all correct images.

NOTE: In a dual management configuration, the standby management module will be automatically upgraded as well.

NOTE: We recommend that customers use the upgrade procedure described above. For debugging purposes, Technical Assistance Center (TAC) personnel may want you to disable this operation by entering “ctrl-c” during the upgrade process when the following message is printed on the console:

```
ALERT: The version checker found that one or more embedded
images require upgrade. These files are identified using (*).
The system will automatically reload and perform auto-upgrade in
the next 5 seconds… To terminate this auto-upgrade, enter ctrl-c
now (not recommended)
```

Defects closed with code in ServerIron ADX 12.5.02y

Defect ID: DEFECT000737800	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** SLB
Reported In Release: SI 12.5.02	**Technology Area:** Port State
Symptom: Barrel Processor is reset while receiving IPC packets in rare circumstances.	
Condition: Issue observed while changing the server port state with domain configuration.	

Defect ID: DEFECT000737802	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** SLB
Reported In Release: SI 12.5.02	**Technology Area:** GSLB
Symptom: GSLB health check failure occurred when we configure “host-info www” to existing DNS zone.	
Condition: Issue observed when we configured “host-info www” to existing DNS zone.	

Defects closed with code in ServerIron ADX 12.5.02x

Defect ID: DEFECT000737785	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Layer 3
Reported In Release: SI 12.5.02	**Technology Area:** OSPF (IPv4)
Symptom: Static route entries are missing in routing table with OSPF configured.	
Condition: Issue observed when management processor reload.	

Defects closed with code in ServerIron ADX 12.5.02w

Defect ID: DEFECT000737794	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** SSL
Reported In Release: SI 12.5.02	**Technology Area:** SSL
Symptom: Management processor reset occurs when the SSL traffic is offloaded.	
Condition: Issue observed when cavium count reaches maximum value.	

Defects closed with code in ServerIron ADX 12.5.02v

Defect ID: DEFECT000737783	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** config-sync
Reported In Release: SI 12.5.02	**Technology Area:** config-sync
Symptom: Symmetric states are mismatch while removing the virtual IP with config-sync and sym-priority configured.	
Condition: Issue observed while disabling the port on the peer device.	

Defect ID: DEFECT000737784	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** Session Management
Symptom: Barrel Processor is reset while deleting SLB session in rare circumstances.	
Condition: Issue observed while deleting the SLB session.	

Defect ID: DEFECT000737786	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Debug Filter
Reported In Release: SI 12.5.02	**Technology Area:** Debug Filter
Symptom: Incorrect date and time shown in pcap packet capture.	
Condition: Issue observed while converting debug filter packet capture into pcap packet.	

Defect ID: DEFECT000737787	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** System
Reported In Release: SI 12.5.02	**Technology Area:** OS
Symptom: Management Processor is reset while handling the NEFS file system in rare circumstances.	
Condition: Issue observed when processing NEFS file system in very rare scenario.	

Defect ID: DEFECT000737788	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** SLB
Reported In Release: SI 12.5.02	**Technology Area:** Multi Binding
Symptom: Incorrect value seen in “show server virtual” command output.	
Condition: Issue observed when multi binding configured.	

Defect ID: DEFECT000737791	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** Session Management
Symptom: Barrel Processor is reset while handling session age in rare circumstances.	
Condition: Issue observed when process session age in very rare scenario.	

Defects closed with code in ServerIron ADX 12.5.02u

Defect ID: DEFECT000737774	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** Web Management
Symptom: Incorrect time shown when export throughput data from system dashboard of ADX web GUI.	
Condition: Issue observed on the ADX web GUI for throughput data.	

Defect ID: DEFECT000737776	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** SSL
Symptom: SSL handshake failure observed when the SSL traffic is offloaded.	
Condition: Issue observed when cavium count reaches maximum value.	

Defect ID: DEFECT000737777	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Layer 3
Reported In Release: SI 12.5.02	**Technology Area:** Routing
Symptom: Static route entries are missing when the device is rebooted.	
Condition: Issue observed when reboot the device with static route configuration.	

Defect ID: DEFECT000737778	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** SNMP
Symptom: Management Processor is reset while handling the SNMP packets in rare circumstances.	
Condition: Issue observed when process SNMP packets in very rare scenario.	

Defect ID: DEFECT000737779	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** Web Management
Symptom: Incorrect total count of real server in traffic configuration dashboard of ADX web GUI.	
Condition: Issue observed on the ADX web GUI.	

Defect ID: DEFECT000737780	
Technical Severity: High	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** IPC
Reported In Release: SI 12.5.02	**Technology Area:** IPC
Symptom: Barrel Processor is reset while receiving IPC packets in rare circumstances.	
Condition: Issue observed when process IPC packets in very rare scenario.	

Defect ID: DEFECT000737781	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** config-sync
Reported In Release: SI 12.5.02	**Technology Area:** config-sync
Symptom: Real server configuration is not synced to the receiver device.	
Condition: Issue observed when removing the real server from the sender device is not synced to the receiver device.	

Defects closed with code in ServerIron ADX 12.5.02t

Defect ID: DEFECT000737772	
Technical Severity: High	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** Layer 3
Reported In Release: SI 12.5.02	**Technology Area:** OSPF (IPv4)
Symptom: Static route entry shows in routing table even though static route is deleted.	
Condition: Issue observed when interface is down.	

Defect ID: DEFECT000737773	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** SSL Ciphers
Symptom: OpenSSL vulnerabilities CVE-2019-1559.	
Condition: CVE-2019-1559 - Prior versions of OpenSSL 1.0.2r has the Vulnerability.	

Defect ID: DEFECT000737762	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** Web Management
Symptom: Incorrect time display in traffic dashboard of ADX web GUI	
Condition: Issue observed on the ADX web GUI.	

Defects closed with code in ServerIron ADX 12.5.02s

Defect ID: DEFECT000737757	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** System
Reported In Release: SI 12.5.02	**Technology Area:** OS
Symptom: Barrel Processor is reset while handling the TCP packets in rare circumstances.	
Condition: Issue observed in very rare scenario and is a spin lock issue.	

Defect ID: DEFECT000737758	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** SLB
Reported In Release: SI 12.5.02	**Technology Area:** GSLB
Symptom: In GSLB host, running configuration displays only 20 “ip hash weight” entries even it has more entries.	
Condition: Issue observed when we have more than 20 “ip hash weight”.	

Defect ID: DEFECT000737760	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** Health Checks
Symptom: Port policy Configuration cannot be synced on ADX load balancer.	
Condition: Issue observed when without port profile type configuration.	

Defect ID: DEFECT000737763	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** SNI
Reported In Release: SI 12.5.02	**Technology Area:** SSL
Symptom: SNI feature is not working with modified SSL profile.	
Condition: Issue observed when we modify SSL profile.	

Defect ID: DEFECT000737764	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** System
Reported In Release: SI 12.5.02	**Technology Area:** OS
Symptom: Barrel Processor is reset while handling the highest process task in rare circumstances.	
Condition: Issue observed when process queue is empty.	

Defect ID: DEFECT000737766	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** SLB
Reported In Release: SI 12.5.02	**Technology Area:** Session Management
Symptom: Barrel Processor is reset while deleting SLB session.	
Condition: Issue observed while deleting the SLB session.	

Defect ID: DEFECT000737767	
Technical Severity: High	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** SLB
Reported In Release: SI 12.5.02	**Technology Area:** CAM
Symptom: CAM entries are missing when we configure “vip-group”	
Condition: Observed that CAM entries are missing when more “vip-group” configured.	

Defect ID: DEFECT000737769	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** SLB
Reported In Release: SI 12.5.02	**Technology Area:** PORT
Symptom: Traffic failure occurred on the second VIP after reboot when the first VIP configured with ‘track-group’ and CSW.	
Condition: Traffic failure occurs only the second VIP after reboot.	

Defect ID: DEFECT000737770	
Technical Severity: High	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** SSL
Reported In Release: SI 12.5.02	**Technology Area:** SSL
Symptom: SSL health check failure occurred when we configure SHA-2 certificate in server.	
Condition: Issue observed when server configured with SHA-2 certificate.	

Defects closed with code in ServerIron ADX 12.5.02r

Defect ID: DEFECT000737750	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** SLB
Reported In Release: SI 12.5.02	**Technology Area:** GSLB
Symptom: Barrel Processor is reset unexpectedly and all the interfaces are marked down while processing GSLB query in rare circumstances.	
Condition: While handling the GSLB query packet causes Barrel Processor reset.	

Defect ID: DEFECT000737751	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** SLB
Reported In Release: SI 12.5.02	**Technology Area:** GSLB
Symptom: GSLB query time out with dns override and dns cache-proxy modes are configured.	
Condition: Issue observed while sending the GSLB query for unknown domain which is not configured in ServerIron	

Defect ID: DEFECT000737752	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** SLB
Reported In Release: SI 12.5.02	**Technology Area:** Session Management
Symptom: Barrel Processor is reset while stateful is configured.	
Condition: Issue observed while handling stateful session.	

Defect ID: DEFECT000737753	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** SSL Ciphers
Symptom: OpenSSL vulnerabilities CVE-2017-3737 and CVE-2017-3738	
Condition: CVE-2017-3737 - Prior versions of OpenSSL 1.0.2 has the vulnerability. CVE-2017-3738 - Prior versions of OpenSSL 1.0.2 has the vulnerability.	

Defect ID: DEFECT000737755	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** System
Reported In Release: SI 12.5.02	**Technology Area:** OS
Symptom: Barrel Processor is reset and all interface was gone down temporary in rare circumstances.	
Condition: Issue observed in very rare scenario and is a timing issue.	

Defect ID: DEFECT000737754	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** SSL Ciphers
Symptom: OpenSSL vulnerabilities CVE-2018-0739.	
Condition: Prior versions of OpenSSL 1.0.2n has these Vulnerabilities.	

Defect ID: DEFECT000737748	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Global Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** GSLB controller
Symptom: Barrel Processor is reset when adding the external sticky policies in GSLB.	
Condition: Issue observed only when GSLB sticky policy is configured under the DNS zone.	

Defect ID: DEFECT000737756	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** System
Reported In Release: SI 12.5.02	**Technology Area:** Component
Symptom: Barrel Processor is reset while handling the IPC error packet in rare circumstances.	
Condition: Issue observed when trying to update the MAC entry of IPC error packet.	

Defects closed with code in ServerIron ADX 12.5.02q

Defect ID: DEFECT000642829	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** SSH - Secure Shell
Symptom: Management processor is reset on closing SSH session.	
Condition: Continuously generating SSL key using script via SSH session causes Management processor reset.	

Defect ID: DEFECT000648609	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Layer 3
Reported In Release: SI 12.5.02	**Technology Area:** Other IPv4
Symptom: Management Processor drops DHCP Discover broadcast packet.	
Condition: When DHCP client is enabled and helper address is not configured, Management Processor drops DHCP discover broadcast packet.	

Defect ID: DEFECT000645727	
Technical Severity: High	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** Multi tenancy
Reported In Release: SI 12.5.02	**Technology Area:** Filesystem
Symptom: Management processor is reset while trying to delete the disabled tenants and executing writing memory	
Condition: Issue observed in ServerIron ADX 4000 while deleting disabled tenant only.	

Defect ID: DEFECT000645413	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Firewall Health Check
Reported In Release: SI 12.5.02	**Technology Area:** ICMP
Symptom: Management processor is reset unexpectedly while processing ICMP echo reply in rare circumstances.	
Condition: While handling the firewall health check packet causes Management processor reset.	

Defect ID: DEFECT000651126	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** SLB
Reported In Release: SI 12.5.02	**Technology Area:** GSLB
Symptom: Management processor is reset when deleting GSLB host-info name and port that does not exist.	
Condition: Issue observed when deleting GSLB host-info name and port that does not exist from telnet/SSH/tconsole	

Defect ID: DEFECT000653393	
Technical Severity: Medium	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** Secure Socket Layer (SSL)
Reported In Release:	**Technology Area:** SSL Proxy
Symptom: Observed application CPU reset while receiving the SSL proxy traffic with the unsupported signature	
Condition: Virtual Server needs to be configured to receive the SSL proxy traffic with Signature Algorithm in the SSL extension.	

Defect ID: DEFECT000653793	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Secure Socket Layer (SSL)
Reported In Release:	**Technology Area:** SSL Health check
Symptom: Observed SSL health check failure when the ADX sends unsupported signature algorithm in the Health check.	
Condition: Virtual Server needs to be configured to send the SSL health check with signature algorithms.	

Defect ID: DEFECT000654544	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** SSL Termination
Symptom: Observed Management and Barrel Processors reset while receiving the huge number of TLS 1.2 traffic.	
Condition: Virtual Server needs to be configured to receive the SSL traffic with TLS 1.2 and EC ciphers	

Defect ID: DEFECT000655317	
Technical Severity: Low	**Probability:** Low
Product: Brocade ServerIron ADX	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** SSL Termination
Symptom: Observed Management Processor reset while executing 'show ssl cert <name>' for a specific certificate	
Condition: Management Processor resets only when user execute show command for a specific certificate.	

Defect ID: DEFECT000658166	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Server load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** Configuration Synchronization
Symptom: Symmetric VIP state transition adds config-sync mode to running config even if config-sync is not configured	
Condition: When a symmetric VIP becomes active or standby 'config-sync mode sender/receiver' is automatically added to the running configuration by default.	

Defect ID: DEFECT000644921	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** SSL Termination
Symptom: Observed Barrel Processor reset while receiving the huge number of TLS 1.2 traffic with EC ciphers selected.	

Defects closed with code in ServerIron ADX 12.5.02p

Defect ID: DEFECT000624011	
Technical Severity: Medium	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** High Availability
Reported In Release: SI 12.5.02	**Technology Area:** Hot-Standby SLB
Symptom: Unless a unique SNMP engine ID is explicitly configured on both ADXs in a config-sync pair, HA fail over and fail back will cause "show config-sync status" to show as out of sync.	
Condition: As default SNMP engine ID is not part of running config and it does not sync with peer that leads out of sync.	

Defect ID: DEFECT000624058	
Technical Severity: Medium	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** System
Reported In Release: SI 12.5.02	**Technology Area:** Component
Symptom: SSL diag test is failed due to wrong minor device number in ServerIron ADX.	
Condition: When executing SSL diag test command "ssl diag 1 1" command, SSL diag test is always failed due to wrong minor device number.	

Defect ID: DEFECT000632758	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** SNMPv2, SNMPv3 & MIBs
Symptom: After adding or modifying SNMPv3 configuration on ServerIron ADX, some of the SNMPv3 configuration may get corrupted intermittently, causing SNMP authentication failure for the users.	
Condition: SNMPv3 configuration is corrupted if a user accidently adds extra white spaces while adding/modifying/deleting SNMPv3 configuration.	

Defect ID: DEFECT000635096	
Technical Severity: Medium	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** Layer 3
Reported In Release: SI 12.4.01	**Technology Area:** Other IPv6
Symptom: Last configured IPv6 address on VE interface was not functional.	
Condition: The last interface configured with IPv6 addresses is unable to correctly send or receive IPv6 traffic without reloading the ServerIron ADX.	

Defect ID: DEFECT000636271	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Server Load Balancing
Reported In Release: SI 12.4.01	**Technology Area:** Policy-based SLB
Symptom: Too many error messages related to timer cancellation are seen on the console.	
Condition: Continuous messages are popped up after configuring DNS health check.	

Defect ID: DEFECT000638203	
Technical Severity: High	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** System Management
Symptom: High Management Processor CPU observed during code upgrade from 12502g to 12502m.	
Condition: Issue observed while reloading the ServerIron ADX with SSL profile configuration on 4U or 10U.	

Defect ID: DEFECT000638293	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Global Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** GSLB metrics
Symptom: In multi-tenancy, GSLB controller ignores IP weight metric, when two zones are configured with different IP weights.	
Condition: Weighted IP metric selection does not work properly when tenant is configured with 2 barrel processor of same ASM module and gslb-max-zone-host value differs between the barrel processor.	

Defect ID: DEFECT000638669	
Technical Severity: High	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** System
Reported In Release: SI 12.5.02	**Technology Area:** CLI
Symptom: Trunk ports comes up during boot-up even though it is disabled when the trunk port is configured with port-name which contains user added quotes.	
Condition: Issue observed only when trunk port is configured with double quotes.	

Defect ID: DEFECT000641256	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** Complex protocols
Symptom: Passive mode FTP is not working in optimization path enabled in ServerIron ADX.	
Condition: Issue observed only when sending FTP traffic.	

Defect ID: DEFECT000642291	
Technical Severity: High	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** Layer 7 Content Switching
Symptom: If next-hop feature is enabled on any of the VIPs on ServerIron ADX, a virtual server configured with full stack features such as SSL-Termination, SSL-proxy etc may not work.	
Condition: Issue observed when next-hop feature configured under any virtual server.	

Defect ID: DEFECT000644264	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** SNMPv2, SNMPv3 & MIBs
Symptom: snL4BindingRealServerPortState returns invalid value (7), if primary multi-port binding is removed	
Condition: Issue observed when primary multi-port binding removed.	

Defects closed with code in ServerIron ADX 12.5.02n

Defect ID: DEFECT000584269	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.4.00	**Technology Area:** SSL Health-checks
Symptom: Management process is getting reset when corrupted complete SSL health check packet received in L3 DSR enabled setup.	
Condition: Observed when receiving the corrupted complete SSL health check packet in L3 DSR enabled setup.	

Defect ID: DEFECT000606624	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** Source-NAT
Symptom: SLB connections from certain client IPs to a virtual server fails in ServerIron ADX 10K chassis.	
Condition: SLB connections gets failed while passing through ASM slot 3.	

Defect ID: DEFECT000615283	
Technical Severity: Medium	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** SSH - Secure Shell
Symptom: Observed SSH Management processor HEAP memory leak.	
Condition: With repeated SSH login/logout over time, Management processor HEAP memory slowly leaks over time and does not get freed.	

Defect ID: DEFECT0006110060	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Server Load Balancing
Reported In Release: SI 12.4.00	**Technology Area:** DSR
Symptom: When DSR feature is enabled in a one-arm setup, if reverse SLB packets are received on ServerIron ADX, the Application CPU processes the packets and sends them out on the same port causing mac-flaps on intermediate devices.	
Condition: If an intermediate device loses local client's MAC entry, it floods the reverse SLB packet causing the packet to be sent to ServerIron ADX.	

Defect ID: DEFECT000620090	
Technical Severity: High	**Probability:** Low
Product: Brocade ServerIron ADX	**Technology:** Global Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** Secure GSLB
Symptom: ServerIron ADX management processor resets while executing debug command "debug secure-gslb" under rare circumstances.	
Condition: Issue occurs rarely while executing debug command "debug secure-gslb".	

Defect ID: DEFECT000620570	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Security
Reported In Release: SI 12.4.01	**Technology Area:** SYN-proxy/SYN-defense
Symptom: Application CPU reset observed while enabling SYN-PROXY.	
Condition: Enabling SYN-PROXY on-fly with traffic causes application CPU reset.	

Defect ID: DEFECT000621574	
Technical Severity: Medium	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** Global Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** Secure GSLB
Symptom: Management processor does not have Debug/error counters for SSL health checks and secure GSLB	
Condition: Management processor does not have Debug/error counters for SSL health checks and secure GSLB	

Defect ID: DEFECT000621772	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** Web Management
Symptom: Observed management processor reset while connecting to serverIron ADX GUI through HTTPS.	
Condition: Management processor reset occurs when connecting to HTTPS GUI using invalid secret_data	

Defect ID: DEFECT000624019	
Technical Severity: Medium	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** High Availability
Reported In Release: SI 12.5.02	**Technology Area:** Hot-Standby SLB
Symptom: Applying "config-sync enable-peer" command and executing "write memory" on a sender fails to save "config-sync enable-peer" to the receiver startup configuration.	
Condition: On config-sync enabled setup, executing "config-sync enable-peer" command followed by "write memory" command on a sender fails to save "config-sync enable-peer" command to the receiver startup configuration.	

Defect ID: DEFECT000628448	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** Web Management
Symptom: Software information is not shown in ServerIron ADX web GUI login page.	
Condition: Starting from 12502k release, the software information is missing from ServerIron ADX web GUI login page.	

Defect ID: DEFECT000629449	
Technical Severity: Critical	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** Web Management
Symptom: Management processor reset observed while doing user interface operation from ServerIron ADX web GUI.	
Condition: Issue observed when user tries continuous operations like login and log out the user interface page.	

Defect ID: DEFECT000631896	
Technical Severity: Critical	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** Global Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** GSLB Controller
Symptom: GSLB communication failure with error messages on the controller seen such as "gslb secure communication xx.xx.xx.xx failed peer public key check failed".	
Condition: GSLB controller loses ARP entry due to upstream interface disabled or clear ARP and then GSLB connections goes down and retries.	
Recovery: Reload GSLB controller.	

Defect ID: DEFECT000632749	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** Web Management
Symptom: Management processor reset observed while doing user interface operation.	
Condition: Issue observed when user does continuous operations like login and log out on web GUI.	

Defect ID: DEFECT000633200	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** Web Management
Symptom: Management processor reset observed occasionally when user tries to login and log out from web GUI.	
Condition: Issue observed when user tries continuous operations like login and log out on the user interface	

Defect ID: DEFECT000633247	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** Stateful SLB
Symptom: The application CPU may reset while establishing a client connection to windows terminal server VIP, if the command "port 3389 win-term-server" is removed from the VIP on the fly.	
Condition: Issue occurs while removing “win-term-serv” configuration on the fly.	

Defect ID: DEFECT000633254	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** SSL Ciphers
Symptom: OpenSSL vulnerabilities CVE-2017-3730, CVE-2017-3731 and CVE-2017-3732.	
Condition: CVE-2017-3730 - not applicable for serverIron ADX. Applicable only for OpenSSL 1.1.0 code series. CVE-2017-3731 - Prior versions of OpenSSL 1.0.2 has the vulnerability. CVE-2017-3732 - Prior versions of OpenSSL 1.0.2 has the vulnerability.	

Defect ID: DEFECT000633378	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** DSR
Symptom: Real server MAC address is not updating	properly with Layer 2 DSR configuration.
Condition: Issue observed with optimization mode configuration in Layer 2 DSR.	

Defect ID: DEFECT000634183	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** System Management
Symptom: Management processor reset observed	while saving the save tech file.
Condition: Issue observed while saving the save tech file with special characters.	

Defect ID: DEFECT000634522	
Technical Severity: Medium	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** Configuration Synchronization
Symptom: Observed error message while doing	incremental sync via web GUI.
Condition: Error messages are seen while using the Web GUI to modify SSL profiles and apply them to virtual servers.	

Defect ID: DEFECT000634578	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Management
Reported In Release: SI Virtual ADX 4.0.00	**Technology Area:** Web Management
Symptom: Openssl vulnerability CVE-2016-2183.	
Condition: Vulnerable for CVE-2016-2183 when weak ciphers are enabled.	

Defect ID: DEFECT000637149	
Technical Severity: High	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** SSL Health-checks
Symptom: ServerIron ADX is sending corrupted SSL health check client hello packet.	
Condition: Observed when we configure the health check policy under SSL port.	

Defect ID: DEFECT000633948	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** Session Management
Symptom: Application CPU reset observed while enabling SYN-PROXY.	
Condition: Enabling SYN-PROXY on the fly with traffic causes application CPU reset.	

Defects closed with code in ServerIron ADX 12.5.02m

Defect ID: DEFECT000560396	
Technical Severity: High	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** Health Checks
Symptom: Application CPU domain health check states are not sync with Management processor.	
Condition: Issue observed while executing "show server bind HTTP-Domain domain" command on application CPU console.	

Defect ID: DEFECT0005100493	
Technical Severity: High	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** Monitoring/RAS
Reported In Release: SI 12.5.02	**Technology Area:** Syslog
Symptom: CLI command "debug destination ……" is not available in a non-Multi-Tenancy mode.	
Condition: CLI command "debug destination ?" is executed; “debug d?” is executed on non-Multi-Tenancy mode.	

Defect ID: DEFECT000605841	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** SSL Health-checks
Symptom: ServerIron ADX TLS 1.x SSL health check client hello does not include signature algorithm extension.	
Condition: Observed when SSL health check is enabled.	

Defect ID: DEFECT000606760	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** SSL Termination
Symptom: ServerIron ADX does not support max-tcp- conn-rate feature for full stack.	
Condition: ServerIron ADX does not support max-tcp-conn-rate feature for full stack.	

Defect ID: DEFECT000606791	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** Layer 7 Content Switching
Symptom: Application CPU reset observed during debug session for finding connection failures due to CSW.	
Condition: Issue observed while executing "show server proxy detail" command on application CPU console.	

Defect ID: DEFECT0006010030	
Technical Severity: High	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** Multitenancy
Reported In Release: SI 12.5.02	**Technology Area:** Tenant Monitoring
Symptom: Unable to create more than 12 Tenants in ServerIron ADX 10000 and ServerIron ADX 4000.	
Condition: Tenant's default value for source-ip parameter is set as 10 in ServerIron ADX and maximum 128 source-ip can be configured, Default value for source-ip parameter in Tenant is configured based on license type in multiTenancy mode.	

Defect ID: DEFECT000610083	
Technical Severity: High	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** Multitenancy
Reported In Release: SI 12.5.02	**Technology Area:** Tenant Monitoring
Symptom: Not able to figure out which tenant is generating the syslog messages in event log file.	
Condition: Issue observed when 'write memory' and 'show logging' commands are executed on tenant console.	

Defect ID: DEFECT000611723	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** Source-NAT
Symptom: The reverse SLB traffic from real server to ServerIron ADX causes application CPU reset when source NAT IP configured.	
Condition: Issue observed while sending reverse TCP traffic in standalone ServerIron ADX with single application CPU selection.	

Defect ID: DEFECT000613671	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** L7 SSL
Symptom: OpenSSL vulnerabilities CVE-2016-2180.	
Condition: Prior versions of OpenSSL 1.0.2h has these Vulnerabilities.	

Defect ID: DEFECT000615851	
Technical Severity: Medium	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** Stateful SLB
Symptom: Port Slow-start functionality does not work as expected.	
Condition: After configuring slow-start under real server ports, slow-start rate does not come into effect.	

Defect ID: DEFECT000617007	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** High Availability
Reported In Release: SI 12.5.02	**Technology Area:** Hot-Standby SLB
Symptom: In a Hot-Standby setup, MAC address for the real server was not populated in software tables of the Active ServerIron ADX.	
Condition: When the real server MAC address is not removed from the hardware table after disabling the trunk ports, It will not be populated in software tables when re-enable trunk ports.	

Defect ID: DEFECT000617168	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** SSL Ciphers
Symptom: OpenSSL vulnerability CVE-2016-2182.	
Condition: CVE-2016-2182 - Prior versions of OpenSSL 1.1.0 has the Vulnerability.	

Defect ID: DEFECT000617226	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** System Management
Symptom: ServerIron ADX not throwing any warning message while running 'more' command to display large files on console.	
Condition: Observed this issue when executing more command to display large files on console like event log file.	

Defect ID: DEFECT000617906	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Multitenancy
Reported In Release: SI 12.5.02	**Technology Area:** Tenant Monitoring
Symptom: Management processor reset observed when executing "ip sntp source-interface mgmt1" command.	
Condition: Issue observed while executing "ip sntp source-interface mgmt1" command on tenant console.	

Defect ID: DEFECT000618709	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** Health Checks
Symptom: When content check health checks are configured for unknown ports, health check flaps even though the matching content exists.	
Condition: Issue observed when content-check match-list health check is configured for unknown ports.	

Defect ID: DEFECT000619349	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** SNMPv2, SNMPv3 & MIBs
Symptom: ServerIron ADX chassis gives incorrect power supply operational status values when polled using SNMP.	
Condition: When the power supply operational status values of ServerIron ADX chassis are polled using SNMP.	

Defect ID: DEFECT000620200	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** L7 SSL
Symptom: OpenSSL vulnerabilities CVE-2016-6302, CVE-2016-6303, CVE-2016-6304 and CVE-2016-6306.	
Condition: CVE-2016-6302 - Prior versions of OpenSSL 1.1.0 has the Vulnerability. CVE-2016-6303 - Prior versions of OpenSSL 1.1.0 has the Vulnerability. CVE-2016-6304 - Prior versions of OpenSSL 1.0.1u, 1.0.2 before 1.0.2i, and 1.1.0 before 1.1.0a has the Vulnerability. CVE-2016-6304 - Prior versions of OpenSSL 1.0.1u and 1.0.2 before 1.0.2i has the Vulnerability.	

Defect ID: DEFECT000620350	
Technical Severity: Critical	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** SSL Termination
Symptom: ServerIron ADX may ex perience an application CPU reset during heavy SSL traffic load.	
Condition: Observed when running out of 8K buffers and heavy SSL traffic load.	

Defect ID: DEFECT000621030	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Management
Reported In Release: SI 12.4.00	**Technology Area:** System Management
Symptom: Time difference is observed between the device clock and the debug filter time stamp.	
Condition: Issue is observed between "show clock" command output and debug filter time stamp	

Defect ID: DEFECT000621475	
Technical Severity: Medium	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** SSL Ciphers
Symptom: The "show ssl stat counters" command does not include counters to indicate if remote peer closed SSL connection during SSL handshake or data transfer. Also, "show ssl con" command does not take starting index and # of entries as arguments, to display list of SSL connections.	
Condition: Observed when issuing the "show ssl stat" command and "show ssl con" command.	

Defect ID: DEFECT000621741	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** SSL Termination
Symptom: Application CPU resets when a TCP FIN is received on a Virtual Server configured for SSL-Terminate.	
Condition: Issue observed when 'enable-close-notify' is present in the SSL profile configuration on the SSL-Terminate virtual server.	

Defect ID: DEFECT000622034	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** Health Checks
Symptom: UDP keepalive status is not displayed properly even functionality works fine.	
Condition: Issue observed while issuing the 'show server real keep <port>' command.	

Defect ID: DEFECT000622232	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Management
Reported In Release: SI 12.4.01	**Technology Area:** Web Management
Symptom: Observed ADX web GUI vulnerable to XSS vulnerabilities.	
Condition: Observed ADX web GUI vulnerable to XSS vulnerabilities.	

Defect ID: DEFECT000622690	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** Health Checks
Symptom: Comp lete SSL Health Check for unknown port fails with content match configuration.	
Condition: Issue observed when a user configures content match with complete SSL Health Check on an unknown port.	

Defect ID: DEFECT000623720	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Monitoring/RAS
Reported In Release: SI 12.5.02	**Technology Area:** Syslog
Symptom: Syslog messages are not lo gged when SNMP traps are disabled.	
Condition: Issue observed only when SNMP traps are disabled.	

Defect ID: DEFECT000624022	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** High Availability
Reported In Release: SI 12.5.02	**Technology Area:** Hot-Standby SLB
Symptom: In rare circumstances, a hot standby config-sync pair can enter a persistent double sender state, with one ADX as "active/sender" and the other stuck as "standby/sender" instead of the expected "standby/receiver".	
Condition: Issue observed while executing interface "no disable" command instead of "enable" command.	

Defect ID: DEFECT000627830	
Technical Severity: Medium	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** System
Reported In Release: SI 12.5.02	**Technology Area:** CLI
Symptom: CLI command "show ssl mem" output does not have memory used percentage.	
Condition: Observed that "show ssl mem" output does not have memory used percentage.	

Defects closed with code in ServerIron ADX 12.5.02k

Defect ID: DEFECT000591747	
Technical Severity: Medium	**Probability:** Mediu m
Product: Brocade ServerIron ADX	**Technology:** Layer 3
Reported In Release: SI 12.5.02	**Technology Area:** Other IPv6
Symptom: IPv6 address related configuration is accepted but is not seen in running-config and does not get saved to startup config with write mem.	
Condition: IPv6 address for specific virtual interfaces is accepted but is not seen in running-config although it is programmed correctly and is functional. Since it is not seen in running-config it does not get saved in startup-config with write mem. So upon reload IPv6 address config is neither seen in running config nor is functional.	

Defect ID: DEFECT000606496	
Technical Severity: Low	**Probability:** Low
Product: Brocade ServerIron ADX	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** L7 SSL
Symptom: OpenSSL vulnerabilities CVE-2016-2177 and CVE-2016-2178	
Condition: Prior versions of OpenSSL 1.0.2h has these Vulnerabilities.	

Defect ID: DEFECT000608847	
Technical Severity: Medium	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** Monitoring/RAS
Reported In Release: SI 12.5.02	**Technology Area:** Syslog
Symptom: Power supply positions are shown is inconsistent between "show logging" and "show chassis" command outputs.	
Condition: Power supply positions are shown in reverse order only on "show logging" command output.	

Defect ID: DEFECT0006121006	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** Health Checks
Symptom: Management Processor reset in Serveriron ADX Continuously when TCP and UDP configured under SIP port.	
Condition: Issue was observed while configure both TCP and UDP with different keepalive intervals under SIP port.	

Defects closed with code in ServerIron ADX 12.5.02j

Defect ID: DEFECT000389287	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Server Load Balancing
Reported In Release: SI 12.3.01	**Technology Area:** Health Checks
Symptom: Under rare circumstances, real server port get stuck in testing state and serverIron ADX not sending health checks to that port.	
Condition: This issue is rare event.	

Defect ID: DEFECT000469622	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** High Availability
Reported In Release: SI 12.4.00	**Technology Area:** Hot-Standby SLB
Symptom: In a Hot-Standby setup, there was a slight configuration mismatch, with the element health check configuration, missing from the standby ADX. When same 'server source-ip' address was configured on Active and Standby ADXs accidently, the Standby ADX reset itself.	
Condition: Issue observed only in Hot-standby HA setup.	
Workaround: Configure the same element/boolean health checks on both active and standby ADXs.	

Defect ID: DEFECT000581454	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Server Load Balancing
Reported In Release: SI 12.4.00	**Technology Area:** Session Management
Symptom: Under rare circumstances, ServerIron ADX fails to delete particular remote server sessions.	
Condition: Specific remote server which has the index value of 4096 has this session deletion issue, this index is created by serverIron ADX internally and there is no way to identify the index by user.	

Defect ID: DEFECT000594635	
Technical Severity: Medium	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** SSL Ciphers
Symptom: SSL Proxy connections fail when backend server selects ECDHE_RSA_WITH_AES_256_CBC_SHA cipher when using TLS1.0	
Condition: Observed when backend server selects ECDHE_RSA_WITH_AES_256_CBC_SHA cipher with TLS1.0	

Defect ID: DEFECT000596395	
Technical Severity: Medium	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** SSL Ciphers
Symptom: Enhancement to allow prioritization of stronger elliptic curve cipher suites by default when pfs-prioritize and all cipher-suites are enabled under the SSL-profile.	
Condition: Observed when attempting to make a connection from client to ServerIron ADX with SSL terminate/proxy, the ServerIron ADX will respond to the client hello with cipher suite that is not the strongest that it is capable of supporting.	

Defect ID: DEFECT000596576	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** System Management
Symptom: 10U chassis running with dual MM1 management modules, both having SSL modules might cause high interrupts on MP CPU when used with SSL terminate traffic. This is mainly due to improper initialization of key store on some of the cryptographic devices in the SSL modules.	
Condition: Customer should be using 10U Chassis with dual MM1 using SSL modules running SI12502 GA or later firmware.	

Defect ID: DEFECT000597109	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Multitenancy
Reported In Release: SI 12.5.02	**Technology Area:** Tenant Monitoring
Symptom: During the boot-up serverIron ADX does not retain the implicit virtual interface value of the default resource profile in multi tenancy mode, if the default value has been changed in the default resource profile. If this changed value is higher than the available virtual interface for the new tenant, then the tenant will not be brought up and the tenant related configuration on the master will disappear.	
Condition: This issue is observed during the boot-up serverIron ADX, if the default profile is modified with higher value after all tenant creation.	

Defect ID: DEFECT000597567	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** Multiple Port Binding
Symptom: Health check track-port-state is DOWN even all ports are in ‘Active’ state.	
Condition: Observed this issue when deleting primary port, disabling and re-enabling NIC card at server side.	

Defect ID: DEFECT0005100708	
Technical Severity: High	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** System Management
Symptom: Output of CLI command 'show run | inc xxxx' in ServerIron ADX has multiple CLI prompts in between the actual output under certain conditions.	
Condition: Issue observed when the user login to ServerIron ADX through console/TELNET/SSH and goes to RCONSOLE mode then executes 'show run | inc xxxx' CLI command, exit from RCONSOLE happens due to timeouts (console/TELNET/SSH timeouts).	

Defect ID: DEFECT000600351	
Technical Severity: Low	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** System
Reported In Release: SI 12.5.02	**Technology Area:** Component
Symptom: CLI command "dm cputracker restart all" missing reset spike.	
Condition: Observed while issuing "dm cputracker restart all" command.	

Defect ID: DEFECT0006004100	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** SSL Proxy
Symptom: Open SSL vulnerabilities CVE 2016-2005, 2106, 2110 2108, 2109 and 2176.	
Condition: Prior versions of open SSL 1.0.2.c has this Vulnerabilities.	

Defect ID: DEFECT000601282	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** SSL Termination
Symptom: When crypto chip was exerted beyond the threshold, the memory used for hardware SSL instructions was corrupted causing application CPU resets.	
Condition: Issue observed when SSL terminate and CSW configured on the VIP, elliptical curve ciphers are configured on SSL profile.	

Defect ID: DEFECT000601866	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** Health Checks
Symptom: Continuous SSL error messages seen on console and it prevents users from entering any command.	
Condition: Observed when the SSL health check client hello received.	

Defect ID: DEFECT000601868	
Technical Severity: High	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** Monitoring/RAS
Reported In Release: SI 12.5.02	**Technology Area:** Syslog
Symptom: ServerIron ADX not able to delete old event log files.	
Condition: Issue was observed when the event log files were copied manually and then reload the ServerIron ADX.	

Defect ID: DEFECT000602266	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** Web Management
Symptom: Management processor reset is observed when user tries to establish a HTTPS connection through web-GUI using duplicate certificate.	
Condition: Issue observed when user tries to connect to web-GUI through HTTPS connection with illegitimate certificate.	

Defect ID: DEFECT000602392	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** SSL Proxy
Symptom: ServerIron ADX FIN closes server side connection with 'bad length' error after receiving 'change cipher spec' from server.	
Condition: Observed when attempting to make a connection from ServerIron ADX to server with SSL proxy, the server will respond to the ServerIron ADX with the 'change cipher spec' message.	

Defect ID: DEFECT000602820	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** XML API
Symptom: XMLAPI 'getAllSslCertificatesSummary' fails to retrieve more than 10 certificates in single request.	
Condition: Issue observed only on single XMLAPI request.	

Defect ID: DEFECT000603720	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Multitenancy
Reported In Release: SI 12.5.02	**Technology Area:** Tenant Monitoring
Symptom: System resets when user tries to save PCAP file in USB1 device.	
Condition: System reset happens when user tries to save PCAP file in /USB1/ location.	

Defect ID: DEFECT000604225	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** System
Reported In Release: SI 12.5.02	**Technology Area:** CLI
Symptom: System reset observed while executing CLI 'use-cmd-script'.	
Condition: Under rare circumstances the issue observed while executing the CLI command 'use-cmd-script'.	

Defect ID: DEFECT000607561	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Global Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** GSLB Controller
Symptom: Memory leaked for GSLB hosts with Url option configured during the GSLB controller handling VIP list update from sites.	
Condition: Memory leak observed for GSLB hosts with Url option configured during the GSLB controller handling VIP list update from sites	
Workaround: Disable Distributed HC or remove Url option for host SSL port	

Defect ID: DEFECT000607579	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Global Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** GSLB Controller
Symptom: Rarely system resets while configuring GSLB host-info status code on tenant in multi-tenancy mode.	
Condition: GSLB host-info status code configuration on tenant in multi-tenant environment causes system reset.	

Defect ID: DEFECT000607783	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** SSL Termination
Symptom: SSL traffic failure due to almost all of sockets were stuck in CLOSE_WAIT and CLOSED state	
Condition: Observed when ServerIron ADX has some load and receives immediate FIN after the client hello then sockets will be in CLOSE_WAIT state.	

Defect ID: DEFECT000607794	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** SSL Termination
Symptom: CLI display issue for the command “show sock state”. This command displays 4 billion value for the counters "Time-wait" and "Open sockets"	
Condition: Observed when issue the command "show sock state", at rare scenario.	

Defect ID: DEFECT000608774	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Global Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** Secure GSLB
Symptom: Secure GSLB functionality does not work in mixed secure GSLB configurations scenario: Controller/site using 12.5.02e or later version, controller/site using 12.4.	
Condition: The issue happens only when the site or controller has 12.5.02e and later versions in serverIron ADX.	

Defect ID: DEFECT000609495	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Multitenancy
Reported In Release: SI 12.5.02	**Technology Area:** Tenant Monitoring
Symptom: ServerIron ADX may reset without debug logs when disabling a tenant. After the reset it shows a cold start.	
Condition: The chance of hitting this bug is not high. But higher when the tenant's activity is high or the overall system's activities are high.	
Workaround: Do the tenant disabling at low traffic hours has lower probability of hitting the problem.	
Recovery: When the problem occurs system automatically reboots.	

Defect ID: DEFECT000612455	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** System Management
Symptom: Under rare circumstances, one of the ServerIron ADX may experience a system reset in High Availability (HA) configuration.	
Condition: Issue observed in ServerIron ADX 4000 configured with High Availability.	

Defects closed with code in ServerIron ADX 12.5.02h

Defect ID: DEFECT000587623	
Technical Severity: Medium	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** Management
Reported In Release: SI 12.4.00	**Technology Area:** System Management
Symptom: Loop back interface does not support all source-interface commands for TFTP, TACACS, TELNET and Syslog services.	
Condition: Loop back interface support does not exist while configuring source-interface commands.	

Defect ID: DEFECT000590086	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** SSL Ciphers
Symptom: Application CPU perform a reset while processing TCP RST from a client to a Virtual Server enabled with SSL-Terminate+CSW, in the middle of SSL handshake	
Condition: The issue observed while sending RST from client to SSL-terminate CSW VIP	

Defect ID: DEFECT000590545	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Transparent Cache Switching
Reported In Release: SI 12.4.01	**Technology Area:** Layer 7 TCS
Symptom: When group-failover is enabled and multiple cache servers are configured with different group in TCS configuration, CSW rule configured does not select appropriate cache server instead sending the traffic to the internet directly.	
Condition: This issue is seen when group failover enabled for L7 TCS.	

Defect ID: DEFECT000590941	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** SSL Termination
Symptom: SSL connections became slow and pages failed to load completely.	
Condition: ServerIron ADX configured with SSL-termination or SSL-proxy, may leak transmit buffers under rare circumstances when using CBC ciphers	

Defect ID: DEFECT000592596	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** SSL Termination
Symptom: Multiple Vulnerabilities in openSSL for Brocade ServerIron ADX CVE-2016-0702 CVE-2016-0703 CVE-2016-0704 CVE-2016-0705 CVE-2016-0797 CVE-2016-07100 CVE-2016-07100 CVE-2016-0800	
Condition: OpenSSL version 1.0.2.c has this Vulnerabilities.	

Defect ID: DEFECT000593517	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** SSL Termination
Symptom: Session-cache flushes after 256 entries instead of configured value of 512	
Condition: When the count for "ssl accept session finished" goes beyond 256, session-cache gets flushed even though the configured value is 512.	

Defect ID: DEFECT000595372	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Server Load Balancing
Reported In Release: SI 12.4.00	**Technology Area:** SLB Debug
Symptom: In rare circumstances, Application Processor resets unexpectedly in HA standby device If NAT64 is configured.	
Condition: Application Processor on a standby device is reset in a HA setup when NAT64 is configured.	

Defect ID: DEFECT000597251	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** Layer 7 Content Switching
Symptom: When ServerIron ADX configured with SSL-termination or SSL-PROXY received pipe lined requests, it experienced a gradual leak in transmit buffers. This led to buffer exhaustion over time and causing some traffic failure.	
Condition: Issue happens when SSL-termination or SSL-PROXY is configured on ServerIron ADX AND pipe line requests received.	

Defect ID: DEFECT000597529	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** Web Management
Symptom: Virtual Interface (ve) configuration gets deleted after changing VLAN name in web GUI	
Condition: Issue applicable only when changing the VLAN name through web GUI	

Defect ID: DEFECT000597932	
Technical Severity: High	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** System
Reported In Release: SI 12.5.02	**Technology Area:** Component
Symptom: ServerIron ADX 10000 in a Multi-tenancy (MT) mode when reloaded keeps continuously rebooting and does not come up.	
Condition: This issue observed only in ServerIron ADX 10000; with multi-tenancy is enabled and when reloaded.	

Defects closed with code in ServerIron ADX 12.5.02g

Defect ID: DEFECT000567135	
Technical Severity: Medium	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** Layer 2
Reported In Release: SI 12.4.00	**Technology Area:** Static Trunk
Symptom: Outgoing server facing traffic was not balanced among the configured trunk ports.	
Condition: ADX did not balance the outgoing traffic among the trunk ports which are connected to the real servers.	

Defect ID: DEFECT000571050	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Layer 2
Reported In Release: SI 12.5.01	**Technology Area:** IEEE 801.2w RSTP
Symptom: ADX sends packet out on RSTP ALTERNATE port, causing mac flap on upstream. HA sends advertisement packets and periodic inter-switch keep-alive message on CONTROL VLAN which causes mac flap on upstream.	
Condition: The HA logic scans all the valid VLANs and sends a packet out on each such VLAN including control VLAN. Control VLAN is used for special purpose like sending control packets for protocol like LACP.	

Defect ID: DEFECT000571941	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Server Load Balancing
Reported In Release: SI 12.4.00	**Technology Area:** Source-NAT
Symptom: Source-NAT source port exhaustion messages are not logged by default.	
Condition: Source port exhaustion messages for SNAT are not logged by default. It will be printed only when it is enabled.	

Defect ID: DEFECT000572609	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** Stateful SLB
Symptom: Multi Tenancy SLB packet drops to tenant after VRRP-E failover	
Condition: When ECMP OSPF routes are installed, Multi Tenancy SLB packet are dropped after failover.	

Defect ID: DEFECT000575912	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Layer 2
Reported In Release: SI 12.4.00	**Technology Area:** ARP
Symptom: After reload, ServerIron ADX is not sending health check packets to some IPv6 real servers.	
Condition: Issue is observed after configuring more than 20 IPv6 servers.	

Defect ID: DEFECT000577046	
Technical Severity: Medium	**Probability:** Low
Product: Brocade ServerIron ADX	**Technology:** Server Load Balancing
Reported In Release: SI 12.3.01	**Technology Area:** Configuration Synchronization
Symptom: Customer cannot re-add a real server which was deleted before. Some ports in the real server gets stuck in graceful shutdown queue.	
Condition: Issue is seen in very rare condition while deleting a real server.	

Defect ID: DEFECT000577301	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Management
Reported In Release: SI Virtual ADX 3.1.00	**Technology Area:** XML API
Symptom: GSLB WSDL is not accessible through http url (http://<ADX IP>/wsdl/gslb_service.wsdl).	
Condition: GSLB XMLAPIs are accessible through GUI.	

Defect ID: DEFECT000577513	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** System
Reported In Release: SI 12.5.02	**Technology Area:** Component
Symptom: USB map file entries are present even after removal of the SSL certificate/key files from the system. Deleted files are shown with prefix symbol '*'.	
Condition: When the user tries to delete the SSL certificate and key files, the files are deleted and stale entry present in USB map. Show SSL command does not show these deleted files.	

Defect ID: DEFECT000579003	
Technical Severity: Critical	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** Web Management
Symptom: ServerIron ADX may experience a system reset under rare circumstances, when a rouge user tries to access ADX over web management and gets auto-locked out.	
Condition: Observed the issue with same credential after user lock out.	

Defect ID: DEFECT000579522	
Technical Severity: Medium	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** System
Reported In Release: SI 12.4.00	**Technology Area:** CLI
Symptom: External TCAM counters are able to exceed beyond configured External TCAM value.	
Condition: Issue is applicable if External TCAM counter reaches Maximum configured External TCAM value.	

Defect ID: DEFECT000579524	
Technical Severity: Medium	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** System
Reported In Release: SI 12.4.00	**Technology Area:** CLI
Symptom: TCAM (Ternary Content Addressable Memory) entry count shows incorrect value when more than one line-card is used in ServerIron ADX-4K and ServerIron ADX-10K systems. This counter shows as actual count multiplied by the number of line-cards in the system	
Condition: The issue is applicable for only ServerIron ADX-4K and ServerIron ADX-10K systems when more than one line-card is used.	

Defect ID: DEFECT000579641	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** SSH - Secure Shell
Symptom: Under rare circumstances, ServerIron ADX may experience a system reset during SSH session termination.	
Condition: In rare cases SSH termination induces double free of memory resulting in system reset.	

Defect ID: DEFECT0005710013	
Technical Severity: Critical	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** System
Reported In Release: SI 12.5.01	**Technology Area:** Component
Symptom: ServerIron ADX may experience an Application CPU reset when an Openscript with 'Sub::StrictDecl' is being bound to a virtual server port.	
Condition: As user binds an OpenScript with 'Sub::StrictDecl' to a virtual server port.	

Defect ID: DEFECT0005710027	
Technical Severity: Critical	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.01	**Technology Area:** Health Checks
Symptom: After the Application CPU on ServerIron ADX experiences a reset and comes back up, user may experience traffic failure when accessing a virtual server.	
Condition: After application CPU resets, it is unable to program MAC address for some of the servers. This causes the real server's MAC to be shown as 'unknown' on the Application CPU.	

Defect ID: DEFECT000580529	
Technical Severity: High	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** NAT
Reported In Release: SI 12.5.02	**Technology Area:** Stateful NAT
Symptom: UDP traffic is not successful during outside to inside NAT.	
Condition: ServerIron ADX fails to send UDP traffic when outside to inside NAT is performed.	

Defect ID: DEFECT000580695	
Technical Severity: High	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** Configuration Synchronization
Symptom: ServerIron partner ADX fails to switch to the receiver mode even after the interface has come UP.	
Condition: In some rare cases ServerIron partner ADX stays in Sender mode even after the interface is enabled.	

Defect ID: DEFECT000581279	
Technical Severity: High	
Product: Brocade ServerIron ADX	
Reported In Release: SI 12.5.02	**Technology Area:** SSH - Secure Shell
Symptom: Customer may experience an Management Processor Reset while executing "crypto random-number-seed generate"	
Condition: When the user executes "crypto random-number-seed generate" command	

Defect ID: DEFECT000581787	
Technical Severity: High	
Product: Brocade ServerIron ADX	
Reported In Release: SI 12.5.01	**Technology Area:** VRRP & VRRP-E (IPv4)
Symptom: Enhancing the existing "show ip vrrp-e stat" command output to include additional counters.	
Condition: Enhancement to add additional counters in "show ip vrrp-e stat".	

Defect ID: DEFECT000581919	
Technical Severity: High	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** Configuration Synchronization
Symptom: ServerIron ADX Syncs disabled interface details to its partner ADX.	
Condition: During the config Sync Serveriron ADX syncs the interface details even for the disabled interfaces.	

Defect ID: DEFECT000582054	
Technical Severity: High	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** Layer 3
Reported In Release: SI 12.4.01	**Technology Area:** Other IPv4
Symptom: Non-head fragmented IPv4 packet can get dropped and Rx buffer used for the same packet can be leaked if ADX also processes Native IPv6 fragmented traffic at the same time.	
Condition: Issue happens during the combination of native IPv6 non head fragments send to ADX followed by IPv4 non head fragments. Packet rate should exceed 2500 fragmented packets/sec for both IPv4 and IPv6 fragments.	

Defect ID: DEFECT000582213	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Security
Reported In Release: SI 12.4.01	**Technology Area:** Secure Socket Layer (SSL) Acceleration
Symptom: CA certificate file is not getting upload when there is a <CR><LF>.	
Condition: ServerIron ADX fails to upload the CA certificate when there is a null line between the two certificates.	

Defect ID: DEFECT000582512	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** SSH - Secure Shell
Symptom: ServerIron ADX throws improper SYSLOG messages when the SSH connection is terminated or timed out.	
Condition: Improper syslog messages are sent only when SSH connections are terminated or times out.	

Defect ID: DEFECT000583569	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Layer 2
Reported In Release: SI 12.5.02	**Technology Area:** Static Trunk
Symptom: Packets are distributed to different ports in trunk group even when it is single Source /Destination IP pair.	
Condition: When TCP SYN-PROXY is configured, ServerIrin ADX shows a unequal/unusual pattern in traffic distribution among the trunk ports. As per the document, for SYN PROXY enabled/SLB traffic ADX will only use the Source /Destination IP for traffic distribution.	

Defect ID: DEFECT000583572	
Technical Severity: Medium	**Probability:** Mediu m
Product: Brocade ServerIron ADX	**Technology:** Layer 3
Reported In Release: SI 12.4.01	**Technology Area:** Other IPv4
Symptom: Customer is unable to track fragmentation packet processing using 'show server debug' command.	
Condition: Included additional counters to track fragmentation packet processing in 'show server debug' command.	

Defect ID: DEFECT000583728	
Technical Severity: Critical	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Management
Reported In Release: SI Virtual ADX 3.1.01	**Technology Area:** System Management
Symptom: Management process resets and becomes unstable due to buffer depletion	
Condition: Happens when trying to establish a connection from a non-BGP peer to vADX's port 179	

Defect ID: DEFECT000586148	
Technical Severity: Critical	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** System
Reported In Release: SI 12.4.00	**Technology Area:** Component
Symptom: IPC checksum error seen on packet received on Application processor resulting in reset without any core dump.	
Condition: Likely a HW issue	

Defect ID: DEFECT000588467	
Technical Severity: High	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** Security
Reported In Release: SI 12.4.00	**Technology Area:** SYN-proxy/SYN-defense
Symptom: Optimized SLB traffic doesn't work when SYN-PROXY feature is enabled and DA VLAN table is full.	
Condition: Issue is seen only when SYN-PROXY feature enabled and with optimized SLB feature when DA VLAN table is full.	

Defect ID: DEFECT000589333	
Technical Severity: Critical	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** Layer 2
Reported In Release: SI 12.5.02	**Technology Area:** ARP
Symptom: ServerIron ADX does not refresh MAC age and ages out the MAC entry of the gateway even with continuous traffic	
Condition: ServerIron ADX fails to refresh the MAC age of default gateway	

Defect ID: DEFECT000590949	
Technical Severity: High	**Probability:** High
Product: Brocade ServerIron ADX	**Technology:** System
Reported In Release: SI 12.5.01	**Technology Area:** CLI
Symptom: CLI command "server set-hw-buf-usage-threshold" accepts the threshold value in the range of 1-512 instead of 1-65535.	
Condition: User tries to setup hardware buffer usage threshold, to monitor if hardware buffer usage is more than a configurable threshold value.	

Defect ID: DEFECT000591547	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** XML API
Symptom: Support for XML API disable real server port health check is missing for h/w adx	
Condition: Only the XML API support for disable real server port health check is missing.	

Defect ID: DEFECT000593897	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.01	**Technology Area:** SLB Predictors
Symptom: Configuration related to associated backup-server feature was not synced from Management Processor to Application processor for some of the servers after a system restart.	
Condition: Observed if we try to configure back-up port configuration before configure the real server configuration at boot-up time.	

Defect ID: DEFECT000594178	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** SSL Termination
Symptom: Added additional counters under "show ssl mem" and "show ssl heap-summary".	
Condition: The commands are used to turn on/off shared buffer leak detection and print debug data for potentially leaking buffer track and content, SSL PCIe memory management track and content.	

Defects closed with code in ServerIron ADX 12.5.02f

Defect ID: DEFECT000530089	
Technical Severity: High	**Probability:** High
Product: Brocade ServerIron ADX	**Technology Group:** NAT
Reported In Release: SI Virtual ADX 3.1.01	**Technology:** Stateful NAT
Symptom: ServerIron ADX does not program L4-7 CAM entries for Virtual Server IP correctly when Virtual Server name or NAT pool names first three letters are "NAT".	
Condition: Virtual Server and NAT IP is same;	
Workaround: Do not use the VIP and NAT Pool name starting with word "NAT".	

Defect ID: DEFECT000531057	
Technical Severity: High	**Probability:** High
Product: Brocade ServerIron ADX	**Technology Group:** Layer 3
Reported In Release: SI 12.5.01	**Technology:** Other IPv4
Symptom: High CPU may be observed on the Management CPU.	
Condition: The issue may be seen when customer has high number of virtual servers configured along with multiple IP addresses under interfaces.	
Workaround: The CPU utilization can be reduced by disabling L2 and L3 periodic health-checks and increasing the interval of L4 health-checks.	

Defect ID: DEFECT000533245	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology Group:** Layer 2
Reported In Release: SI 12.5.01	**Technology:** ARP
Symptom: add_ip_host_route error logs seen in MT setup during ARP learning	
Condition: MT setup; pass-through traffic; tenant looks to resolve ARP for pass-through traffic	

Defect ID: DEFECT000561457	
Technical Severity: Critical	**Probability:** High
Product: Brocade ServerIron ADX	**Technology Group:** Server Load Balancing
Reported In Release: SI 12.5.02	**Technology :** Policy-based SLB
Symptom: Traffic sent to single real server when csw policy is bound to Virtual Server port even if sticky is not configured for the port.	
Condition: Issue happens only when the csw policy is bound to Virtual port.	

Defect ID: DEFECT000562044	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology Group:** Layer 2
Reported In Release: SI 12.5.01	**Technology:** ARP
Symptom: ServerIron ADX does not remove MAC addresses from the MAC table even when there is no traffic from these MAC addresses for more than mac-age value or after aged out.	
Condition: When pumping high traffic using traffic generator in High Availability configuration with hardware mac aging is enabled in non-multitenancy mode, ServerIron ADX keeps learning MAC addresses and stores in its MAC table. After stopping the traffic, the learned MAC addresses are not removed from MAC table even when there is no traffic and age for those MAC entries are exceeded.	

Defect ID: DEFECT000563954	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology Group:** Server Load Balancing
Reported In Release: SI 12.4.00	**Technology:** DSR
Symptom: In active mode FTP, client is able to connect the server and subsequent data connection fails when L3DSR is configured in the ServerIron ADX.	
Condition: Issue happens only if L3DSR is configured and Virtual Server port has two or more real servers bound to it.	
Workaround: Binding default Virtual Server port with default real server ports.	

Defect ID: DEFECT0005642100	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology Group:** Layer 3
Reported In Release: SI 12.4.00	**Technology :** VRRP & VRRP-E (IPv6)
Symptom: Tunnel traffic is not forwarded to destination device when ServerIron ADX VRRP-E IP is configured as a default route on vRouter	
Condition: VRRP-E ip was not pingable from the vRouter.	

Defect ID: DEFECT000564554	
Technical Severity: Medium	**Probability:** High
Product: Brocade ServerIron ADX	**Technology Group:** Management
Reported In Release: SI 12.5.01	**Technology:** Configuration Synchronization
Symptom: Executing 'Config sync diff' functionality resets the ServerIron ADX when huge config exists in multi tenancy.	
Condition: Issue happens only at sender side when huge config exists in multi tenancy mode.	

Defect ID: DEFECT000565256	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology Group:** Layer 3
Reported In Release: SI 12.5.02	**Technology:** Other IPv4
Symptom: show arp displays "-" in MAC address for some host and ADX does not have IP reachability for this host.	
Condition: This issue happens when ARP entry with invalid MAC is created. Since it is a Invalid MAC interface does not have IP reachability.	

Defect ID: DEFECT0005660100	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology Group:** Server Load Balancing
Reported In Release: SI 12.5.01	**Technology:** Layer 7 Content Switching
Symptom: Pseudo stack L7 SLB Application processor resets when processing client side OOS packets	
Condition: The primary ServerIron ADX stopped working and an automatic failover did not occur.	

Defect ID: DEFECT000566333	
Technical Severity: High	**Probability:** High
Product: Brocade ServerIron ADX	**Technology Group:** Server Load Balancing
Reported In Release: SI 12.5.01	**Technolo gy:** Health Checks
Symptom: While performing health checks in keepalive mode and when server sends TCP RST in response to TCP SYN, ServerIron ADX continues to send TCP SYN at keepalive interval for configured number of retries before marking the port DOWN.	
Condition: General health check request	

Defect ID: DEFECT000566337	
Technical Severity: High	**Probability:** High
Product: Brocade ServerIron ADX	**Technology Group:** Management
Reported In Release: SI 12.5.01	**Technology:** Configuration Synchronization
Symptom: Under rare circumstances, a receiver tenant may experience Application CPU reset when 'config-sync full' is executed on the sender tenant.	
Condition: ServerIron ADX is configured with multi-tenancy and config-sync. Full configuration sync is initiated on sender tenant.	

Defect ID: DEFECT000567153	
Technical Severity: High	**Probability:** High
Product: Brocade ServerIron ADX	**Technology Group:** System
Reported In Release: SI 12.5.01	**Technology:** Component
Symptom: Application Processors are not coming up on the tenants.	
Condition: Issue observed while issuing the "config -sync full" on the sender tenant.	

Defect ID: DEFECT000567506	
Technical Severity: High	**Probability:** High
Product: Brocade ServerIron ADX	**Technology Group:** Server Load Balancing
Reported In Release: SI 12.5.01	**Technology:** VIP RHI
Symptom: ServerIron ADX marks SLB state as "Not Healthy" for virtual server port, even at least one of the bound port is Active.	
Condition: Issue observed only when track port is configured.	

Defect ID: DEFECT000567519	
Technical Severity: Medium	**Probability:** High
Product: Brocade ServerIron ADX	**Technology Group:** Management
Reported In Release: SI 12.4.00	**Technology:** SNMPv2, SNMPv3 & MIBs
Symptom: Dynamic memory relation information such as, Total Physical Memory, Available Physical Memory, Max Heap-Master MP, Available Heap-Master MP, Heap Usage-Master MP were not in line with CLI output when retrieving using SNMP command. Added missing OIDs to display memory related information.	
Condition: Added new OIDs to display dynamic memory relation information from SNMP command. Now SNMP output is in line with CLI output.	

Defect ID: DEFECT000568817	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology Group:** Server Load Balancing
Reported In Release: SI 12.4.00	**Technology:** Health Checks
Symptom: ServerIron ADX box may get reloaded if SSL health check URL updated on the fly	

Condition: Issue will only appear if SSL health check URL is updated when particular health check component is active.

Defect ID: DEFECT000569076	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology Group:** Management
Reported In Release: SI 12.5.02	**Technology:** Web Management
Symptom: New strong SSL/TLS ciphers are not configurable nor visible in web GUI	
Condition: Missing feature in UI	

Defect ID: DEFECT000569134	
Technical Severity: Medium	**Probability:** High
Product: Brocade ServerIron ADX	**Technology Group:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.01	**Technology:** SSL Ciphers
Symptom: SSL Proxy configuration is lost after upgrading from ServerIron ADX patch release12501h to 12501j or later	
Condition: Issue is seen only when both the following conditions are met 1. When upgrading from below versions of ServerIron ADX 12501j to 12501j or later versions. 2. Before upgrade, if SSL proxy server profile is not configured with cipher-suites.	

Defect ID: DEFECT0005692100	
Technical Severity: High	**Probability:** High
Product: Brocade ServerIron ADX	**Technology Group:** Server Load Balancing
Reported In Release: SI 12.5.01	**Technology:** Stateful SLB
Symptom: Non head fragmented packets are stored in frag queue for 0.2 seconds or less.	
Condition: Issue happens only for out of order fragmentation case	

Defect ID: DEFECT000569526	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology Group:** System
Reported In Release: SI 12.5.02	**Technology:** Component
Symptom: MAC entry gets removed earlier than configured MAC aging value which should be in line with the configured value.	
Condition: MAC entry gets removed when clearing internal flag	

Defect ID: DEFECT0005610022	
Technical Severity: Medium	**Probability:** High
Product: Brocade ServerIron ADX	**Technology Group:** Management
Reported In Release: SI 12.5.01	**Technology:** System Management
Symptom: Time mismatch in RTC clock and syslog time stamp	
Condition: Time mismatch in show clock command output and syslog time stamp	

Defect ID: DEFECT000570823	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology Group:** Server Load Balancing
Reported In Release: SI 12.4.00	**Technology:** Layer 7 Content Switching
Symptom: Configuration of SYM-ACTIVE on virtual server and CSW on one of the virtual server ports lead to undesired behavior on ADX	
Condition: Issue happens only on SYM-ACTIVE and CSW configured for the VIP and its port.	

Defect ID: DEFECT000571763	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology Group:** Management
Reported In Release: SI 12.5.02	**Technology:** Web Management
Symptom: Virtual Server status for all the Virtual servers are shown as unknown in SSL Profiles Page of Web GUI	
Condition: While configuring SSL profile bindings, Virtual Server status for all the Virtual Servers are not shown properly in the Web GUI.	

Defect ID: DEFECT000571776	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology Group:** Server Load Balancing
Reported In Release: SI 12.4.00	**Technology :** Layer 7 Content Switching
Symptom: BP is getting restarted while sending HTTP request to real port which is bound with CSW + sym-active enabled virtual server port.	
Condition: Issue happens only when source NAT port pool is depleted.	

Defect ID: DEFECT000572128	
Technical Severity: Critical	**Probability:** High
Product: Brocade ServerIron ADX	**Technology Group:** System
Reported In Release: SI 12.5.02	**Technology:** Component
Symptom: ServerIron ADX will get reloaded upon issuing CLI command "usb format 0" in 12.5.02.e version.	
Condition: "usb format 0" is executed when eventlog feature is enabled on ServerIron ADX	
Workaround: Disable eventlog feature on ServerIron ADX box	

Defect ID: DEFECT000573526	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology Group:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology:** SSL Proxy
Symptom: SSL-Proxy server side TLS 1.2 handshake fails when TCP FIN close is sent to server socket after server hello.	
Condition: If SSL server hello split over 4 TCP segments when using SSL Proxy.	

Defect ID: DEFECT000573919	
Technical Severity: Medium	**Probability:** High
Product: Brocade ServerIron ADX	**Technology Group:** Management
Reported In Release: SI 12.4.00	**Technology:** XML API
Symptom: XMLAPI fails to display URL details when nonstandard ports are configured for real server.	
Condition: XMLAPI Fails to display URL only when configuring nonstandard ports for real server.	

Defect ID: DEFECT000573920	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology Group:** Monitoring/RAS
Reported In Release: SI 12.5.01	**Technology:** Syslog
Symptom: In a rare circumstance, ServerIron ADX reloads during syslog generation.	
Condition: Happens only in very rare scenario when syslog is generated	

Defect ID: DEFECT000574594	
Technical Severity: Critical	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology Group:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology:** SSL Proxy
Symptom: ServerIron ADX Client Hello should only send supported elliptical curve.	
Condition: When ServerIron ADX sends unsupported elliptical curve in the client hello.	

Defect ID: DEFECT000575281	
Technical Severity: High	**Probability:** High
Product: Brocade ServerIron ADX	**Technology Group:** Server Load Balancing
Reported In Release: SI 12.5.01	**Technology:** Stateful SLB
Symptom: When ServerIron ADX receives head fragment and non-head fragment on different BPs but on same AXP then non-head fragment is not forwarded correctly to flow BP	
Condition: Issue applicable only for 10U	

Defect ID: DEFECT000576940	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology Group:** System
Reported In Release: SI 12.4.00	**Technology:** Component
Symptom: A user reported some of the VIPs and servers being down due to Application CPU reset.	
Condition: This issue is occurring in very rare scenario and is a timing issue.	

Defect ID: DEFECT000577153	
Technical Severity: High	**Probability:** Medium
Product: Brocade ServerIron ADX	**Technology Group:** Layer 2
Reported In Release: SI 12.5.02	**Technology:** LACP
Symptom: While removing and adding back the LAG interface ServerIron ADX Management Processor resets	
Condition: ServerIron ADX failed to handle the request and caused the ServerIron ADX Management Processor reset, when the interface connected to LAG was removed and added back again to the LAG group.	

Defects closed with code in ServerIron ADX 12.5.02e

Defect ID: DEFECT000558683	
Technical Severity: Medium	**Probability:** Medium
Product: ServerIron	**Technology:** Layer 2
Reported In Release: SI 12.5.01	**Technology Area:** ARP
Symptom: HSRP default gateway ARP entry flushes after changing trunk port vlan membership	
Condition: Device loses its ARP entry to the default gateway as soon as we add the vlan to the existing trunk. This makes the device inaccessible or hung for few seconds till the time it gets the response from upstream router for the new ARP query.	

Defect ID: DEFECT000559377	
Technical Severity: Medium	**Probability:** High
Product: ServerIron	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** XML API
Symptom: getSlbGlobalConfiguration API session limit value is not matching actual configured value. And Packet Fragmentation and enableReassignIgnoreServerReset fields in the API were not working as designed.	
Condition: Some of the fields in the APIs were not working as designed.	

Defect ID: DEFECT000559473	
Technical Severity: Medium	**Probability:** High
Product: ServerIron	**Technology:** Management
Reported In Release: SI 12.4.00	**Technology Area:** XML API
Symptom: XML GUI API does not allow configuring track-group under virtual server configuration.	
Condition: Issue occurs even after selecting Track Group option during virtual server configuration	

Defect ID: DEFECT000559478	
Technical Severity: High	**Probability:** Medium
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.4.00	**Technology Area:** Stateful SLB
Symptom: When all the SLB bindings for a server are removed from the configuration on the ServerIron ADX, traffic from that server may still be received by the ServerIron ADX causing an increase in CPU utilization on the application CPUs.	
Condition: All SLB bindings of a Server are removed from the ServerIron ADX configuration, either by unbinding the ports or deleting the VIPs.	
Workaround: If possible, delete the real server before deleting VIP or unbinding real server ports.	

Defect ID: DEFECT000560163	
Technical Severity: Critical	**Probability:** Low
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.4.00	**Technology Area:** Health Checks
Symptom: Customer may see system reset or some time stack trace debug messages.	
Condition: Start sending keep-alive messages from real servers and do the below configurations repetitively. port radius no-health-check no port radius no-health-check port radius no-health-check no port radius no-health-check port radius no-health-check no port radius no-health-check	

Defect ID: DEFECT000560285	
Technical Severity: Medium	**Probability:** Medium
Product: ServerIron	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** L7 SSL
Symptom: ServerIron ADX caused APP CPU to reset when receiving random client connection to a VIP configured with SSL-terminate and CSW.	
Condition: Heap memory usage hit peak level. Client accessing VIP configured with SSL-terminate and CSW.	
Workaround: Avoid using TLS1.2 with AES and DES cipher suites	

Defect ID: DEFECT000560822	
Technical Severity: High	**Probability:** Medium
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.3.01	**Technology Area:** Stateless SLB
Symptom: Application CPU on the ServerIron ADX may reset while processing DNS traffic on a Virtual Port configured for Stateless SLB if there was a TCP SYN flood attack on the ServerIron ADX.	
Condition: TCP SYN attack causing the session table to be full; Stateless SLB configured for DNS; New connection request received for the DNS Virtual Port.	
Workaround: Configure either SYN-Proxy or TRL (Transaction Rate Limiting) to limit the session exhaustion.	

Defect ID: DEFECT000561138	
Technical Severity: Medium	**Probability:** Medium
Product: ServerIron	**Technology:** Multitenancy
Reported In Release: SI 12.5.02	**Technology Area:** Tenant Provisioning
Symptom: Although tenant resource profile permits configuring maximum usb flash size parameter upto 16GB, it does not take effect for size more than 4GB upon binding resource profile with tenant and does not throw any error message.	
Condition: This issue is seen when tenant max usb flash size configuration value exceeds 4096MB.	

Defect ID: DEFECT000561525	
Technical Severity: Medium	**Probability:** Medium
Product: ServerIron	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** Web Management
Symptom: SSL certificates with validity beyond year ~2028 shown as expired in GUI.	
Condition: Issue observed only for SSL certificates with validity beyond year ~2028.	

Defect ID: DEFECT000561704	
Technical Severity: Medium	**Probability:** Medium
Product: ServerIron	**Technology:** Management
Reported In Release: SI 12.5.01	**Technology Area:** Web Management
Symptom: When user imports cert/key for HTTPS WEB Management (This is done via TFTP commands) then new HTTP WEB Management connections do not work and ADX sends TCP RST once it is done sending Server Hello.	
Condition: Default certificate is already generated. New certificate is imported onto ServerIron ADX. The imported certificate size is more than 2 KB. User makes HTTPS connections to WEB GUI Management.	
Workaround: Write mem and reload ADX.	

Defect ID: DEFECT000561943	
Technical Severity: Critical	**Probability:** High
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** Stateful SLB
Symptom: ServerIron ADX does not allow to bind SSL port (443) for 664 SLB (IPv6 VIP with IPv4 Server) or 446 SLB (IPv4 VIP with IPv6 Server) for L4 SLB.	
Condition: 664/446 SLB binding with Layer4 SSL (SSL Pass-through)	

Defect ID: DEFECT000562042	
Technical Severity: Critical	**Probability:** Medium
Product: ServerIron	**Technology:** Layer 3
Reported In Release: SI 12.5.01	**Technology Area:** VRRP & VRRP-E (IPv4)
Symptom: When a ServerIron ADX becomes VRRP-E Master it does not route the pass-through non-SLB traffic as it fails to program VRRP-E MAC on the line card as a "owner".	
Condition: ServerIron ADX becomes VRRP-E Master. Gratuitous ARP is received from the partner ADX. Management CPU is under High CPU load.	
Recovery: Deactivate/Activate VRRP-E instance again.	

Defect ID: DEFECT000562043	
Technical Severity: Critical	**Probability:** Medium
Product: ServerIron	**Technology:** Layer 3
Reported In Release: SI 12.5.01	**Technology Area:** VRRP & VRRP-E (IPv4)
Symptom: When a ServerIron ADX becomes VRRP-E Master it does not route the SLB or pass-through traffic from the servers as it fails to program VRRP-E MAC on Application CPU as a "owner".	
Condition: ServerIron ADX becomes VRRP-E Master. Gratuitous ARP is received from the partner ADX. Management CPU is under High CPU load.	
Recovery: Deactivate/Activate VRRP-E instance again.	

Defect ID: DEFECT000562225	
Technical Severity: High	**Probability:** High
Product: ServerIron	**Technology:** Layer 2
Reported In Release: SI 12.4.00	**Technology Area:** Static Trunk
Symptom: ServerIron ADX does not distribute the Return SLB traffic (Server -> Client) evenly across the trunk ports.	
Condition: CSW is configured; Trunk ports are configured.	

Defect ID: DEFECT000562500	
Technical Severity: Critical	**Probability:** Medium
Product: ServerIron	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** SSH - Secure Shell
Symptom: ServerIron resets when a user executes a CLI command "crypto random-number-seed generate"	
Condition: ServerIron resets when a user executes a CLI command "crypto random-number-seed generate"	

Defect ID: DEFECT000562742	
Technical Severity: High	**Probability:** High
Product: ServerIron	**Technology:** Global Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** GSLB Controller
Condition: GSLB Config-Sync is enabled and user configures a master weight of 255 or more.	

Defect ID: DEFECT000562818	
Technical Severity: Medium	**Probability:** Medium
Product: ServerIron	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** System Management
Symptom: Management CPU utilization spikes up when a user executes summary command in a "debug filter" mode and there are around 200K packets captured.	
Condition: Management CPU utilization spikes up when a user executes summary command in a "debug filter" mode and there are around 200K packets captured.	
Workaround: Use smaller buffer size and define granular filter rules so as the number of packets captured are less than 10K.	

Defect ID: DEFECT000562837	
Technical Severity: Medium	**Probability:** High
Product: ServerIron	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** Web Management
Symptom: Web GUI does not display more than 10 certificates in "Append to" dropdown field.	
Condition: Issue is seen after creating more than 10 certificates in ADX and clicking on "Append to" dropdown field.	

Defect ID: DEFECT000563851	
Technical Severity: Critical	**Probability:** High
Product: ServerIron	**Technology:** Global Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** Secure GSLB
Symptom: ServerIron performs system reset when configuring secure GSLB for a GSLB site	
Condition: ServerIron performs system reset when configuring secure GSLB for a GSLB site	

Defect ID: DEFECT000564550	
Technical Severity: High	**Probability:** Medium
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.01	**Technology Area:** Layer 7 Content Switching
Symptom: Eventlog file fills up with URL-HA error messages such as below leaving less space for other messages.. "KA: response not end at packet end(0x400ecd7e, > </html> , 0x400ecd8c)! Change to UNKNOWN! "; "URL-HA: KA Error: URL recv ASP KA_status, server tcb null"	
Condition: CSW and High Availability is configured and eventlog is enabled.	

Defects closed with code in ServerIron ADX 12.5.02d

Defect ID: DEFECT0004638100	
Technical Severity: High	**Probability:** Low
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.01	**Technology Area:** VIP RHI
Symptom: System reset noticed when VIP RHI is enabled with vip-route-subnet-mask-length configured to less than 64.	
Condition: "VIP RHI should be enabled with vip-route-subnet-mask-length configured to less than 64. System reset is not seen if vip-route-subnet-mask-length configured to more than or equal to 64."	

Defect ID: DEFECT000533254	
Technical Severity: Medium	**Probability:** Medium
Product: ServerIron	**Technology:** Management
Reported In Release: SI 12.4.00	**Technology Area:** AAA
Symptom: The command "enable <super-user-password>" does not honor super-user privilege level and instead gives read only access	
Condition: The issue happens only when the user provides the password along with "enable <password>" command.	
Workaround: The user can get the correct privilege by giving only "enable" command and provide the password when it is requested by ADX.	

Defect ID: DEFECT000533419	
Technical Severity: Medium	**Probability:** Low
Product: ServerIron	**Technology:** Management
Reported In Release: SI 12.4.00	**Technology Area:** XML API
Symptom: "save tech" and pcap files generated for XMLAPI/GUI on the ServerIron ADX are accessible without user login credentials.	
Condition: Only temporary files generated for webGUI/XMLAPIs only are accessible.	

Defect ID: DEFECT000545243	
Technical Severity: Medium	**Probability:** Medium
Product: ServerIron	**Technology:** Management
Reported In Release: SI 12.4.00	**Technology Area:** SSH - Secure Shell
Symptom: SSH session is not terminated as long as receiving SSH keepalive after the configured "ip ssh idle-time" elapses.	
Condition: SSH keep-alive configured on the ServerIron ADX; SSH session to manage the ServerIron ADX.	
Workaround: Disable SSH keep-alive.	

Defect ID: DEFECT000551120	
Technical Severity: High	**Probability:** Medium
Product: ServerIron	**Technology:** Security
Reported In Release: SI 12.4.00	**Technology Area:** Security Vulnerability
Symptom: SSL termination of the application traffic on the ServerIron ADX could be susceptible to OpenSSL vulnerabilities.	
Condition: SSL Terminate or Proxy configured on the ServerIron ADX. Following are the specific vulnerabilities: CVE-2015-0204 (Reclassified: RSA silently downgrades to EXPORT_RSA) CVE-2015-0286 (Segmentation fault in ASN1_TYPE_cmp) CVE-2015-0287 (ASN.1 structure reuse memory corruption) CVE-2015-0288 (X509_to_X509_REQ NULL pointer deref) CVE-2015-0289 (PKCS7 NULL pointer dereferences) CVE-2015-0292 (Base64 decode) CVE-2015-0293 (DoS via reachable assert in SSLv2 servers) CVE-2015-0209 (Use After Free following d2i_ECPrivatekey error)	

Defect ID: DEFECT000551963	
Technical Severity: Medium	**Probability:** High
Product: ServerIron	**Technology:** Management
Reported In Release: SI 12.4.00	**Technology Area:** SNMPv2, SNMPv3 & MIBs
Symptom: Unsupported command "no snmp-server enable traps locked-addr" is added in the default configuration.	
Condition: Unsupported CLI global command "no snmp-server enable traps locked-addr" is always shown in default configuration.	

Defect ID: DEFECT000552924	
Technical Severity: Medium	**Probability:** Medium
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** Session Management
Symptom: In a Hot-Standby High-Availability setup with Layer7 CSW configured, the Standby ADX may notice high current connection counter.	
Condition: Hot-Standby High-Availability setup of ServerIron ADX; Layer7 SLB enabled with a CSW policy; client sends multiple HTTP requests over the same connection that are forwarded to different real servers; The output of "show server virtual vs_name" may show the curconn counter increasing incorrectly on the Standby ADX while that counter works fine on the Active ADX.	

Defect ID: DEFECT000554241	
Technical Severity: Medium	**Probability:** Medium
Product: ServerIron	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** SSL Termination
Symptom: With SSL Terminate/Proxy configured on the ServerIron ADX, download of large files may fail with a TCP RESET of the server connections.	
Condition: SSL Terminate/Proxy configured on the ServerIron ADX; Client sends new request on the same SSL session while the Real Server is responding with large amount of data for the previous request.	

Defect ID: DEFECT000556068	
Technical Severity: High	**Probability:** Medium
Product: ServerIron	**Technology:** Management
Reported In Release: SI 12.5.01	**Technology Area:** System Management
Symptom: Config file can get lost if user enters "write mem" under low memory condition.	
Condition: This can happen if system is using near 100.100% of available memory.	
Workaround: Wait a bit of time till memory usage becomes lower and enter "write mem" again.	

Defect ID: DEFECT000556223	
Technical Severity: Medium	**Probability:** Medium
Product: ServerIron	**Technology:** Global Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** GSLB Controller
Symptom: The secondary ADX throws dynamic resource allocation failure logs every 5 seconds.	
Condition: Log throws for VIP server configured with low sym priority in redundant setup.	

Defect ID: DEFECT000556470	
Technical Severity: Low	**Probability:** Medium
Product: ServerIron	**Technology:** Layer 3
Reported In Release: SI 12.4.00	**Technology Area:** Other IPv4
Symptom: The state of IP follow interface goes down after reloading the ServerIron ADX in "show interface" output, but the functionality of the followed interface works fine.	
Condition: IP follow interface configured on the ServerIron ADX; ServerIron ADX reload; User enters "show interface" display command.	
Recovery: Disable and enable the interface.	

Defect ID: DEFECT000556796	
Technical Severity: High	**Probability:** Medium
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.4.00	**Technology Area:** Health Checks
Symptom: SSL Layer7 content-match health-checks would fail for unknown port if the HTTP response is getting split into two packets and the actual text we are matching on is in the second packet.	
Condition: SSL Layer7 content-match health-checks configured on an unknown port, and the HTTP health-check response from the server is split into two packets with the matching test in the second packet.	

Defect ID: DEFECT000558822	
Technical Severity: Medium	**Probability:** Medium
Product: ServerIron	**Technology:** Management
Reported In Release: SI 12.5.01	**Technology Area:** Web Management
Symptom: While using the Web GUI to manage the ServerIron ADX, clicking and dragging the scroll bar in the 'Bound RS-Ports' box is not functional. However, mouse wheel scrolling works.	
Condition: Clicking and dragging the scroll bar in the 'Bound RS-Ports' box of the Web GUI.	

Defect ID: DEFECT000559095	
Technical Severity: Medium	**Probability:** Medium
Product: ServerIron	**Technology:** Management
Reported In Release: SI 12.5.01	**Technology Area:** Web Management
Symptom: Web UI fails to display vip port binding info if 9 or more real server ports are bound to vip port.	
Condition: When 9 or more real server ports are bound to vip port then binding info will not displayed on web UI.	

Defect ID: DEFECT000559154	
Technical Severity: Medium	**Probability:** Medium
Product: ServerIron	**Technology:** Management
Reported In Release: SI 12.4.00	**Technology Area:** System Management
Symptom: In Layer2 Switch mode, ServerIron ADX cannot synchronize with NTP server through a Management port.	
Condition: NTP client configured on the ServerIron ADX in Layer2 Switch mode.	

Defect ID: DEFECT000559410	
Technical Severity: Medium	**Probability:** Medium
Product: ServerIron	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** Configuration Synchronization
Symptom: Incremental config sync VIP name update only changes name of 1st VIP on receiver	
Condition: This issue pops up at receiver on config sync enabled HA setup.	

Defect ID: DEFECT000559460	
Technical Severity: Critical	**Probability:** Medium
Product: ServerIron	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.4.00	**Technology Area:** L7 SSL
Symptom: A Layer7 SLB connection may be reset when server sends "100 Continue".	
Condition: SSL Proxy and CSW configured on the ServerIron ADX; HTTP response message "HTTP/1.1 100 Continue" is split into multiple SSL records.	

Defect ID: DEFECT000560165	
Technical Severity: Critical	**Probability:** Medium
Product: ServerIron	**Technology:** System
Reported In Release: SI 12.5.01	**Technology Area:** CLI
Symptom: ServerIron ADX reset while displaying detailed CPU utilization.	
Condition: If the command "dm cput show utilization" is entered after the system has been up for over 16 hours.	
Workaround: Do not use the full show utilization command; Instead, use the command that shows individual sections of CPU utilization like "dm cput show util-summary", and "dm cput show util-pkts".	

Defect ID: DEFECT000560220	
Technical Severity: Critical	**Probability:** High
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** Multiple Port Binding
Symptom: Under some special circumstances, ServerIron ADX may perform system reset when the user is trying to unbind a real port from a multiple-bound virtual port.	
Condition: ServerIron ADX performs system reset under some special circumstances when the user is trying to unbind a real port from a multiple-bound virtual port.	

Defect ID: DEFECT000560815	
Technical Severity: Critical	**Probability:** Medium
Product: ServerIron	**Technology:** Management
Reported In Release: SI 12.5.01	**Technology Area:** System Management
Symptom: ServerIron ADX reset while displaying CPU utilization samples.	
Condition: Command "dm sample-on 1" to sample CPU utilization. This happens in rare cases when there are lots of PC samples collected due to system handling different kind of jobs during the sampling period.	

Defect ID: DEFECT000560818	
Technical Severity: High	**Probability:** Medium
Product: ServerIron	**Technology:** Management
Reported In Release: SI 12.5.01	**Technology Area:** System Management
Symptom: In case of CPU reset, the stack trace may not be displayed completely.	
Condition: CPU reset	

Defect ID: DEFECT000561106	
Technical Severity: Critical	**Probability:** High
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** Configuration Synchronization
Symptom: Entering "dir" command a couple of times under low memory condition can cause system reset. The command shows nothing.	
Condition: System is running under very low memory (100.100% used).	
Workaround: When seeing "dir" command showing nothing, avoid doing it again. Check memory (by "show mem" command) and do it again if there are at least a few percent left.	

Defect ID: DEFECT000561257	
Technical Severity: High	**Probability:** High
Product: ServerIron	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** SSL Termination
Symptom: SSL session caching fails on ServerIron ADX 4U/10U with multiple cryptographic chips.	
Condition: ServerIron ADX chassis 4U or 10U; SSL Terminate or Proxy configured on the ServerIron ADX; SSL session-caching enabled on the SSL profile.	

Defects closed with code in ServerIron ADX 12.5.02c

Defect ID: DEFECT000496837	
Technical Severity: High	**Probability:** Low
Product: ServerIron	**Technology:** Layer 2
Reported In Release: SI 12.5.00	**Technology Area:** ARP
Symptom: Failover on the real server NIC (hot standby) connected via cross-link to ADX HA pair (Sym-Active) results in the ADX ARP entry being pointed to the new interface and MAC entry to the old interface, leading to SLB traffic failure.	
Condition: ADX HA pair (Sym-Active mode) and Real server having dual NIC (hot-standby) connected to the ADX pair via cross-link.	
Recovery: Clear MAC for the MAC address for the server.	

Defect ID: DEFECT000515672	
Technical Severity: High	**Probability:** High
Product: ServerIron	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI Virtual ADX 3.1.00	**Technology Area:** SSL Ciphers
Symptom: Downloading SSL Key via GUI was resulting in an empty SSL key file	
Condition: Using the GUI for SSL Key download	

Defect ID: DEFECT000517132	
Technical Severity: Medium	**Probability:** Medium
Product: ServerIron	**Technology:** Other
Reported In Release: SI 12.4.00	**Technology Area:** Other
Symptom: When the IPv6 cache table is full and traffic comes in to ServerIron ADX that needs to create a new IPv6 cache entry, the traffic will be dropped.	
Condition: IPv6 cache table is full	

Defect ID: DEFECT000526664	
Technical Severity: Medium	**Probability:** High
Product: ServerIron	**Technology:** System
Reported In Release: SI 12.5.01	**Technology Area:** CLI
Symptom: In a Hot-Standby High-Availability setup, running "show task" command on a ServerIron ADX could generate a small spike and trigger fail-over.	
Condition: Hot-Standby High-Availability setup.	
Workaround: Run "show task" from the OS-level CLI rather than the Management CPU prompt.	

Defect ID: DEFECT000529662	
Technical Severity: Medium	**Probability:** High
Product: ServerIron	**Technology:** System
Reported In Release: SI 12.4.00	**Technology Area:** CLI
Symptom: If a Virtual Server is disabled but one of the Virtual Ports under that VIP is enabled, after executing "write mem" and "reload", the Virtual Port may stop processing SLB traffic.	
Condition: Virtual server is disabled and Virtual port is enabled.	
Recovery: Execute "no port <port> disable" for individual virtual ports, or execute "no disable" under the affected virtual server.	

Defect ID: DEFECT000530637	
Technical Severity: Medium	**Probability:** High
Product: ServerIron	**Technology:** System
Reported In Release: SI 12.4.00	**Technology Area:** CLI
Symptom: Commands containing "?" are saved in the CLI history.	
Condition: Using CLI command history to re-run previous commands.	

Defect ID: DEFECT0005331004	
Technical Severity: Medium	**Probability:** High
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.4.00	**Technology Area:** Health Checks
Symptom: When a real server port is bound to multiple VIPs, in Layer2 DSR setup, ADX sends separate health-checks destined to the different VIP IPs as expected. However, during the initial bring-up, if one of the health-checks fails, ADX marks all the VIPs as down.	
Condition: L2 DSR with multi-binding configured on the ADX.	

Defect ID: DEFECT000534956	
Technical Severity: Medium	**Probability:** Low
Product: ServerIron	**Technology:** Management
Reported In Release: SI 12.4.00	**Technology Area:** System Management
Symptom: Application CPU may reset while debugging high CPU using the embedded CPU profiler.	
Condition: User tries to enable CPU profiling using "asm dm cputracker spike-samples enable" on the Application CPU console. User then tries to display the actual profiling samples using "asm dm cputracker spike-samples show 1".	

Defect ID: DEFECT0005361100	
Technical Severity: Medium	**Probability:** High
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** Layer 7 Content Switching
Symptom: When Layer7 switching is configured on the ServerIron ADX and a CSW match rule is configured with redirect to port 80 and HTTP status code 302, ServerIron ADX will not redirect the request to the specified port.	
Condition: Layer7 switching configured on the ServerIron ADX with a CSW redirect rule.	

Defect ID: DEFECT000537175	
Technical Severity: High	**Probability:** Medium
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.4.00	**Technology Area:** Layer 7 Content Switching
Symptom: In Layer7 content-switching configuration, user cannot add a HTTP method rule into a case-insensitive CSW policy.	
Condition: User tries to add a HTTP method rule into a case-insensitive csw-policy.	

Defect ID: DEFECT000537690	
Technical Severity: Medium	**Probability:** Medium
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.01	**Technology Area:** Layer 7 Content Switching
Symptom: ServerIron ADX incorrectly logs error message "max connection rate [actual/limit] 4294967295/4000000 reached"	
Condition: "max-conn" or "max-tcp-conn-rate" configured under Real Server or Real Server Port.	

Defect ID: DEFECT000537707	
Technical Severity: High	**Probability:** Low
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.4.00	**Technology Area:** Stateful SLB
Symptom: Application CPU connection-log messages are being sent to the default Syslog UDP port 514 rather than the configured port.	
Condition: Customer has configured SYSLOG server with custom UDP port other than the default UDP port 514. Application CPU connection-log related messages are being sent out on the default port UDP 514 rather than the non-standard port.	

Defect ID: DEFECT000537708	
Technical Severity: High	**Probability:** Medium
Product: ServerIron	**Technology:** Layer 3
Reported In Release: SI 12.4.00	**Technology Area:** Other IPv4
Symptom: If VIP -Next-Hop feature is configured on the ServerIron ADX and SLB traffic is received from a client, the pass-through traffic from the client may be sent out with an incorrect VLAN ID.	
Condition: VIP next-hop feature is configured; A client pings the VIP consistently; Pass-through traffic from the same client is handled by the ServerIron ADX.	
Recovery: Stop ICMP traffic to the VIP, then clear the MAC and ARP entries on the ServerIron ADX by entering "clear mac" and "clear arp".	

Defect ID: DEFECT000538160	
Technical Severity: Medium	**Probability:** Medium
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.01	**Technology Area:** Layer 7 Content Switching
Symptom: ServerIron ADX fails to do passive Cookie persistence.	
Condition: When the other HTTP header has string "Set-Cookie".	

Defect ID: DEFECT000538181	
Technical Severity: High	**Probability:** Medium
Product: ServerIron	**Technology:** Global Server Load Balancing
Reported In Release: SI 12.4.00	**Technology Area:** GSLB Controller
Symptom: GSLB Controller is unable to gather Active-RTT information and hence GSLB does not use Active-RTT metric and ends up selecting host IP addresses per round-robin.	
Condition: When a user changes prefix-length for round-trip-time then GSLB controller does not delete existing Active-RTT client entries from internal buffer created before the prefix-length change.	
Recovery: Manually delete the internal active RTT cache.	

Defect ID: DEFECT000538457	
Technical Severity: Medium	**Probability:** High
Product: ServerIron	**Technology:** Management
Reported In Release: SI 12.4.00	**Technology Area:** DHCP (IPv4)
Symptom: DHCP persist configuration option is allowed even when DHCP Client is not enabled.	
Condition: DHCP Client is disabled; DHCP persist option is configured.	

Defect ID: DEFECT000539267	
Technical Severity: High	**Probability:** High
Product: ServerIron	**Technology:** Management
Reported In Release: SI 12.4.00	**Technology Area:** DHCP (IPv4)
Symptom: If ServerIron ADX is rebooted without connecting the management port cable, DHCP client is not initialized.	
Condition: Reboot the ADX when the management port cable is unplugged.	
Recovery: Disable and Enable the Management port; This will start the DHCP client.	

Defect ID: DEFECT000539676	
Technical Severity: Medium	**Probability:** Medium
Product: ServerIron	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.4.00	**Technology Area:** SSL Termination
Symptom: An invalid value is accepted for the TCP Window-Scale option by the Application CPU even though the option is rejected by the Management CPU.	
Condition: User sets "tcp-wnd-scale" to 10 in the TCP profile.	

Defect ID: DEFECT000540386	
Technical Severity: High	**Probability:** High
Product: ServerIron	**Technology:** Management
Reported In Release: SI Virtual ADX 4.0.00	**Technology Area:** XML API
Symptom: API deleteTcpMss request to delete multiple TCP MSS values is deleting only the first entry.	
Condition: When multiple TCP MSS values are provided for deletion to deleteTcpMss API.	
Workaround: Delete the TCP MSS values one at a time using deleteTcpMss API.	

Defect ID: DEFECT000541481	
Technical Severity: High	**Probability:** Medium
Product: ServerIron	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** SSL Proxy
Symptom: Application CPU on the ServerIron ADX may reset while handling SSL traffic if SSL Proxy is configured without configuring any cipher-suite in the server-side profile.	
Condition: SSL Proxy ("ssl-proxy") configured on the Virtual Port; SSL profile on the server has no cipher-suite defined.	
Workaround: Add cipher-suites in the server SSL profile.	

Defect ID: DEFECT000541492	
Technical Severity: Medium	**Probability:** High
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.4.00	**Technology Area:** Stateful SLB
Symptom: Using the Web GUI on the ServerIron ADX, when a user tries to remove the description under a Virtual Server, the description is not removed.	
Condition: Using Web GUI to remove description under a Virtual Server.	
Workaround: Use CLI to remove the Virtual Server description.	

Defect ID: DEFECT000541693	
Technical Severity: Medium	**Probability:** High
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.4.00	**Technology Area:** DSR
Symptom: When using Layer3 DSR (Direct Server Return), a Remote Server may be marked incorrectly as Active by the health-checks.	
Condition: ServerIron ADX is configured to use L3 DSR health -checks without element health-checks. Real servers are incorrectly configured such that they use their real IP addresses as Source-IP in health-check replies instead of the VIP IP.	

Defect ID: DEFECT000542216	
Technical Severity: High	**Probability:** High
Product: ServerIron	**Technology:** NAT
Reported In Release: SI 12.4.00	**Technology Area:** Stateful NAT
Symptom: NAT sessions could be stuck if the IP NAT pool configuration on the ServerIron ADX is deleted and a new IP NAT pool is created with the same name.	
Condition: IP NAT pool is deleted and added with the same name.	
Workaround: Create the new IP NAT Pool with different name.	

Defect ID: DEFECT000544082	
Technical Severity: Medium	**Probability:** Medium
Product: ServerIron	**Technology:** Layer 3
Reported In Release: SI 12.4.00	**Technology Area:** Other IPv4
Symptom: Traffic to the ServerIron ADX with destination MAC address that belongs to VRRPe [prefix: 0x02e052] but not owned by the ADX is routed.	
Condition: Traffic received by the ADX with destination MAC as VRRPe MAC owned by a downstream router.	

Defect ID: DEFECT000544706	
Technical Severity: High	**Probability:** Medium
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.01	**Technology Area:** Layer 7 Content Switching
Symptom: In Symmetric High-Availability ServerIron ADX setup configured with CSW, the application CPU on the Active ADX may reset while processing a CSW packet.	
Condition: Symmetric High-Availability setup; CSW configured; HTTP client traffic randomly goes to one of the ServerIron ADXs, and loss of synchronization packets between the ADXs.	

Defect ID: DEFECT000544766	
Technical Severity: Medium	**Probability:** Medium
Product: ServerIron	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.01	**Technology Area:** SSL Ciphers
Symptom: SSL health-checks on the ServerIron ADX are vulnerable to CVE-2014-3570, CVE-2014-8275 and CVE-2015-0204. There is no such vulnerability on data plane SSL.	
Condition: SSL health-checks are enabled on the ADX.	

Defect ID: DEFECT000544939	
Technical Severity: High	**Probability:** Medium
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.01	**Technology Area:** Layer 7 Content Switching
Symptom: In Symmetric High-Availability ServerIron ADX setup configured with CSW, the application CPU may reset while processing a CSW packet.	
Condition: Symmetric High-Availability setup; CSW configured; Client sends a TCP packet with two pipelined HTTP requests, and later, the client retransmits this packet with some new data of the third request.	

Defect ID: DEFECT000546356	
Technical Severity: High	**Probability:** High
Product: ServerIron	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.4.00	**Technology Area:** SSL Proxy
Symptom: With SSL Proxy configured on the ServerIron ADX, large file transfers could fail after certain downloads.	
Condition: SSL Proxy ("ssl- proxy") configured on the Virtual Port; Large files are downloaded multiple times; Transmit buffers and Application CPU heap memory could be depleted over time.	

Defect ID: DEFECT000546591	
Technical Severity: Medium	**Probability:** High
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.4.00	**Technology Area:** Layer 7 Content Switching
Symptom: user may experience slow response with ssl- proxy or ssl-terminate mode	
Condition: client doesn't support TCP window scale option while it is configured	
Workaround: disable window scale option in TCP profile	

Defect ID: DEFECT000546634	
Technical Severity: High	**Probability:** High
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.4.00	**Technology Area:** DSR
Symptom: ServerIron ADX is unable to process fragmented UDP packets received on a Virtual Port if another Virtual Port under same or different Virtual Server has SIP Switching configured.	
Condition: Virtual Port has "sip-switch" or "sip-stateful" configured; Fragmented UDP traffic received by ADX.	

Defect ID: DEFECT000546978	
Technical Severity: High	**Probability:** Medium
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.4.00	**Technology Area:** Session Management
Symptom: The configured timeout for UDP is not effective until the next reload of the ServerIron ADX.	
Condition: "udp-age" configured on the ServerIron ADX.	

Defect ID: DEFECT000547567	
Technical Severity: Medium	**Probability:** Low
Product: ServerIron	**Technology:** Management
Reported In Release: SI 12.4.00	**Technology Area:** System Management
Symptom: In Router Build: If we configure a route for 0.0.0.0/8, Management Interface IP address is lost up on reboot. In Switch Build: 0.0.0.0/8 management route is not allowed when we already have a management default route 0.0.0.0/0	
Condition: Issue is seen when user tries to configure routes for both 0.0.0.0/0 & 0.0.0.0/8 pointing to Management network.	

Defect ID: DEFECT000547703	
Technical Severity: Critical	**Probability:** Medium
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.4.00	**Technology Area:** Health Checks
Symptom: ServerIron ADX configured with port-range with large number of port-range profiles for a given real server causes some of the UDP ports to get stuck in testing.	
Condition: Large number of UDP ports configured using port-range and port profiles.	

Defect ID: DEFECT000548007	
Technical Severity: Medium	**Probability:** Medium
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.4.00	**Technology Area:** Layer 7 Content Switching
Symptom: With SSL Proxy configured on the ServerIron ADX, certain client request may experience high latency.	
Condition: SSL Proxy configured; HTTP/1.1 keep-alive mode, and the first HTTP response is split into multiple TCP segments.	

Defect ID: DEFECT000548333	
Technical Severity: Medium	**Probability:** Medium
Product: ServerIron	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.4.00	**Technology Area:** SSL Health-checks
Symptom: With SSL health-checks enabled on the ServerIron ADX, the ports using SSL health-checks along with a HTTP Layer7 request may remain in Failed state in certain conditions.	
Condition: SSL health-checks enabled on the ServerIron ADX; Web server sends the Response in multiple TLS records with small amounts of data.	
Workaround: One of the following workarounds may be used: 1. Configure server in a way that the HTTP response is sent in larger TLS records 2. Use http match list to validate the response	
Recovery: Configure "l4-check-only" command for the failed port under the real server, and once the port is active, this command may be removed to continue normal health-checks.	

Defect ID: DEFECT000549492	
Technical Severity: Critical	**Probability:** High
Product: ServerIron	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.4.00	**Technology Area:** SSL Ciphers
Symptom: ServerIron ADX negotiates export RSA cipher-suites during full SSL health-checks. But, this does not lead to any leak of data as ADX does not exchange any data during full SSL health-checks.	
Condition: Full SSL health-checks enabled on the ADX; OpenSSL vulnerability with export cipher-suites.	

Defect ID: DEFECT0005410020	
Technical Severity: Critical	**Probability:** Medium
Product: ServerIron	**Technology:** Multitenancy
Reported In Release: SI 12.5.01	**Technology Area:** Tenant Provisioning
Symptom: The Application CPU will reset when assigning the only tenant to the second CPU and enable full stack.	
Condition: 1. Skip the first application CPU, assign the tenant to the second application CPU. 2. enable full stack by configuring "port http tcp-proxy"	
Workaround: Assign the tenant to the first CPU	

Defect ID: DEFECT000550680	
Technical Severity: Medium	**Probability:** Medium
Product: ServerIron	**Technology:** Layer 2
Reported In Release: SI 12.5.02	**Technology Area:** LACP
Symptom: In a Multi-Tenancy setup, the LACP ports of a tenant on the ServerIron ADX may be stuck in LAG-BLOCK state.	
Condition: ServerIron ADX configured in Multi-Tenancy mode; A tenant is created and its ports are configured in a LAG.	

Defect ID: DEFECT000551111	
Technical Severity: Medium	**Probability:** Low
Product: ServerIron	**Technology:** High Availability
Reported In Release: SI 12.4.00	**Technology Area:** Symmetric SLB
Symptom: In case of a link failure in a High-Availability ServerIron ADX setup, an ADX which has a Standby VIP might take ownership of the VIP before health -check to the Real server is successful.	
Condition: ADX in HA Sym-Active configuration in one- arm topology.	

Defect ID: DEFECT000551230	
Technical Severity: High	**Probability:** Medium
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.4.00	**Technology Area:** Stateful SLB
Symptom: If SSL or Layer7 is configured on the ServerIron ADX, Real Servers bound to those Virtual Ports may go into Failed state with "reassign" reason even though the reassign threshold feature is not configured.	
Condition: SSL or CSW content-rewrite rules configured on the Virtual Port; Heavy load on the Real Servers causing Servers to fail to respond to client connection requests; Real Port may go into Failed state with reason "reassign".	

Defect ID: DEFECT000551376	
Technical Severity: Medium	**Probability:** Medium
Product: ServerIron	**Technology:** Management
Reported In Release: SI 12.4.00	**Technology Area:** System Management
Symptom: When commands that output multiple pages, were run through runCLI API, the ServerIron ADX lost all the 17 display buffers over time and following error was thrown "INFO: all 17 display buffers are busy, please try later."	
Condition: Command run through runCLI API, or WEB GUI's CLI access tab and the output spans multiple pages.	
Recovery: Reset the display buffer manually using 'dm display-buffer reset' command.	

Defect ID: DEFECT000551670	
Technical Severity: Medium	**Probability:** Medium
Product: ServerIron	**Technology:** Management
Reported In Release: SI 12.5.01	**Technology Area:** Configuration Synchronization
Symptom: With a large configuration, Management CPU may reset when running the command "config-sync diff".	
Condition: Command "config-sync diff" when the configuration file is large (> 3000 lines).	

Defect ID: DEFECT000551930	
Technical Severity: Medium	**Probability:** High
Product: ServerIron	**Technology:** Management
Reported In Release: SI 12.4.00	**Technology Area:** XML API
Symptom: When commands that output multiple pages, were run through runCLI API or Web GUI, the outputs were truncated.	
Condition: Command run through runCLI API or Web GUI's CLI access and the output spans multiple pages.	

Defect ID: DEFECT000552140	
Technical Severity: High	**Probability:** High
Product: ServerIron	**Technology:** Management
Reported In Release: SI 12.5.01	**Technology Area:** DHCP (IPv4)
Symptom: Ping doesn't work if DHCP client on management interface is disabled.	
Condition: Disabling DHCP client on management interface results in this issue.	

Defect ID: DEFECT000552824	
Technical Severity: High	**Probability:** Medium
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** OpenScript
Symptom: ServerIron ADX when configured with Openscript for Response Rewrite and SSL with Layer7 CSW then it may add duplicate HTTP response header to the server's HTTP Response.	
Condition: When both SSL and Layer7 CSW are configured on the ServerIron ADX, and Openscript has HTTP response rewrite.	

Defect ID: DEFECT000552924	
Technical Severity: Medium	**Probability:** Medium
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** Session Management
Symptom: In a Hot-Standby High-Availability setup with Layer7 CSW configured, the Standby ADX may notice high current connection counter.	
Condition: Hot-Standby High-Availability setup of ServerIron ADX; Layer7 SLB enabled with a CSW policy; client sends multiple HTTP requests over the same connection that are forwarded to different real servers; The output of "show server virtual vs_name" may show the curconn counter increasing incorrectly on the Standby ADX while that counter works fine on the Active ADX.	

Defect ID: DEFECT000553332	
Technical Severity: High	**Probability:** Medium
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.4.00	**Technology Area:** Stateful SLB
Symptom: If Source-NAT and BP selection mask is configured on the ServerIron ADX, SLB traffic may fail.	
Condition: Source-NAT configured on the ServerIron ADX; "server select-bp-mask" is configured to include more than 1 BP.	
Recovery: Remove and add Source-IP/Source-NAT-IP/Interface-IP to redistribute Source-NAT traffic properly.	

Defect ID: DEFECT000553425	
Technical Severity: Medium	**Probability:** Medium
Product: ServerIron	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** Web Management
Symptom: After upgrade to 12501d+ or 12502+ patch, users get the GUI error “If you have just upgraded your system with a new software image, please clear you cache to get the latest version of the GUI”. This happens even if clearing all browser history and logging in again from IE, Chrome, or Mozilla. The issue happens on HTTP or HTTPS.	
Condition: Cache clearing warning message occurs after successful login to ADX GUI every time even though the cache is cleared. Build info is blank on the login page and thus causing to display warning after every successful login to GUI.	

Defect ID: DEFECT000553469	
Technical Severity: High	**Probability:** High
Product: ServerIron	**Technology:** Management
Reported In Release: SI 12.4.00	**Technology Area:** System Management
Symptom: After reload, the ServerIron ADX ignores source interface command if management interface is configured with DHCP.	
Condition: Configure source interface command for any protocol such as DNS and SNTP, save the configuration and reload the ServerIron ADX.	

Defect ID: DEFECT000553558	
Technical Severity: High	**Probability:** Medium
Product: ServerIron	**Technology:** Management
Reported In Release: SI 12.5.01	**Technology Area:** System Management
Symptom: ServerIron ADX does not save the old eventlog file when there is already another file named elog_old.txt	
Condition: There is a file named elog_old.txt on usb0; Current event log file (eventlog.txt) on the ServerIron ADX reaches max size of 256MB; ADX tries to create a file name elog_old.txt to save the current eventlog file but fails to delete and create.	
Workaround: Save the elog_old.txt file from usb0 with different name as soon as it gets created and delete elog_old.txt file	

Defect ID: DEFECT000554293	
Technical Severity: High	**Probability:** Medium
Product: ServerIron	**Technology:** Management
Reported In Release: SI 12.5.01	**Technology Area:** Web Management
Symptom: When ServerIron ADX is configured with more than 31 VLANs, user login through GUI or XML API command getSystemDashboard may trigger a Management CPU reset.	
Condition: More than 31 VLANs configured on the ServerIron ADX; User login through GUI or getSystemDashboard XML API call may trigger a stack overflow and a subsequent Management CPU reset.	

Defect ID: DEFECT000554792	
Technical Severity: Medium	**Probability:** Medium
Product: ServerIron	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** Configuration Synchronization
Symptom: In High-Availability ServerIron ADX setup with config-sync enabled, Virtual Server name update on sender does not sync with receiver.	
Condition: High-Availability ServerIron ADX setup; Config-sync enabled; Virtual server name is updated on the Sender ADX.	

Defect ID: DEFECT000555213	
Technical Severity: Medium	**Probability:** High
Product: ServerIron	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** SSL Termination
Symptom: When user tries to upload an SSL certificate to the ServerIron ADX, the upload fails if the certificate name is longer than 25 characters.	
Condition: Upload of an SSL certificate with name longer than 25 characters.	

Defect ID: DEFECT000556329	
Technical Severity: Medium	**Probability:** Medium
Product: ServerIron	**Technology:** System
Reported In Release: SI 12.5.02	**Technology Area:** CLI
Symptom: When user tries to save the running configuration and reloads the ServerIron ADX, Management CPU may reset in certain scenarios.	
Condition: Historical statistics data collection is turned on through GUI; User tries to run "write mem" and then "reload" to save the running configuration and reload the ServerIron ADX.	

Defect ID: DEFECT000556625	
Technical Severity: Low	**Probability:** Medium
Product: ServerIron	**Technology:** Monitoring/RAS
Reported In Release: SI 12.5.02	**Technology Area:** Syslog
Symptom: ADX syslog format uses comma after hostname, RFC 5424 says to use space as delimiter.	
Condition: "rsyslog" used to parse ServerIron ADX syslog messages.	

Defects closed with code in ServerIron ADX 12.5.02b

Defect ID: DEFECT000537744	
Technical Severity: High	**Probability:** Medium
Product: ServerIron	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** SSL Termination
Symptom: If SSL is configured on the ServerIron ADX, incoming TLS 1.1 or 1.2 connections may cause the Application CPU to reset if the decrypted Finished message is greater than 80 bytes	
Condition: SSL configured on the ServerIron ADX in Terminate or Proxy mode; SSL connections from clients using TLS 1.1/1.2 versions, and the decrypted Finish message greater than 80 bytes.	

Defect ID: DEFECT000539432	
Technical Severity: High	**Probability:** Medium
Product: ServerIron	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.01	**Technology Area:** SSL Termination
Symptom: SSL connections through the ServerIron ADX may be vulnerable to the TLS POODLE issue CVE-2014-8730.	
Condition: SSL configured on the ServerIron ADX.	

Defect ID: DEFECT0005310071	
Technical Severity: Medium	**Probability:** High
Product: ServerIron	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** SSL Termination
Symptom: The SSL option to send an Alert to close the connection is not working. SSL Client does not receive any Close-Notify Alert message when session is closed.	
Condition: SSL configured on the ServerIron ADX in either Terminate or Proxy mode, and "enable-close-notify" configured in the SSL profile.	

Defect ID: DEFECT0005310095	
Technical Severity: High	**Probability:** Medium
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.01	**Technology Area:** Health Checks
Symptom: If GSLB is configured, Management CPU on the ServerIron ADX may reset when user configures GSLB host with ip-list unreachable with Remote server Layer3 health-checks disabled.	
Condition: The issue is seen at the time of sending GSLB health-check with Remote Server L3 health-checks disabled. If no route is found for the IP in the GSLB Host IP-List configuration, Management CPU may reset. A minimum of 2 IPs have to be configured in host ip-list for this issue to be seen.	
Workaround: Configure routes for IPs in ip-list before configuring host ip-list.	

Defect ID: DEFECT000540120	
Technical Severity: Medium	**Probability:** Medium
Product: ServerIron	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** SSL Termination
Symptom: SSL connections using TLS 1.2 version may fail if Client-Authentication is enabled in the SSL profile.	
Condition: SSL configured on the ServerIron ADX; Client-Authentication configured in the SSL profile; Incoming TLS 1.2 connections from SSL clients.	

Defect ID: DEFECT000540745	
Technical Severity: High	**Probability:** High
Product: ServerIron	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** SSL Termination
Symptom: If SSL termination is configured on the ServerIron ADX, certain SSL connections may leak memory.	
Condition: SSL configured on the ServerIron ADX in Terminate or Proxy mode; TLS 1.1/1.2 connections coming in from SSL clients while uploading files or downloading large files.	

Defect ID: DEFECT000540825	
Technical Severity: High	**Probability:** Medium
Product: ServerIron	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** SSL Ciphers
Symptom: Web Management connections to the ServerIron ADX may be vulnerable to the POODLE issue CVE-20148730	
Condition: Customer uses the Web GUI to manage the ServerIron ADX.	

Defects closed with code in ServerIron ADX 12.5.02a

Defect ID: DEFECT000536681	
Technical Severity: Critical	**Probability:** Low
Product: ServerIron	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** SSL Proxy
Symptom: With SSL Proxy configured and SSL traffic running over a day, some TCP sockets may be stuck and the memory reserved by those sockets not released causing a memory leak.	
Condition: SSL Proxy configured on the ServerIron ADX.	

Defects closed with code in ServerIron ADX 12.5.02

Defect ID: DEFECT000377908	
Technical Severity: High	**Probability:** Medium
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.4.00	**Technology Area:** Health Checks
Symptom: ServerIron ADX, configured with hc-l3-dsr and TOS value, does not send UDP health check packets with TOS bit set, resulting in health check failure.	
Condition: ServerIron ADX, configured with hc-l3-dsr and TOS value, does not send UDP health check packets with TOS bit set, resulting in health check failure.	
Workaround: Disable health checks on the UDP port.	

Defect ID: DEFECT000411759	
Technical Severity: Medium	**Probability:** Medium
Product: ServerIron	
Reported In Release: SI 12.5.00	

Defect ID: DEFECT000462391	
Technical Severity: Medium	**Probability:** High
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.00	**Technology Area:** Stateful SLB
Symptom: Field of "Effective max conn" shows "2147483647" in the output of "show server real detail"	
Condition: The max-conn is not configured under real server port, when user types "show server real detail"	

Defect ID: DEFECT000467243	
Technical Severity: Critical	**Probability:** Low
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.4.00	**Technology Area:** Source-NAT
Symptom: All traffic fails while "server source- NAT" is configured.	
Condition: All traffic fails while "server source- NAT" is configured.	

Defect ID: DEFECT000483712	
Technical Severity: Medium	**Probability:** Medium
Product: ServerIron	**Technology:** Management
Reported In Release: SI Virtual ADX 3.0.00	**Technology Area:** Telnet
Symptom: When the telnet server is disabled on the ADX, any client connecting to the telnet port will receive a TCP reset by default.	
Condition: telnet server disabled on the ADX; "no telnet server suppress-reject-message" not configured; client connects to the telnet port on the ADX;	

Defect ID: DEFECT000485535	
Technical Severity: Medium	**Probability:** Medium
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI Virtual ADX 3.0.00	**Technology Area:** Health Checks
Symptom: Layer7 health-check may not work in DSR mode when DNS is configured on an unknown port.	
Condition: DSR mode; DNS health-check policy configured on an unknown port;	

Defect ID: DEFECT000504795	
Technical Severity: High	**Probability:** Medium
Product: ServerIron	**Technology:** Layer 2
Reported In Release: SI 12.4.00	**Technology Area:** ARP
Symptom: Application CPU may reset while refreshing ARP entries during a continuous flapping of an interface	
Condition: ARP entries greater than or equal to 8192; interface flapping	

Defect ID: DEFECT0005134100	
Technical Severity: High	**Probability:** Low
Product: ServerIron	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.0.00	**Technology Area:** SSL Ciphers
Symptom: OpenSSL advisory recommendation SSL/TLS MITM vulnerability (CVE-2014-0224)	
Condition: SSL-Terminate or SSL-Proxy configured on ADX; Potential Man-In-The-Middle attack launched by a malicious 3rd party;	

Defect ID: DEFECT000516670	
Technical Severity: Critical	**Probability:** Medium
Product: ServerIron	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.4.00	**Technology Area:** SSL Proxy
Symptom: ssl-proxy: tcp fragmented server response packets, with stress run for 20-30 mins, all traffic failed, there are rx buffer and ssl memory loss	
Condition: This HW ADX only issue due to that Cavium cannot retrieve incoming packets correctly	

Defect ID: DEFECT000516805	
Technical Severity: High	**Probability:** High
Product: ServerIron	**Technology:** Management
Reported In Release: SI 12.4.00	**Technology Area:** XML API
Symptom: Content Check configuration under Real Server Port unavailable via API or GUI	
Condition: Accessing the RealServerPort API via any client program	
Workaround: Using CLI command instead of XML API or using the runCLI option via API	

Defect ID: DEFECT000518646	
Technical Severity: Medium	**Probability:** Medium
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.4.00	**Technology Area:** Complex protocols
Symptom: Layer4 port translation does not work on ADX for fragmented IPv6 UDP traffic.	
Condition: SLB configured; Layer4 Port translation is configured; Fragmented IPv6 UDP traffic is received by ADX;	

Defect ID: DEFECT000519053	
Technical Severity: High	**Probability:** Medium
Product: ServerIron	**Technology:** Layer 2
Reported In Release: SI 12.4.00	**Technology Area:** VLAN
Symptom: ServerIron ADX adds the port as untagged into all VLANs with certain command sequences.	
Condition: ADX configured with port in dual-mode. The command "dual-mode" is removed from the said port and then port is added to any new VLAN as tagged without dual-mode.	
Workaround: Disable FDP.	

Defect ID: DEFECT000523189	
Technical Severity: High	**Probability:** Medium
Product: ServerIron	**Technology:** Global Server Load Balancing
Reported In Release: SI 12.5.01	**Technology Area:** GSLB Site
Symptom: When a VIP at a GSLB site falls below the configured minimum- servers threshold value, the distributed health check for the VIP may still be sent as UP to the GSLB controller.	
Condition: GSLB configured; "minimum-server" configured on the GSLB site VIP; Real-Servers fail health-checks to cause VIP to fall below "minimum-server" threshold;	

Defect ID: DEFECT000524573	
Technical Severity: High	**Probability:** Medium
Product: ServerIron	**Technology:** Global Server Load Balancing
Reported In Release: SI 12.5.01	**Technology Area:** GSLB Controller
Symptom: The ServerIron ADX that receives GSLB configuration sent from the master ServerIron ADX does not respond to DNS queries for the newly added host-info.	
Condition: User has a DNS cache-proxy-override configuration; User added some “host-info” entries after upgrading the GSLB controllers from 12400p to 12501d.	

Defect ID: DEFECT000525800	
Technical Severity: Critical	**Probability:** High
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.4.00	**Technology Area:** Stateful SLB
Symptom: For IPv6 traffic, there will be a degraded performance (higher CPU % on BP or lower CPS numbers than expected).	
Condition: If ADX is running in Translation IPv6 mode there will be a performance degradation seen on the BP when processing IPv6 traffic. The impact will be seen on stateless, statefull SLB and pass-through cases for L4/L7 configs.	
Workaround: There is no workaround for this defect. Since this issue is not seen in Native IPv6 mode moving to Native IPv6 mode if possible can reduce the BP CPU %.	
Recovery: No recovery. Upgrading to current patch release will fix the issue.	

Defect ID: DEFECT000525832	
Technical Severity: Medium	**Probability:** Medium
Product: ServerIron	**Technology:** Management
Reported In Release: SI 12.4.00	**Technology Area:** Web Management
Symptom: After 100 WEB GUI connections to ServerIron ADX are established and terminated, additional WEB GUI connections cannot be established.	
Condition: User logs in to the ADX over GUI 100 times and logs out each time.	
Workaround: User need not log out of the GUI session but rather let the session expire with a low timeout.	

Defect ID: DEFECT000526507	
Technical Severity: Critical	**Probability:** Medium
Product: ServerIron	**Technology:** Global Server Load Balancing
Reported In Release: SI 12.4.00	**Technology Area:** GSLB Site
Symptom: ADX configured with GSLB may reset when user tries to remove host-info with health check parameters which are either removed earlier or never configured.	
Condition: GSLB configured; host-info configured and removed.	

Defect ID: DEFECT000528776	
Technical Severity: Medium	**Probability:** Medium
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.01	**Technology Area:** OpenScript
Symptom: OS_HTTP_RESPONSE::code() API can only replace status code, so when the input parameter string has both status code and its description, the old status code's description is not removed.	
Condition: OS_HTTP_RESPONSE::code() API input parameter has both the status code and its description	

Defect ID: DEFECT000529070	
Technical Severity: High	**Probability:** Medium
Product: ServerIron	**Technology:** Layer 2
Reported In Release: SI 12.4.00	**Technology Area:** ARP
Symptom: ServerIron ADX running switch code continues to send out ARP requests even after receiving gratuitous ARPs from the upstream VRRP-e Master. ADX moves the MAC address from one port to another and goes into loop. This causes HIGH CPU condition on ADX Management CPU.	
Condition: ServerIron ADX running switch code is reloaded or "clear arp" is performed; ADX sends out ARP requests for the very first time; Upstream routers (MLX) are configured with feature Short Path Forwarding wherein both VRRP-Routers will respond to ARP requests (This behavior is a design issue and being changed in next major releases); ADX moves the MAC address from one port to another and goes into loop; This causes HIGH CPU condition on ADX Management CPU.	

Defect ID: DEFECT000529117	
Technical Severity: High	**Probability:** High
Product: ServerIron	**Technology:** Other
Reported In Release: SI 12.4.00	**Technology Area:** Other
Symptom: The command “unknown-unicast-hw-enable" does not persist across reload.	
Condition: Configure “unknown-unicast-hw-enable" ; save configuration and reload	
Workaround: Remove and reconfigure “unknown-unicast-hw-enable" following a reload	

Defect ID: DEFECT000529228	
Technical Severity: Medium	**Probability:** High
Product: ServerIron	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** SSL Ciphers
Symptom: SSLv2 client authentication fails when "per-connection request" is configured and no certificate is sent	
Condition: Client- Authentication "per-connection request" is configured on the SSL profile, and client sends SSLv2 traffic without a certificate	

Defect ID: DEFECT000529312	
Technical Severity: Medium	**Probability:** High
Product: ServerIron	**Technology:** Other
Reported In Release: SI 12.5.01	**Technology Area:** Other
Symptom: ADX only displays 16 Real server groups bound to a VIP	
Condition: ADX only displays 16 real-server groups bound to a VIP.	

Defect ID: DEFECT0005210054	
Technical Severity: High	**Probability:** High
Product: ServerIron	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.4.00	**Technology Area:** SSL Termination
Symptom: ServerIron ADX continues to send a RST when the vport is down even after adding the command "server l7-dont-reset-on-vip-port-fail "	
Condition: ServerIron ADX continues to send a RST when the vport is down even after adding the command "server l7-dont-reset-on-vip-port-fail "	

Defect ID: DEFECT000530064	
Technical Severity: High	**Probability:** Low
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.01	**Technology Area:** Layer 7 Content Switching
Symptom: System will crash during inserting cookie string into the HTTP response.	
Condition: When the cookie configuration cannot be retrieved from CSW rule actions.	

Defect ID: DEFECT000530534	
Technical Severity: High	**Probability:** High
Product: ServerIron	**Technology:** Global Server Load Balancing
Reported In Release: SI 12.5.01	**Technology Area:** IPv6 GSLB
Symptom: In Cache-proxy override mode, when adding IP-list with ipv4 and ipv6 together in a single CLI, ipv6 IPs were not synced to the local BP	
Condition: In Cache-proxy override mode, when adding IP-list with ipv4 and ipv6 together in a single CLI, ipv6 IPs were not synced to the local BP	

Defect ID: DEFECT000530734	
Technical Severity: High	**Probability:** Medium
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.4.00	**Technology Area:** Stateless SLB
Symptom: SLB traffic may fail in one arm topology since ADX does not change source mac for load balanced traffic	
Condition: SLB stateless is configured in one arm topology	
Workaround: Enable SLB fast stateless feature by configuring "server fast-stateless" globally	

Defect ID: DEFECT000531462	
Technical Severity: High	**Probability:** Medium
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.4.00	**Technology Area:** Layer 7 Content Switching
Symptom: ADX configured with response-rewrite may experience application CPU reset while processing server response	
Condition: CSW response-rewrite configured; Server response received	

Defect ID: DEFECT000531690	
Technical Severity: Medium	**Probability:** High
Product: ServerIron	**Technology:** Management
Reported In Release: SI 12.5.02	**Technology Area:** XML API
Symptom: User cannot unbind the SSL profile which was applied to a Virtual Server Port as SSL Proxy.	
Condition: Recent validations added in 12.5.02 codebase for below defect fix in the SSL profile unbinding CLI exposed this issue.	

Defect ID: DEFECT000532068	
Technical Severity: Critical	**Probability:** High
Product: ServerIron	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.4.00	**Technology Area:** SSL Ciphers
Symptom: ServerIron ADX configured with SSL-termination OR SSL-PROXY is vulnerable to Poodle (Padded Oracle On Downgraded Legacy Encryption) Attack, SSL vulnerability CVE-2014-3566.	
Condition: ServerIron ADX configured with SSL-Terminate or SSL-PROXY.	

Defect ID: DEFECT000532069	
Technical Severity: Critical	**Probability:** High
Product: ServerIron	**Technology:** Management
Reported In Release: SI 12.4.00	**Technology Area:** Web Management
Symptom: Web management access over HTTPS is vulnerable to Poodle (Padded Oracle On Downgraded Legacy Encryption) attack (CVE-2014-3566).	
Condition: Customer using web management over HTTPS. HTTPS web-management when using SSLv3 is vulnerable.	
Workaround: Disable Web-management. Use CLI to access ServerIron ADX.	

Defect ID: DEFECT000532070	
Technical Severity: Critical	**Probability:** High
Product: ServerIron	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.4.00	**Technology Area:** SSL Health-checks
Symptom: ServerIron ADX configured with SSL health check may be vulnerable to POODLE (Padded Oracle On Downgraded Legacy Encryption) attack, CVE-2014-3566.	
Condition: ServerIron ADX is configured with SSL health check.	
Workaround: Enable "l4-check-only" under server port profile or under real/remote server configuration. OR If SSL health check is a must then please enable complete SSL health check with the command, "no server use-simple-ssl-health-check" AND also disable SSLv3 on the server itself.	

Defects closed without code in ServerIron ADX 12.5.02

Defect ID: DEFECT000456692	
Technical Severity: Medium	**Probability:** Medium
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.01	**Technology Area:** Configuration Synchronization
Symptom: CLI involving hardware CAM programming take longer to finish, during which CLI will not allow any more commands pending completion of the CAM programming. If user tried to enter another command, they will be prompted with message "ADX is currently programming/accessing CAM entries. Please wait for completion and retry the current command" on the console. If ADX is being configured through CLI using copy-and-paste, this does not leave enough time to finish the CLI commands and user will be prompted with above message. This restriction applies to CAM programming for ACLs and SLB configuration of VIPs and Servers.	
Condition: In a scenario involving large CAM tables, any CLI command involving additional CAM programming will take longer time to complete. Instead of freezing the CLI until command completion, CLI will instead give a prompt message when user tries to issue another command. In this scenario, it is not allowed to copy-paste CLI commands involving CAM programming, until prior CLI command has finished programming the CAM.	
Workaround: Large CAM tables need more time to program more entries. Copy-Paste of CLI configuration should be avoided. It is recommended to wait till the issued CLI command finished programming the CAM entries before issuing a new command.	

Open Defects in ServerIron ADX 12.5.02

Defect ID: DEFECT000448629	
Technical Severity: Medium	**Probability:** High
Product: ServerIron	**Technology:** Layer 3
Reported In Release: SI 12.5.01	**Technology Area:** OSPF (IPv4)
Symptom: In the output of 'show ip ospf interface', Backup Designated Router is abbreviated as BD instead of BDR. Also, enabling 'debug ip ospf packet' doesn't show any packets when OSPF neighbors are cleared. These are display issues and do not affect functionality.	
Condition: "show ip ospf interface" and "debug ip ospf packet" commands	

Defect ID: DEFECT000461220	
Technical Severity: Medium	**Probability:** High
Product: ServerIron	**Technology:** Layer 3
Reported In Release: SI 12.5.01	**Technology Area:** OSPF (IPv4)
Symptom: ISIS routes will not be redistributed to neighbors by OSPF router after clearing OSPF neighbor-ship.	
Condition: This issue occurs in a network where both OSPF and ISIS are used for learning routes.	

Defect ID: DEFECT000461478	
Technical Severity: Medium	**Probability:** High
Product: ServerIron	**Technology:** Layer 3
Reported In Release: SI 12.5.01	**Technology Area:** OSPF (IPv4)
Symptom: "Log first overflow and enable DABR" messages may be displayed while removing OSPF from configuration.	
Condition: Remove OSPF from configuration	

Defect ID: DEFECT000467640	
Technical Severity: Medium	**Probability:** High
Product: ServerIron	**Technology:** Layer 3
Reported In Release: SI 12.5.01	**Technology Area:** OSPF (IPv4)
Symptom: No error message is prompted to user, when there is inconsistency in OSPF Area-id format.	
Condition: When user configures Area Id in OSPF configuration & Interface configuration in different format.	

Defect ID: DEFECT000471112	
Technical Severity: High	**Probability:** High
Product: ServerIron	**Technology:** Layer 3
Reported In Release: SI 12.5.01	**Technology Area:** OSPFv3 (IPv6)
Symptom: IPv6 default route is not advertised to neighbors by OSPF router in Multi-Tenancy mode	
Condition: Configuring 'default-information-originate' for OSPFv3 in Multi-Tenancy mode	

Defect ID: DEFECT000473484	
Technical Severity: Medium	**Probability:** High
Product: ServerIron	**Technology:** Layer 3
Reported In Release: SI 12.5.01	**Technology Area:** OSPFv3 (IPv6)
Symptom: OSPFv3 neighbor -ship state gets stuck in INIT state in a particular scenario	
Condition: Forming OSPFv3 neighbor-ship with IPSec enabled & removing IPSec configuration from one of the Neighbors	

Defect ID: DEFECT000492790	
Technical Severity: Medium	**Probability:** High
Product: ServerIron	**Technology:** Layer 3
Reported In Release: SI 12.5.01	**Technology Area:** BGP4+ (IPv6)
Symptom: In the output of 'show ipv6 route', Internal BGP route is abbreviated as B instead of Bi	
Condition: This is display issue. This doesn't break any BGP functionality	

Defect ID: DEFECT000493458	
Technical Severity: Medium	**Probability:** High
Product: ServerIron	**Technology:** Layer 3
Reported In Release: SI 12.4.00	**Technology Area:** OSPFv3 (IPv6)
Symptom: When IPv6 load sharing is configured, OSPF routes will not be as per the configured load sharing value.	
Condition: Configuring IPv6 Load sharing in OSPFv3 network	

Defect ID: DEFECT000494021	
Technical Severity: Medium	**Probability:** Medium
Product: ServerIron	**Technology:** Layer 3
Reported In Release: SI Virtual ADX 3.0.00	**Technology Area:** BGP4 (IPv4)
Symptom: IPv4 static route is not getting redistributed when "redistribute static" is enabled with "router bgp" on.	
Condition: same as above.	

Defect ID: DEFECT000524623	
Technical Severity: Medium	**Probability:** High
Product: ServerIron	**Technology:** Secure Socket Layer (SSL)
Reported In Release: SI 12.5.02	**Technology Area:** SSL Termination
Symptom: In SSL-proxy configuration, Cavium Type-2 instruction errors in "show ssl statistics counters" will increment with completion code 0002.	
Condition: Though the BP reports SSL cavium type-2 instruction errors with completion code 0002 in an SSL-Proxy configuration, traffic will not fail. Connections will continue to work as expected.	
Workaround: For now ignore the Cavium Type-2 instruction errors in "show ssl statistics counters" with completion code 0002, in an SSL-proxy configuration.	

Defect ID: DEFECT000527295	
Technical Severity: High	**Probability:** High
Product: ServerIron	**Technology:** Global Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** GSLB Controller
Symptom: CPU utilization is high with max gslb dns zone/host configuration.	
Condition: CPU utilization is high with over 1000 gslb dns zone/host configuration.	

Defect ID: DEFECT000527802	
Technical Severity: High	**Probability:** High
Product: ServerIron	**Technology:** High Availability
Reported In Release: SI 12.5.02	**Technology Area:** Active-Active SLB
Symptom: " vrrp-e standby" command does not work properly when both devices are configured with long dead Interval. Both devices will stay in backup state for around 30 seconds.	
Condition: " vrrp-e standby" command does not work properly when both devices are configured with long dead Interval. Both devices will stay in backup state for around 30 seconds.	
Workaround: Reduce the dead interval value or use default value.	

Defect ID: DEFECT000530760	
Technical Severity: High	**Probability:** Medium
Product: ServerIron	**Technology:** Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** Source-NAT
Symptom: When a vip-group of source-nat-IPs are configured for a VRRP -E and the VRRP-E is failed over, the source-nat-ips in the vip-group on the new active box may take a few seconds to send gratuitous ARPs. This may cause traffic using source-nat-ip to fail for a few seconds.	
Condition: Issue may be seen after a vrrp-e failover which has source-nat-ip configured in the bound vip-group.	
Workaround: Configure "server sym-pdu-rate" CLI to reduce the heartbeat interval.	

Defect ID: DEFECT000531057	
Technical Severity: High	**Probability:** High
Product: ServerIron	**Technology:** Layer 3
Reported In Release: SI 12.5.01	**Technology Area:** Other IPv4
Symptom: High CPU is observed on the MP.	
Condition: The issue may be seen when customer has high number of virtual servers configured along with multiple IP addresses under interfaces.	
Workaround: The CPU utilization can be reduced by disabling L2 and L3 periodic health-checks and increasing the interval of L4 health-checks.	

Defect ID: DEFECT000532021	
Technical Severity: Critical	**Probability:** High
Product: ServerIron	**Technology:** Global Server Load Balancing
Reported In Release: SI 12.5.02	**Technology Area:** GSLB Controller
Symptom: MP crash observed during gslb config-sync tests.	
Condition: When GSLB is configured with big number of DNS site IP-lists and they are synced, we may see the above issue.	