April 2022

Extreme SLX-OS 20.4.1

Release Notes

Supporting ExtremeRouting and ExtremeSwitching SLX 9740, SLX 9640, SLX 9540, SLX 9250, SLX 9150, Extreme 8720, and Extreme 8520

Part Number 9037423-00 Rev AA

Contents

Document History

Version	Summary of changes	Publication date
1.0	Initial version for 20.4.1	April 2022

Preface

Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

- Extreme Portal: Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training and certifications.
- The Hub: A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees but is not intended to replace specific guidance from GTAC.
- Call GTAC: For immediate support, call (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2826. For the support phone number in your country, visit www.extremenetworks.com/support/contact.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribe to Service Notifications

You can subscribe to email notifications for product and software release announcements, Vulnerability Notices, and Service Notifications.

1. Go to www.extremenetworks.com/support/service-notification-form.
2. Complete the form. All fields are required.
3. Select the products for which you want to receive notifications.
   Note: You can change your product selections or unsubscribe at any time.
4. Select **Submit**.

Extreme Resources

Visit the Extreme website to locate related documentation for your product and additional Extreme resources.

White papers, data sheets, and the most recent versions of Extreme software and hardware manuals are available at www.extremenetworks.com. Product documentation for all supported releases is available to registered users at https://www.extremenetworks.com/support/documentation/.

Document Feedback

The Information Development team at Extreme Networks has made every effort to ensure the accuracy and completeness of this document. We are always striving to improve our documentation and help you work better, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information
- Improvements that would help you find relevant information in the document
- Broken links or usability issues

You can provide feedback in the following ways:

- In a web browser, select the feedback icon and complete the online feedback form.
- Access the feedback form at http://www.extremenetworks.com/documentation-feedback-pdf/.
- Email us at documentation@extremenetworks.com.

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

Release Overview

Release SLX-OS 20.4.1 provides the following features:

- SLX based TPVM upgrade optimization
- Additional SNMP notification event support
- SE Linux based IMA policy
- MAC (Mandatory Access Control) policy for user space binaries
- Ability to upgrade ONIE/GRUB
- Force port 1G speed/duplex via constrained advertised capabilities
- Processing ACL rule for Tunneled traffic
- BGP Dynamic Peering Scale Enhancement
- IPV6 configuration support in TPVM
- IPv6 Support for Peer-Address in a Route Map for BGP
- BGP dampening for peer flaps
- TPVM security patches till April 03rd, 2022 are included in TPVM 4.5.0

Behavior Changes

The following are the behavioral changes for SLX-OS 20.4.1

- CLI `threshold-monitor` is modified as follows:
  - Default action is changed from RASlog to RASlog and SNMP Trap.
  - `threshold-monitor Memory` has removed parameters – limit and low-limit.
  - Default values for `threshold-monitor Cpu` and `threshold-monitor Memory` are changed.
- SNMP trap for BFD module contains additional info and is implemented via Enterprise BFD MIB. BFD Enterprise MIB is the default option. This means, snmp-server trap needs to be specifically configured for BFD standard MIB via newly added CLI in this release.
- TPVM patch upgrade (incremental upgrade) that helps upgrading only the patches without stopping the running TPVM instance. Use the command `tpvm upgrade incremental`.
- TPVM IPv6 support
- Added security patches till April 03rd, 2022 in TPVM 4.5.0

Software Features

The following key software features are added in the SLX-OS 20.4.1 release

Feature Name	Supported SLX Platforms	Description

SLX based TPVM upgrade optimization	All	`tpvm upgrade incremental` command is introduced.
		• avoids reinstallation of TPVM and EFA during upgrade
		• 2 Debian files for each installation type
		  ○ One for full installation
		  ○ One for upgrade installation

Feature Name	Supported SLX Platforms	Description
Additional SNMP Notification Event support	All	New and enhanced SNMP notifications are added: • BFD enterprise notifications with BFD session specific information • Cluster up and down notifications for MCT cluster • Maintenance mode traps for entry and exit transitions • CPU and memory threshold monitoring traps. • NTP status change trap • Enhanced BGP IPv6 notifications - Established & BackwardTransition traps • Enhanced Fan failure / recovery traps • Enhanced Power Supply failure / recovery traps
SE Linux based IMA policy	All	Security Enhanced Linux is added as an additional layer of system security for access controls for the applications, processes, and files on the SLXOS system.
MAC policy for user space binaries	All	Security Enhanced Linux (SE Linux) implements Mandatory Access Control (MAC). Every process and system resource is issued a special security label called an SE Linux context.
Ability to upgrade ONIE/GRUB	SLX 9150, SLX 9250, Extreme 8720 and Extreme 8520	Provides the ability to install *onie, diag* and *onie-grub* images from SLXOS
Force port 1G speed/duplex via constrained advertised capabilities	SLX 9150, Extreme 8520	Adds the support of 10G port in 1G forced mode in full duplex with clock parameter to auto negotiate based on peer capabilities
Processing ACL rule for Tunneled traffic	SLX 9740	Supports ingress ACL on tunnels to match the inner headers for VxLAN, GRE and MPLS tunnels
BGP Dynamic Peering Scale Enhancement	All	Increases the number of BGP peers for Dynamic BGP Peers
IPV6 protocol support on TPVM	All	Introduces the initial support of IPv6 protocol for TPVM
IPv6 Support for Peer-Address in a Route Map for BGP	All	Supports of `set ipv6 next-hop peer-address` in route-map for BGP
BGP dampening for peer flaps	All	Adds the BGP peer dampening capability for unusable BGP peers

CLI Commands

The following commands were added, modified, or deprecated for the 20.4.1 program

New commands for 20.4.1

- neighbor peer-dampening
- neighbor peer-dampening (peer-group)
- peer-dampening
- show grubversion
- show [ip|ipv6] bgp peer-dampened
- show onieversion
- show selinux status
- snmp-server trap
- update onie

Modified commands for 20.4.1

- dns (tpvm mode)
- interface management (tpvm mode)
- ntp (tpvm mode)
- set ip next-hop
- set ipv6 next-hop
- speed
- threshold-monitor Cpu
- threshold-monitor Memory
- tpvm download
- tpvm upgrade (tpvm mode)
- vrf-lite-capability

The following show commands were enhanced to show additional information.

- show interface ethernet
- show interface status
- show ipv6 bgp routes

Deprecated commands for 20.4.1

No commands were deprecated in this release.

Hardware Support

Supported devices and software licenses

Supported devices	Description
SLX9740-40C	Extreme SLX 9740-40C Router. Base unit with 40x100GE/40GE capable QSFP28 ports, 2 unpopulated power supply slots, 6 unpopulated fan slots
SLX9740-40C-AC-F	Extreme SLX 9740-40C-AC-F Router. Base unit with 40x100GE/40GE capable QSFP28 ports, 2 AC power supplies, 6 fan modules
SLX9740-80C	Extreme SLX 9740-80C Router. Base unit with 80x100GE/40GE capable QSFP28 ports, 4 unpopulated power supply slots, 4 unpopulated fan slots
SLX9740-80C-AC-F	Extreme SLX 9740-80C-AC-F Router. Base unit with 80x100GE/40GE capable QSFP28 ports, 4AC power supplies, 4 fan modules
SLX9740-ADV-LIC-P	Advanced Feature License for MPLS, BGP-EVPN and Integrated Application Hosting for Extreme SLX 9740
SLX9150-48Y-8C	Extreme SLX 9150-48Y Switch with two empty power supply slots, six empty fan slots. Supports 48x25GE/10GE/1GE + 8x100GE/40GE.
SLX9150-48Y-8C-AC-F	Extreme SLX 9150-48Y Switch AC with Front to Back Airflow. Supports 48x25GE/10GE/1GE + 8x100GE/40GE with dual power supplies, six fans.
SLX9150-48Y-8C-AC-R	Extreme SLX 9150-48Y Switch AC with Back to Front Airflow. Supports 48x25GE/10GE/1GE + 8x100GE/40GE with dual power supplies, six fans.
SLX9150-48XT-6C	Extreme SLX 9150-48XT 10GBaseT Switch with two empty power supply slots, six empty fan slots, Supports 48x10GE/1GE + 6x100GE/40GE.
SLX9150-48XT-6C-AC-F	Extreme SLX 9150-48XT 10GBaseT Switch AC with Front to Back Airflow, Supports 48x10GE/1GE + 6x100GE/40GE with dual power supplies, six fans.
SLX9150-48XT-6C-AC-R	Extreme SLX 9150-48XT 10GBaseT Switch AC with Back to Front Airflow, Supports 48x10GE/1GE + 6x100GE/40GE with dual power supplies, six fans.
SLX9150-ADV-LIC-P	SLX 9150 Advanced Feature License for GuestVM, Analytics Path, PTP, BGP-EVPN.
SLX9250-32C	SLX 9250-32C Switch with two empty power supply slots, six empty fan slots. Supports 32x100/40GE.
SLX9250-32C-AC-F	SLX 9250-32C Switch AC with Front to Back Airflow. Supports 32x100GE/40GE with dual power supplies, six fans.
SLX9250-32C-AC-R	SLX 9250-32C Switch AC with Back to Front Airflow. Supports 32x100GE/40GE with dual power supplies, six fans.
SLX9250-ADV-LIC-P	SLX 9250 Advanced Feature License for GuestVM, Analytics Path, BGP-EVPN.
BR-SLX-9540-48S-AC-R	SLX 9540-48S Switch AC with Back to Front airflow (Non-port Side to port side airflow). Supports 48x10GE/1GE + 6x100GE/40GE. (1+1) redundant power supplies and (4+1) redundant fans included.
BR-SLX-9540-48S-AC-F	SLX 9540-48S Switch AC with Front to Back airflow (Port-side to non-port side airflow). Supports 48x10GE/1GE + 6x100GE/40GE. (1+1) redundant power supplies and (4+1) redundant fans included.
BR-SLX-9540-24S-DC-R	SLX 9540-24S Switch DC with Back to Front airflow (Non-port Side to port side airflow). Supports 24x10GE/1GE + 24x1GE ports.

Supported devices	Description
BR-SLX-9540-24S-DC-F	SLX 9540-24S Switch DC with Front to Back airflow (Port-side to non-port side airflow). Supports 24x10GE/1GE + 24x1GE ports.
BR-SLX-9540-24S-AC-R	SLX 9540-24S Switch AC with Back to Front airflow (Non-port Side to port side airflow). Supports 24x10GE/1GE + 24x1GE ports.
BR-SLX-9540-24S-AC-F	SLX 9540-24S Switch AC with Front to Back airflow (Port-side to non-port side airflow). Supports 24x10GE/1GE + 24x1GE ports.
BR-SLX-9540-48S-DC-R	SLX 9540-48S Switch DC with Back to Front airflow (Non-port Side to port side airflow). Supports 48x10GE/1GE + 6x100GE/40GE. (1+1) redundant power supplies and (4+1) redundant fans included.
BR-SLX-9540-48S-DC-F	SLX 9540-48S Switch DC with Front to Back airflow (Port-side to non-port side airflow). Supports 48x10GE/1GE + 6x100GE/40GE. (1+1) redundant power supplies and (4+1) redundant fans included.
BR-SLX-9540-24S-COD-P	Upgrade 24x1GE to 24x10GE/1GE for SLX 9540
BR-SLX-9540-ADV-LIC-P	Advanced Feature License for SLX 9540
EN-SLX-9640-24S	Extreme SLX 9640-24S Router. Supports 24x10GE/1GE + 4x100GE/40GE. (24S+4C sku no Power supplies or Fans)
EN-SLX-9640-24S-12C	Extreme SLX 9640-24S Router. Supports 24x10GE/1GE + 12x100GE/40GE. (All ports 24S+12C sku with no Power supplies or Fans)
EN-SLX-9640-24S-AC-F	Extreme SLX 9640-24S Router AC with Front to Back airflow. Supports 24x10GE/1GE + 4x100GE/40GE.(1 Power supply 6 Fans)
EN-SLX-9640-24S-12C-AC-F	Extreme SLX 9640-24S Router AC with Front to Back airflow. Supports 24x10GE/1GE + 12x100GE/40GE.(1 Power supply 6 Fans)
EN-SLX-9640-4C-POD-P	Extreme SLX 9640 Ports on Demand License for 4 ports of 100GE/40GE Uplinks
EN-SLX-9640-ADV-LIC-P	Extreme SLX 9640 Advanced Feature License
8720-32C	Extreme 8720-32C Switch with two empty power supply slots, six empty fan slots and a 4-post rack mount kit, Supports 32x100/40GE
8720-32C-AC-F	Extreme 8720-32C Switch with front to back airflow, Supports 32x100/40G with two AC power supplies, six fans and a 4-post rack mount kit
8720-32C-AC-R	Extreme 8720-32C Switch with back to front airflow, Supports 32x100/40G with dual AC power supplies, six fans and a 4-post rack mount kit
8720-32C-DC-F	Extreme 8720-32C Switch with front to back airflow, Supports 32x100/40G with dual DC power supplies, six fans and a 4-post rack mount kit
8720-32C-DC-R	Extreme 8720-32C Switch with back to front airflow, Supports 32x100/40G with dual DC power supplies, six fans and a 4-post rack mount kit
8000-PRMR-LIC-P	Extreme 8000 Premier Feature License (includes Integrated Application Hosting)
8520-48Y-8C	Extreme 8520-48Y Switch with two empty power supply slots, six empty fan slots; Ships with one 4-post rack mount kit; Supports 48x25/10/1G and 8x100/40G ports
8520-48Y-8C-AC-F	Extreme 8520-48Y Switch with front-back airflow; Ships with two AC power supplies, six fans, one 4-post rack mount kit; Supports 48x25/10/1G and 8x100/40G ports

Supported devices	Description
8520-48Y-8C-AC-R	Extreme 8520-48Y Switch with back-front airflow; Ships with two AC power supplies, six fans, one 4-post rack mount kit; Supports 48x25/10/1G and 8x100/40G ports
8520-48Y-8C-DC-F	Extreme 8520-48Y Switch with front-back airflow; Ships with two DC power supplies, six fans, one 4-post rack mount kit; Supports 48x25/10/1G and 8x100/40G ports
8520-48Y-8C-DC-R	Extreme 8520-48Y Switch with back-front airflow; Ships with two DC power supplies, six fans, one 4-post rack mount kit; Supports 48x25/10/1G and 8x100/40G ports
8520-48XT-6C	Extreme 8520-48XT Switch with two empty power supply slots, six empty fan slots; Ships with one 4-post rack mount kit; Supports 48x10/1G copper ports and 6x100/40G fiber ports
8520-48XT-6C-AC-F	Extreme 8520-48XT Switch with front-back airflow; Ships with two AC power supplies, six fans, one 4-post rack mount kit; Supports 48x10/1G copper ports and 6x100/40G fiber ports
8520-48XT-6C-AC-R	Extreme 8520-48XT Switch with back-front airflow; Ships with two AC power supplies, six fans, one 4-post rack mount kit; Supports 48x10/1G copper ports and 6x100/40G fiber ports
8520-48XT-6C-DC-F	Extreme 8520-48XT Switch with front-back airflow; Ships with two DC power supplies, six fans, one 4-post rack mount kit; Supports 48x10/1G copper ports and 6x100/40G fiber ports
8520-48XT-6C-DC-R	Extreme 8520-48XT Switch with back-front airflow; Ships with two DC power supplies, six fans, one 4-post rack mount kit; Supports 48x10/1G copper ports and 6x100/40G fiber ports
8000-PRMR-LIC-P	Extreme 8000 Premier Feature License (includes Integrated Application Hosting)

Supported power supplies, fans, and rack mount kits

XN-ACPWR-1600W-F	SLX 9740 Fixed AC 1600W Power Supply Front to Back. Power cords not included.
XN-ACPWR-1600W-R	SLX 9740 Fixed AC 1600W Power Supply Back to Front. Power cords not included.
XN-DCPWR-1600W-F	SLX 9740 Fixed DC 1600W Power Supply Front to Back. Power cords not included.
XN-ACPWR-1600W-F	SLX 9740 Fixed AC 1600W Power Supply Front to Back. Power cords not included.
XN-FAN-003-F	SLX 9740 FAN Front to Back airflow for SLX9740-40C
XN-FAN-003-R	SLX 9740 FAN Back to Front airflow for SLX9740-40C
XN-FAN-004-F	SLX 9740 FAN Front to Back airflow for SLX9740-80C
XN-FAN-004-R	SLX 9740 FAN Back to Front airflow for SLX9740-80C
XN-4P-RKMT299	2-Post Rail Kit for SLX 9740-40C
XN-2P-RKMT300	2-Post Rail Kit for SLX 9740-80C
XN-4P-RKMT301	4-Post Rail Kit for SLX 9740-80C
XN-4P-RKMT302	4-Post Rail Kit for SLX 9740-40C
XN-ACPWR-750W-F	AC 750W PSU, Front to Back Airflow supported on VSP 7400, SLX 9150, SLX 9250, X695, Extreme 8720, Extreme 8520
XN-ACPWR-750W-R	AC 750W PSU, Back to Front Airflow supported on VSP 7400, SLX 9150, SLX 9250, X695, Extreme 8720, Extreme 8520
XN-DCPWR-750W-F	DC 750W PSU, Front to Back Airflow supported on VSP 7400, SLX 9150, SLX 9250, X695, Extreme 8720, Extreme 8520
XN-DCPWR-750W-R	DC 750W PSU, Back to Front Airflow supported on VSP 7400, SLX 9150, SLX 9250, X695, Extreme 8720, Extreme 8520
XN-FAN-001-F	Front to back Fan for use in VSP 7400, SLX 9150, SLX 9250, X695, Extreme 8720, Extreme 8520
XN-FAN-001-R	Back to Front Fan for use in VSP 7400, SLX 9150, SLX 9250, X695, Extreme 8720, Extreme 8520
XN-4P-RKMT298	Four post rack mount rail kit supported on VSP 7400, SLX 9150, SLX 9250, X695, Extreme 8720, Extreme 8520
XN-2P-RKMT299	Two post rack mount rail kit supported on VSP 7400, SLX 9150, SLX 9250, X695, Extreme 8720, Extreme 8520

Supported Optics and Cables

For a complete list of all supported optics, see **Extreme Optics** at https://optics.extremenetworks.com/.

Supported FEC modes

SLX 9250 and Extreme 8720

Port Type	Media Type	Default FEC Mode	Supported FEC Modes
100G	Passive DAC	RS-FEC	RS-FEC Disabled
100G	SR4	RS-FEC	RS-FEC Disabled
100G	LR4	Disabled	RS-FEC Disabled
25G	Breakout DAC SR	Auto-Neg	RS-FEC FC-FEC Auto-Neg Disabled
25G	Breakout SR4	FC-FEC	RS-FEC FC-FEC Disabled

SLX 9740

Port Type	Media Type	Default FEC Mode	Supported FEC Modes
100G	Passive DAC	RS-FEC	RS-FEC Disabled
100G	SR4	RS-FEC	RS-FEC Disabled
100G	LR4	Disabled	RS-FEC Disabled
25G	Breakout DAC SR	FC-FEC	FC-FEC RS-FEC Disabled
25G	Breakout SR4	FC-FEC	FC-FEC RS-FEC Disabled

SLX 9150 and Extreme 8520

Port Type	Media Type	Default FEC Mode	Supported FEC Modes
100G	Passive DAC	RS-FEC	RS-FEC Disabled

Port Type	Media Type	Default FEC Mode	Supported FEC Modes
100G	SR4	RS-FEC	RS-FEC Disabled
100G	LR4	Disabled	RS-FEC Disabled
25G(Native)	DAC	Auto-Neg	RS-FEC FC-FEC Auto-Neg Disabled
25G(Native)	SFP	FC-FEC	RS-FEC FC-FEC Disabled

SLX 9540 and SLX 9640

Port Type	Media Type	Default FEC Mode	Supported FEC Modes
100G	Passive DAC	RS-FEC	RS-FEC Disabled
100G	SR4	RS-FEC	RS-FEC Disabled
100G	LR4	Disabled	RS-FEC Disabled

Software Download and Upgrade

For more information about the various methods of upgrading to SLX-OS 20.4.1, see the *Extreme SLX-OS Software Upgrade Guide.*

Image files

Download the following images from www.extremenetworks.com.

Image file name	Description
SLX-OS_20.4.1.tar.gz	SLX-OS 20.4.1 software
SLX-OS_20.4.1_mibs.tar.gz	SLX-OS 20.4.1 MIBS
SLX-OS_20.4.1.md5	SLX-OS 20.4.1 md5 checksum
SLX-OS_20.4.1-digests.tar.gz	SLX-OS 20.4.1 sha checksum
SLX-OS_20.4.1-releasenotes.pdf	Release Notes

Notes:

Upgrade to 20.3.x from earlier releases requires “fullinstall” due to change in glibc for all platforms.

Extreme 8720

To / From	20.2.3x	20.3.2/a/b	20.3.2c/d	20.3.3	20.3.4	20.3.4a/ac	20.4.1
20.2.3(MFG)	Use the normal Firmware Download / coldboot	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall
20.2.3ab	Use the normal Firmware Download / coldboot	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall
20.2.3x	NA	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall
20.3.2/a/b	Use fullinstall	NA	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.
20.3.2c/d	Use fullinstall	Use the normal Firmware Download / coldboot	NA	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.
20.3.3	Use fullinstall	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	NA	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot
20.3.4	Use fullinstall	Use the normal Firmware	Use the normal Firmware	Use the normal Firmware	NA		Use the normal Firmware

To / From	20.2.3x	20.3.2/a/b	20.3.2c/d	20.3.3	20.3.4	20.3.4a/ac	20.4.1
		Download / coldboot	Download / coldboot	Download / coldboot		Use the normal Firmware Download / coldboot	Download / coldboot
20.3.4a/ac	Use fullinstall	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	NA	Use the normal Firmware Download / coldboot
20.4.1	Use fullinstall	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	NA

SLX 9740

To / From	20.2.2x	20.2.3x	20.3.1	20.3.2/a/b	20.3.2c/d	20.3.3	20.3.4	20.3.4a/ac	20.4.1
20.2.1a	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall
20.2.2x	Use the normal Firmware Download / coldboot*	Use the normal Firmware Download / coldboot	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall

To / From	20.2.2x	20.2.3x	20.3.1	20.3.2/a/b	20.3.2c/d	20.3.3	20.3.4	20.3.4a/ac	20.4.1
20.2.3_CR	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall
20.2.3x	Use the normal Firmware Download / coldboot	NA	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall
20.3.1	Use fullinstall	Use fullinstall	NA	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.
20.3.2/a/b	Use fullinstall	Use fullinstall	Use the normal Firmware Download / coldboot	NA	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.

To / From	20.2.2x	20.2.3x	20.3.1	20.3.2/a/b	20.3.2c/d	20.3.3	20.3.4	20.3.4a/ac	20.4.1
20.3.2c/d	Use fullinstall	Use fullinstall	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	NA	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.
20.3.3	Use fullinstall	Use fullinstall	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	NA	Use the normal Firmware Download / coldboot.	Use the normal Firmware Download / coldboot.	Use the normal Firmware Download / coldboot.
20.3.4	Use fullinstall	Use fullinstall	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	NA	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot
20.3.4a/ac	Use fullinstall	Use fullinstall	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	NA	Use the normal Firmware Download / coldboot.
20.4.1	Use fullinstall	Use fullinstall	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	NA

*within the patches

Note:

For SLX-9740, downgrade to any 20.2.2x version needs to be done in two steps, with an intermediate step for downgrading to 20.2.2c and then to 20.2.x from 20.2.3x or higher.
This restriction is not applicable for upgrade/downgrade between 20.2.3x and 20.3.x releases.

SLX 9540 and SLX 9640

To / From	20.2.2a/b/c	20.2.3a to 20.2.3h	20.3.1	20.3.2/a/b	20.3.2c/d	20.3.3	20.3.4	20.3.4a/ac	20.4.1
18r.2.00, 18r.2.00a/b/c	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to 20.2.2a/b/c using fullinstall. For SLX 9640: 1. First upgrade to 18r.2.00d via fullinstall. 2. Then upgrade to 20.1.2h	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to targeted 20.2.3 version using fullinstall. For SLX 9640: 1. First upgrade to 18r.2.00d via fullinstall.	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to 20.3.1 version using fullinstall. For SLX 9640: 1. First upgrade to 18r.2.00d via fullinstall. 2. Then upgrade to	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to targeted 20.3.2 version using fullinstall. For SLX 9640: 1. First upgrade to 18r.2.00d via fullinstall.	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to 20.3.2d version using fullinstall. For SLX 9640: 1. First upgrade to 18r.2.00d via fullinstall. 2. Then upgrade to	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to 20.3.3 version using fullinstall. For SLX 9640: 1. First upgrade to 18r.2.00d via fullinstall. 2. Then upgrade to	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to 20.3.4 version using fullinstall. For SLX 9640: 1. First upgrade to 18r.2.00d via fullinstall. 2. Then upgrade to	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to 20.3.4a version using fullinstall. For SLX 9640: 1. First upgrade to 18r.2.00d via fullinstall. 2. Then upgrade to	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to 20.4.1 version using fullinstall. For SLX 9640: 1. First upgrade to 18r.2.00d via fullinstall. 2. Then upgrade to

To / From	20.2.2a/b/c	20.2.3a to 20.2.3h	20.3.1	20.3.2/a/b	20.3.2c/d	20.3.3	20.3.4	20.3.4a/ac	20.4.1
	using fullinstall. 3. Then upgrade to 20.2.2a/b/c using fullinstall.	2. Then upgrade to 20.1.2h using fullinstall. 3. Then upgrade to targeted 20.2.3 version using fullinstall.	20.1.2h using fullinstall. 3. Then upgrade to 20.3.1 version using fullinstall.	2. Then upgrade to 20.1.2h using fullinstall. 3. Then upgrade to targeted 20.3.2 version using fullinstall.	20.1.2h using fullinstall. 3. Then upgrade to 20.3.2d version using fullinstall.	20.1.2h using fullinstall. 3. Then upgrade to 20.3.3 version using fullinstall.	20.1.2h using fullinstall. 3. Then upgrade to 20.3.4 version using fullinstall.	20.1.2h using fullinstall. 3. Then upgrade to 20.3.4a version using fullinstall.	20.1.2h using fullinstall. 3. Then upgrade to 20.4.1 version using fullinstall.
18r.2.00d	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to 20.2.2a/b/c using fullinstall. For SLX 9640: 1. First upgrade to 20.1.2h	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to targeted 20.2.3 version using fullinstall. For SLX 9640:	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to 20.3.1 version using fullinstall. For SLX 9640: 1. First upgrade to	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to targeted 20.3.2 version using fullinstall. For SLX 9640:	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to 20.3.2d version using fullinstall. For SLX 9640: 1. First upgrade to	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to 20.3.3 version using fullinstall. For SLX 9640: 1. First upgrade to	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to 20.3.4 version using fullinstall. For SLX 9640: 1. First upgrade to	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to 20.3.4a version using fullinstall. For SLX 9640: 1. First upgrade to	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to 20.4.1 version using fullinstall. For SLX 9640: 1. First upgrade to

To / From	20.2.2a/b/c	20.2.3a to 20.2.3h	20.3.1	20.3.2/a/b	20.3.2c/d	20.3.3	20.3.4	20.3.4a/ac	20.4.1
	using fullinstall. 2. Then upgrade to 20.2.2a/b/c using fullinstall.	1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to targeted 20.2.3 version using fullinstall.	20.1.2h using fullinstall. 2. Then upgrade to 20.3.1 version using fullinstall.	1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to targeted 20.3.2 version using fullinstall.	20.1.2h using fullinstall. 2. Then upgrade to 20.3.2d version using fullinstall.	20.1.2h using fullinstall. 2. Then upgrade to 20.3.3 version using fullinstall.	20.1.2h using fullinstall. 2. Then upgrade to 20.3.4 version using fullinstall.	20.1.2h using fullinstall. 2. Then upgrade to 20.3.4a version using fullinstall.	20.1.2h using fullinstall. 2. Then upgrade to 20.4.1 version using fullinstall.
20.1.1	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to 20.2.2a/b/c using fullinstall. For SLX 9640: Use fullinstall.	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to targeted 20.2.3 version using fullinstall. For SLX 9640:	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to 20.3.1 version using fullinstall. For SLX 9640: Use fullinstall.	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to targeted 20.3.2 version using fullinstall. For SLX 9640:	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to 20.3.2d version using fullinstall. For SLX 9640: Use fullinstall.	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to 20.3.3 version using fullinstall. For SLX 9640: Use fullinstall.	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to 20.3.4 version using fullinstall. For SLX 9640: Use fullinstall.	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to 20.3.4a version using fullinstall. For SLX 9640: Use fullinstall.	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to 20.4.1 version using fullinstall. For SLX 9640: Use fullinstall.

To / From	20.2.2a/b/c	20.2.3a to 20.2.3h	20.3.1	20.3.2/a/b	20.3.2c/d	20.3.3	20.3.4	20.3.4a/ac	20.4.1
		Use fullinstall.		Use fullinstall.					
20.1.2e, g	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall
20.2.1a	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall
20.2.2x	NA	Use the normal Firmware Download / coldboot	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall
20.2.3x	Use the normal Firmware Download / coldboot	NA	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall
20.3.1	Use fullinstall	Use fullinstall	NA	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.
20.3.2/a/b	Use fullinstall	Use fullinstall	Use the normal Firmware	NA	Use the normal Firmware Download	Use the normal Firmware Download	Use the normal Firmware Download	Use the normal Firmware Download	Use the normal Firmware Download

To / From	20.2.2a/b/c	20.2.3a to 20.2.3h	20.3.1	20.3.2/a/b	20.3.2c/d	20.3.3	20.3.4	20.3.4a/ac	20.4.1
			Download / coldboot		/ coldboot. For downgrade use fullinstall.	/ coldboot. For downgrade use fullinstall.	/ coldboot. For downgrade use fullinstall.	/ coldboot. For downgrade use fullinstall.	/ coldboot. For downgrade use fullinstall.
20.3.2c/d	Use fullinstall	Use fullinstall	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	NA	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.
20.3.3	Use fullinstall	Use fullinstall	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	NA	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot
20.3.4	Use fullinstall	Use fullinstall	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	NA	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot
20.3.4a/ac	Use fullinstall	Use fullinstall	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	NA	Use the normal Firmware Download / coldboot
20.4.1	Use fullinstall	Use fullinstall	Use the normal Firmware	Use the normal Firmware	Use the normal Firmware	Use the normal Firmware	Use the normal Firmware	Use the normal Firmware	NA

To / From	20.2.2a/b/c	20.2.3a to 20.2.3h	20.3.1	20.3.2/a/b	20.3.2c/d	20.3.3	20.3.4	20.3.4a/ac	20.4.1
			Download / coldboot	Download / coldboot	Download / coldboot	Download / coldboot	Download / coldboot	Download / coldboot	

Notes:

- When upgrading from the 18r.1.00x and 18r.2.00a and earlier patches, upgrade first to 18r.2.00bx and then to 20.2.2x, which is a two-step upgrade procedure.
- The MCT upgrade procedure from 18r.2.00bc to 20.2.x is detailed in the *Extreme SLX-OS Software Upgrade Guide.*
- Because SLX 9540 is a bare metal device, use the "fullinstall" option to migrate between the SLX-OS 20.2.2x and SLX-OS 20.1.x releases.
- Because SLX9540 is moved to the bare metal mode in 20.2.1, use 'fullinstall' when migrating between SLX-OS 20.2.2x and SLX-OS 2.1.x releases.
- Upgrade to 20.3.x from earlier releases requires "fullinstall" due to change in glibc.
- Downgrading from 20.3.x/20.2.2x/20.2.3x to 20.1.1 requires 'fullinstall' option for all platforms due to a change in glibc
- Downgrading from 20.3.x/20.2.2x/20.2.3x to 20.1.1 may not require a 2-step procedure.

SLX 9150 and SLX 9250

To / From	20.2.2x	20.2.3x	20.3.1	20.3.2/a/b	20.3.2c/d	20.3.3	20.3.4	20.3.4a/ac	20.4.1
20.1.1	Use the normal firm ware download / coldboot	Use the normal firm ware download / coldboot	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall
20.1.2x	Use the normal firmware download / coldboot	Use the normal firm ware download / coldboot	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall

To / From	20.2.2x	20.2.3x	20.3.1	20.3.2/a/b	20.3.2c/d	20.3.3	20.3.4	20.3.4a/ac	20.4.1
20.2.1x	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall
20.2.2x	Use the normal firmware download / coldboot*	Use the normal firmware download / coldboot	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall
20.2.3_CR	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall
20.2.3x	Use the normal firmware download / coldboot	NA	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall
20.3.1	Use fullinstall	Use fullinstall	NA	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot
20.3.2/a/b	Use fullinstall	Use fullinstall	Use the normal firmware download / coldboot	NA	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot

To / From	20.2.2x	20.2.3x	20.3.1	20.3.2/a/b	20.3.2c/d	20.3.3	20.3.4	20.3.4a/ac	20.4.1
20.3.2c/d	Use fullinstall	Use fullinstall	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	NA	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot
20.3.3	Use fullinstall	Use fullinstall	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	NA	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot
20.3.4	Use fullinstall	Use fullinstall	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	NA	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot
20.3.4a/ac	Use fullinstall	Use fullinstall	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	NA	Use the normal firmware download / coldboot
20.4.1	Use fullinstall	Use fullinstall	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	NA

*within the patches

Extreme 8520

To / From	20.3.3	20.3.4	20.3.4a/ac	20.4.1
20.3.3	NA	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot
20.3.4	Use the normal Firmware Download / coldboot	NA	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot
20.3.4a/ac	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	NA	Use the normal Firmware Download / coldboot
20.4.1	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	NA

SLX TPVM Support Matrix for SLX 9150, SLX 9250, Extreme 8520, and Extreme 8720

SLX Build	TPVM – Fresh Install Supported	EFA
20.2.2	TPVM-4.1.1	EFA-2.3
20.2.2a	TPVM-4.1.2	EFA-2.3.x
20.2.2b	TPVM-4.1.2	EFA-2.3.x
20.2.3	TPVM-4.2.2	EFA-2.4.x, EFA-2.3.x
20.2.3a	TPVM-4.2.3	EFA-2.4.x, EFA-2.3.x, EFA-2.5x *
20.3.1	TPVM-4.2.4	EFA-2.4.x
20.3.2/a/b/c	TPVM-4.2.5	EFA-2.4.x, EFA-2.5x
20.3.2d	TPVM-4.3.0	EFA-2.4.x, EFA-2.5x
20.3.3	TPVM-4.2.5	EFA-2.5x
20.3.4	TPVM-4.4.0	EFA-2.5x
20.3.4a	TPVM-4.4.0	EFA-2.6.0
20.3.4ac	TPVM-4.4.0	EFA-2.6.1
20.4.1	TPVM-4.5.0	EFA-2.7.0

* EFA-2.4.x feature parity in 20.2.3d

Note:
Extreme 8720 and Extreme 8520 are supported from 20.3.3 onwards.

Upgrade and Downgrade considerations for Threshold Monitor configuration:

Downgrade Considerations:

1. If configured value for Cpu "limit" exceeds valid range in older release [0-80] then downgrade will be blocked with error. User can reconfigure Cpu “limit” in the range [0-80] and downgrade.

2. If configured value for Memory "high-limit" exceeds valid range in older release [0-80] or if it is less than the default value of "limit" in older release [60], then downgrade will be blocked with error. User can reconfigure Memory “high-limit” in the range [60-80] and downgrade.

3. If the startup file has “actions” configured as “snmp” or “all”, then config replay process triggered in firmware full-install downgrade, will lead all the corresponding threshold-monitor CLI parameters, such as poll, retry, to reset to respective default values.

Upgrade Considerations:

1. If the startup file has “Memory limit and /or low-limit” configured, then config replay process triggered in firmware full-install downgrade, will lead all the corresponding threshold-monitor CLI parameters, such as poll, retry, to reset to respective default values.

Upgrading the TPVM without configuration persistence (Legacy upgrade method)

Upgrading TPVM from 4.0.x or 4.1.x to 4.2.x, 4.3.x, 4.4.x, 4.5.x

Consider the following when upgrading TPVM from 20.1.2x , 20.2.2/x to 20.2.3x, 20.3.1 to 20.3.2x, 20.3.3, 20.3.4x

- SLX-OS 20.3.x, 20.2.3/x has TPVM 4.2.x. SLX-OS 20.1.2x variants have TPVM 4.0.x, which is based on Ubuntu18.
- To upgrade from TPVM 4.0 to latest, do the following:
  - Upgrade to SLX-OS 20.3.x, 20.2.3/x while the existing TPVM installation continues to run
  - Remove the existing TPVM using the **tpvm stop** and **tpvm uninstall** commands.
  - Copy the new *tpvm-4.x.x-0.amd64.deb* to */tftpboot/SWBD2900* on the SLX device.
  - Install TPVM 4.x.x using the **tpvm install** or **tpvm deploy** command.
    - Note that any additional TPVM disks, including vdb (implicitly created by TPVM 4.0.x or 4.1.x), are preserved with data during the previous steps.
  - If you need to remove the disks and start clean, then use the **tpvm uninstall force** command in place of **tpvm uninstall** in these steps. Alternatively, you can use **tpvm disk remove name <disk name>** to remove each additional disk manually. For example, `tpvm disk remove name vdb`.
- To perform patch upgrade from TPVM 4.5 to latest, do the following:
  - Upgrade to SLX-OS 20.4.x while the existing TPVM 4.5.0 installation continues to run
  - Copy the *new tpvm_inc_upg-4.5.X-X.amd64.deb* to */tftpboot/SWBD2900* on the SLX device.
  - Install TPVM 4.5.x using **tpvm upgrade incremental** command

Consider the following when you upgrade TPVM from releases earlier than SLX-OS 20.2.1 to SLX-OS 20.2.x:

- During startup, the latest TPVM creates an additional TPVM disk (named vdb) and creates an ext4 partition inside it (named vdb1).
- This additional disk partition is mounted at `/apps` inside TPVM.
- The disk uses all the free space available and reserved for TPVM (platform specific) TPVM disk quota.
- If you are running an older TPVM and have the additional TPVM disks already created, it is recommended and as a best practice to make a backup and then delete the old disks. Use the **tpvm disk remove name <disk name>** command to remove the disk, which requires TPVM to be started if not already running.
- Uninstall the older TPVM using the **tpvm stop** and **tpvm uninstall** command.
- Install the new TPVM package using the **tpvm install** or **tvpm deploy** command.

Alternatively, after SLX has been upgraded, you can use one command, **tpvm uninstall force**, to uninstall the TPVM and delete all the disks in the TPVM disk pool.

Important: The **tpvm uninstall force** process is destructive and irreversible, causing all TPVM data to be lost. The process works only if the TPVM is installed on the system.

Entire TPVM Data is automatically backed up in SLX while doing "**tpvm stop**" and restored during the next "**tpvm start**". However, only "/apps" partition and its data are preserved during "tpvm stop, uninstall" & "tpvm install". User installed applications in TPVM are not preserved. During TPVM upgrade, it is advised to take EFA data backup from TPVM using "**efa system backup**" and transfer the backup file outside TPVM to be completely safe. EFA release note document has a section for TPVM upgrade scenario and entire steps are mentioned in that document.

"**When EFA is installed on TPVM, "tpvm stop" followed by "uninstall" automatically takes only EFA database backup and not a backup of EFA installation."**

Notes:

Security updates are added to the TPVM image and also to the separate Debian file used for incremental TPVM update. There is a change in size of the main TPVM image to ~2.3 GB and the TPVM incremental update Debian file size is ~0.5 GB. These TPVM packages contain Ubuntu security patches available up to 03rd April, 2022. You must have at least 1GB of free space on the switch before proceeding with the `tpvm upgrade incremental` command

VDB disk size for EFA has changed to 40 GB to accommodate storage for snapshot and the remaining space is considered as reserved space, for the new TPVM installation.

Upgrading the TPVM with configuration persistence – Recommended method

Consider the following when upgrading TPVM from 20.1.2x , 20.2.2/x, 20.3.x to 20.3.2x, 20.3.3, 20.3.4x

1. SLX-OS old version with tpvm instance installed/deployed and few related config may be set.
2. SLX-OS upgrade done vide `firmware download` CLI command.
3. Across SLX-OS reboots, old TPVM too shall reboot if auto-boot config was there, else shall be there in installed state.
    a. tpvm stop

b. tpvm uninstall

i. (or) tpvm uninstall force – if you plan to delete disk vdb (i.e. the TPVM /apps partition).

ii. Note:

1. New mode like old mode, create disk vdb (/apps) by default upon first install/deploy or reuse previously existing partition.

2. Currently the new mode does not support new disk creation. The **tpvm disk add** command can be used.

4. As simple example for new mode of deploying TPVM:

a. Copy new TPVM debian Image under /tftpboot/SWBD2900. Only one file should be there and no subfolder should be present/created within this folder.

b. Deploy TPVM in Config Mode:

```
SLX # config terminal

SLX (config)# tpvm TPVM

SLX (config-tpvm-TPVM) # deploy
SLX (config-tpvm-TPVM) # end
```

Above will install and start any TPVM image kept under /tftpboot/SWBD2900.

c. Deploy TPVM with some configuration and later update any runtime configuration:

```
SLX # config terminal

SLX (config)# tpvm TPVM

SLX (config-tpvm-TPVM) # password newpassword
SLX (config-tpvm-TPVM) # interface management ip 10.25.24.21/24
SLX (config-tpvm-TPVM) # auto-boot
SLX (config-tpvm-TPVM) # hostname newhostname
SLX (config-tpvm-TPVM) # timezone Europe/Stockholm
SLX (config-tpvm-TPVM) # deploy
SLX (config-tpvm-TPVM) # end

SLX # config terminal

SLX (config)# tpvm TPVM

SLX (config-tpvm-TPVM) # hostname oldhostname
SLX (config-tpvm-TPVM) # no timezone

SLX (config-tpvm-TPVM) # exit
```

5. Note:

a. Now, say, if the **tpvm config hostname xyz** command is used. It will still work and apply on TPVM instance. But this configuration shall not be persisted in SLX Database and will become inconsistent. Same is true for any other configuration done in old way.

b. As in above example, password, management configuration should always be set before deploy. If required later, refer User Guide and use tpvm stop, start for such update/maintenance reason.

c. If **tpvm unstall force** command is used, then you will need to perform a **no deploy** and **deploy** in the new mode.

For more information on configuring TPVM Configuration Persistence, refer the 'Management Configuration Guide' for this version.

TPVM Migration

Upgrading the SLXOS to 20.3.2x, 20.3.3, 20.3.4x results in the creation of TPVM entries in SLX running-config implicitly (This happens when upgrading TPVM from SLXOS 20.1.2x, SLXOS 20.2.2/x, SLXOS 20.3.x to SLXOS 20.3.2x, 20.3.3, 20.3.4x)

Consider the following when upgrading TPVM from SLXOS 20.1.2x, SLXOS 20.2.2/x, SLXOS 20.3.x to SLXOS 20.3.2x, 20.3.3, 20.3.4x

a. SLX-OS old version with tpvm instance installed/deployed and few related config may be set in legacy exec CLI method
b. SLX-OS upgrade done with "`firmware download`" CLI command.
c. Across SLX-OS reboot, TPVM entries are created in SLX running-config implicitly as part of the TPVM migration feature
d. Check the configuration are persisted in TPVM using the CLI "`show running configuration tpvm`"
e. For TPVM upgrade to the latest version use command "`tpvm upgrade` … "
f. For TPVM upgrade incremental to the latest patch use command " `tpvm upgrade incremental …`"

Limitations and Restrictions

Copy flash to startup and reload with TPVM

setNTPServer and setLDAPServer statuses are reported as failed in the output of the `show tpvm status-history`. After reload, TPVM is expected to be running when the above configurations are re-applied. When the TPVM is not running and the NTP and LDAP configurations are applied, these errors are seen. This is a limitation as reapplying NTP and LDAP configurations are not supported.

You need to have minimum 1GB free space on TPVM when you try to perform the security patch upgrade using the command `tpvm upgrade incremental …`

TPVM upgrade incremental command and file support is available only from 4.5 if we try to perform the incremental upgrade from 4.4.0 to latest, the upgrade fails and ask to perform the tpvm upgrade.

TPVM upgrade incremental command will not be supported when you try TPVM deploy in config mode and TPVM upgrade incremental command will not support with snapshot option.

Do not use the **tpvm upgrade incremental** command to upgrade the patches with *tpvm-4.X.X-X.amd64.deb*. Use the *tpvm_inc_upg-4.X.X-X.amd64.deb* image file to perform incremental upgrades.

Similarly, do not use the *tpvm_inc_upg-4.X.X-X.amd64.deb* image file to perform full upgrade. Do not use this file to perform **tpvm deploy** in *config mode* and *option*.

TPVM Migration

The following table lists the various TPVM configurations and their migration status.

Configuration	Migration State	Notes
tpvm auto-boot	Migrated	
tpvm disk	Not Migrated	Disk configuration is not supported in the configuration mode, and therefore, not migrated.
tpvm password	Migrated	Only the old password is migrated. This is due to the password being encrypted and stored and it is not possible to know if the password was changed during the migration.
tpvm config ntp	Migrated	
tpvm config dns	Migrated	
tpvm config ldap	Migrated	Secure LDAP require certificates. It is assumed that certificates are already downloaded and installed. Certificates are not validated during this migration. A notification will be sent to the user to reconfigure LDAP certificate settings.
tpvm config hostname	Migrated	
tpvm config timezone	Migrated	
tpvm deploy <interface> allow-pwless	Not Migrated	This is the new default configuration and is not migrated.
tpvm deploy mgmt [dhcp | static]	Migrated	
tpvm deploy insight	Not Migrated	Insight interface configuration is not supported when configuring using the Privilege Execution Mode commands.
tpvm config ldap ca-cert	Not Migrated	Configuring the TPVM LDAP ca certificate
dns primary-server ipv6_address secondary-server ipv6_address domain domain_name	Migrated	Configuring the TPVM DNS IPv6 with FQDN
ntp ipv6_address	Migrated	TPVM ntp IPV6 config
interface management ipv6 ipv6_address [gw ipv6_gw_address]	Migrated	TPVM management ip with IPV6 ip
tpvm upgrade [protocol protocol user username	Migrated	TPVM upgrade with IPV6 remote server config

Configuration	Migration State	Notes
password <password> host IPv6_host_address directory directory filename filename]		
tpvm upgrade incremental[protocol protocol user username password <password> host IPv6_host_address directory directory filename filename]	Migrated	TPVM upgrade only the patch upgrade
tpvm config trusted-peer	Not Migrated	All trusted-peer configurations are not migrated.

Additional information on TPVM Commands

Following list of TPVM commands under exec mode may not be supported in the future releases. The equivalent commands will continue to be available under config mode. Please refer to latest CLI documentation.

- tpvm config dns
- tpvm config hostname
- tpvm config ldap
- tpvm config ntp
- tpvm config timezone
- tpvm config trusted-peer
- tpvm auto-boot
- tpvm deploy
- tpvm password

Port macro restrictions on breakout port configuration on SLX 9740

A port macro (PM) is a port group. Each PM has 4 ports, which are contiguous. PM0 has ports 0/1-0/4, PM1 has ports 0/5-0/8, PM2 has ports 0/9-0/12, and so on.

There are 9 PMs in the SLX 9740-40C and 18 PMs in the SLX 9740-80C. Only the odd ports can be split to 4x10G or 4x25G using the breakout cables: 0/1, 0/3, 0/9, 0/11, 0/13, 0/15, 0/17, 0/19, 0/21, 0/23, 0/25, 0/27, 0/29, 0/31, 0/33, 0/35, 0/37, 0/39, 0/41, 0/43, 0/49, 0/51, 0/53, 0/55, 0/57, 0/59, 0/61, 0/63, 0/65, 0/67, 0/69, 0/71, 0/73, 0/75, 0/77, and 0/79. Breaking out these ports using the breakout cables results in 72 interfaces for the SLX 9740-40 and 144 interfaces for the SLX 9740-80C.

- Ports 5-8 and 45-48 cannot be broken up and are supported only in 100G.
- For any PM, 40G and 10G ports cannot coexist with 25G ports. The following configurations are not supported:

PM Configuration	Examples
If any port is configured as 40G or 4x10G breakout, no 4x25G breakout is allowed unless the 40G ports will be removed as part of the breakout operation.	• If 0/3 or 0/4 is 40G, you cannot configure 0/1 as 4x25G breakout. • If 0/1 is 4x10G breakout, you cannot configure 0/3 as 4x25G breakout. • If 0/3 is 4x10G breakout, you cannot configure 0/1 as 4x25G breakout. • If 0/1 or 0/2 is 40G, you can configure 0/1 as 4x25G breakout because 0/1 and 0/2 will be removed. • If 0/3 or 0/4 is 40G, you can configure 0/3 as 4x25G breakout because 0/3 and 0/4 will be removed.
If 4x25G breakout is configured, no 40G or 4x10G.	• If 0/1 is configured as 4x25G breakout, you cannot configure 0/3 or 0/4 as 40G. • If 0/1 is configured as 4x25G breakout, you cannot configure 0/3 as 4x10G breakout. • If 0/3 is configured as 4x25G breakout, you cannot configure 0/1 or 0/2 as 40G. • If 0/3 is configured as 4x25G breakout, you cannot configure 0/1 as 4x10G breakout.

QoS

- PCP remarking is not supported for SLX 9740.
- Conformed and Violated counters are not supported for egress rate limiting for SLX 9740.
- Egress rate limiting in a Bridge Domain configuration is not supported for SLX 9740.
- DSCP-COS map is not work correctly for SLX 9740.

Others

- sflow sampling does not work for VLL when BUM rate limiting is applied on interface in SLX 9740
- sflow sample traffic to CPU is rate limited. You can use the **qos cpu slot** command to change the rate.
- When Resilient Hashing CLI is enabled or disabled, or the *max-path* value is changed, it may cause **BFD sessions** in **related VRFs** to go down. However, **BFD sessions in unrelated VRFs will not be affected.**
- Resilient Hashing supports 16K flowset entries for SLX 9740, and 32K flowset entries for SLX 9150/9250.

Open Config Telemetry Support

- User authentication not supported.
- gNMI calls through inband interfaces not supported.
- Usage of wild cards is not supported.
- gNMI SET is not supported.
- gNMI ON CHANGE subscription is not supported.

Open Defects

The following software defects are open in SLX-OS 20.4.1 as of **April 2022**:

Parent Defect ID:	SLXOS-50693	**Issue ID:**	SLXOS-50693
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.1
Technology Group:	Traffic Management	**Technology:**	Rate Limiting and Shaping
Symptom:	Display summation of forwarded and dropped packets for the confirmed counter		
Condition:	Applying Egress Rate Limit on bridge domain and checking the statistics with "show stat bridge-domain x"		

Parent Defect ID:	SLXOS-52599	**Issue ID:**	SLXOS-52599
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.1a
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	IPv6 Addressing
Symptom:	/127 prefix routes are accepted and traffic is dropped for them.		
Condition:	If route profile "ipv6-max-prefix64" is enabled on SLX 9150, or SLX 9250		

Parent Defect ID:	SLXOS-52746	**Issue ID:**	SLXOS-53722
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.1a
Technology Group:	Monitoring	**Technology:**	sFlow
Symptom:	S-flow will not work for Virtual leased lines interface		
Condition:	When Storm control is applied on Virtual leased lines interface		

Parent Defect ID:	SLXOS-55243	**Issue ID:**	SLXOS-55243
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.2
Technology Group:	Security	**Technology:**	HTTP/HTTPS
Symptom:	Extreme switch bootup logs reports(sometimes) unavailable file (/usr/sbin/httpd.0)		
Condition:	Issue is seen after restarting HTTP(S) server multiple times		

Parent Defect ID:	SLXOS-55266	**Issue ID:**	SLXOS-55266
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.2
Technology Group:	Layer 2 Switching	**Technology:**	VLAN - Virtual LAN
Symptom:	On SLX 9740, ARP is not resolved and Source mac is not learned when the incoming IP packets are Priority Tagged (Vlan-0 with PCP bit set).		

Condition:	The connected device to the switch is configured to send Priority tagged packets on an untagged port. The source MACs are not learnt from IP packets on the switch.
Workaround:	Use DSCP instead of using Priority tagging for QoS.
Recovery:	No known recovery methods available.

Parent Defect ID:	SLXOS-56576	**Issue ID:**	SLXOS-56576
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.2
Technology Group:	Other	**Technology:**	Other
Symptom:	On SLX 9740, when the user upgrades software from 20.2.2a to a later release, device becomes unreachable when accessing through an in-band port.		
Condition:	Software upgrade through in-band port.		

Parent Defect ID:	SLXOS-57174	**Issue ID:**	SLXOS-57432
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3b
Technology Group:	Management	**Technology:**	Other
Symptom:	System memory usage increases slowly over time while being managed by EFA		
Condition:	Memory increase is seen when EFA frequently polls SLX for updates and health checks		

Parent Defect ID:	SLXOS-55211	**Issue ID:**	SLXOS-57437
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.2
Technology Group:	Management	**Technology:**	Other
Symptom:	Command is not successful and displays an error saying "Cannot resolve hostname"		
Condition:	Usage of "copy" command with FTP protocol and IPV6 address .		
Workaround:	Use IPv4 interface address		

Parent Defect ID:	SLXOS-57372	**Issue ID:**	SLXOS-57439
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3b
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Convergence times >500 msec are seen for South - North traffic when one of the two ports from Border Leaf to L3 gateway is shut.		
Condition:	This is a test for convergence numbers. There are two port channels between each Border Leaf to the two L3 gateways. One of the port channel is shut down at the Border Leaf. This forces the BL to		

	reprogram the traffic going over that port channel for the South - North traffic to the other port channel. The convergence times vary and there are occasional spikes of over 700 msec.

Parent Defect ID:	SLXOS-56401	**Issue ID:**	SLXOS-57443
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3
Technology Group:	Other	**Technology:**	Other
Symptom:	The following Brocade branded 4x10G breakout DAC modules are not detected sometimes. The affected module SKU's are 40G-DACP-QSFP4SFP1M, 40G-DACP-QSFP4SFP3M, 40G-DACP-QSFP4SFP5M		
Condition:	Over a period of time, the issue is seen from a corruption in the EEPROM MSA programming		

Parent Defect ID:	SLXOS-56740	**Issue ID:**	SLXOS-57454
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Convergence times > 500 msec are seen for South - North traffic when a port from Border Leaf to L3 gateway is shut		
Condition:	This is a test for convergence numbers. The port between a Border Leaf and an L3 gateway is shut which forces the BL to reprogram the next hop for the South - North traffic to go over the ICL. The convergence times vary and there are occasional spikes between 800 to 1000 msec.		

Parent Defect ID:	SLXOS-57721	**Issue ID:**	SLXOS-57721
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.2
Technology Group:	Management	**Technology:**	CLI - Command Line Interface
Symptom:	When we are pinging the destination with the domain name, output will be in decimal format(IP address instead of domain name)		
Condition:	When the firmware is SLXOS 20.1.2, SLXOS 20.2.1 or above ping will have the output in IP address instead of domain name.		

Parent Defect ID:	SLXOS-57738	**Issue ID:**	SLXOS-57738
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.2f
Technology Group:	MPLS	**Technology:**	IP over MPLS
Symptom:	Hops are not displayed in IPoMPLS trace		
Condition:	During traceroute of IPoMPLS traffic		

Parent Defect ID:	SLXOS-58198	**Issue ID:**	SLXOS-58198
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3c
Technology Group:	Other	**Technology:**	Other
Symptom:	ICL interface is not coming up.		
Condition:	After the BGP process is killed.		

Parent Defect ID:	SLXOS-60302	**Issue ID:**	SLXOS-60754
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2a
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	Static Routing (IPv4)
Symptom:	Shutting down the uplink port channel from the border leaf to the L3 gateway leads to traffic convergence of nearly 1 second		
Condition:	SLX-8720 is used as the border leaf pair and SLX-9640 as L3 gateway. There are 32 VRFs configured and there are IPv4 and IPv6 routes. There is a port-channel between the BL nodes and the gateway. The port-channel is shut at a border leaf node and the traffic is redirected from the border leaf node to its peer along the ICL. The convergence times for this are found to be more than expected. With static routes, the convergence times are in the order of 1 second. With only BGP routes and PIC enabled, it was upto around 730 msec.		

Parent Defect ID:	SLXOS-60298	**Issue ID:**	SLXOS-60757
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2a
Technology Group:	Other	**Technology:**	Other
Symptom:	One of the BFD session over MCT flaps on cluster node. There is no visible traffic loss as such because the other MCT peer takes the traffic over ICL and forwards it to CCEP DUT (from L3 GW).		
Condition:	On reload and system maintenance turn-off on an SLX8720 cluster node. System scale: 32 VRFs, at least 2 BFD over MCT, 2 HW BFD and 2 BFD over VxLAN session per VRF. (one IPv4 and one IPv6) (First 20 VRFs have 10+ BFD over MCT sessions towards CCEP DUTs, last 12 VRFs have 2 BFD over MCT sessions towards CCEP DUTs) All VE interfaces configured across all devices are dual stack. SW BFD sessions: 393 HW BFD sessions: 65		

	960 IPv4 routes, 960 IPv6 routes from L3 GW. 960 IPv4 routes, 960 IPv6 routes from CCEP DUTs. System-wide route scale: 3K IPv4 and 3K IPv6
Workaround:	issue seen on Ve's attached to BDs. Remove the VE from BD and reconfigure.

Parent Defect ID:	SLXOS-60448	**Issue ID:**	SLXOS-60912
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.2
Technology Group:	Management	**Technology:**	Configuration Fundamentals
Symptom:	DHCP/BOOTP request is seen sending out from mgmt. interface event after disable DHCP.		
Condition:	BMC is configured as DHCP client.		
Recovery:	Manually disable DHCP option from BMC . [root@slx]# bmc ipmitool lan set 1 ipsrc static		

Parent Defect ID:	SLXOS-60970	**Issue ID:**	SLXOS-60970
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.3
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	On SLX 9640. while programming 500 flowspec rules to hardware, a BFD session is down due to "Detection Time Expired" which in turn terminates BGP session. Some BGP sessions flapping are due to this.		
Condition:	In scaled setup, 500 BGP-flow spec rules are programmed in hardware		

Parent Defect ID:	SLXOS-61208	**Issue ID:**	SLXOS-61283
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2b
Technology Group:	Other	**Technology:**	Other
Symptom:	SLX 9540 device does not respond		
Condition:	Taking suppotsave when the free memory is below 600Mb.		
Recovery:	Power off/on the device		

Parent Defect ID:	SLXOS-61458	**Issue ID:**	SLXOS-61527
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2b
Technology Group:	Other	**Technology:**	Other

Symptom:	When the encrypted password string has “\” or “?” in the startup config, ? or \ is missed in the running-config after config restore and TPVM login will be failed
Condition:	Encrypted password string should not have these charater “\” or “?”
Workaround:	TPVM password command needs to be executed till the encrypted password string doesn't have the '\' and '?'.
Recovery:	TPVM password command needs to be executed again to recover TPVM login

Parent Defect ID:	SLXOS-61347	**Issue ID:**	SLXOS-61598
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2c
Technology Group:	Layer 2 Switching	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	In Multi-homed environment, shutdown of an LACP ES Port-channel may cause traffic flooding to other ES interfaces if the client/host device is not able to detect link flap and continue to send the traffic. Whenever LACP port-channel is shut, member ports will be disaggregated and laser will be down for few msec(around 100ms) to allow peer device to detect link event. After that link comes up and member port will be transitioned to disaggregated individual port. Some old devices may not be able to detect link flap and continue to send traffic for some more time till LACP timeout.		
Condition:	Some old hosts may not be able to detect link flap when the link goes down for short period of time. SLX 9150/9250 keep the link down for 100msec before bring up the link as lacp individual. If the dual homed host is not able to detect the link flap on LACP ESI shut, the host continues to send the traffic till LACP timeout. SLX device may flood the traffic (in vlan) during that period.		
Workaround:	Shutting the individual member ports along with ES port-channel avoids flooding in this scenario.		
Recovery:	This situation will be recovered automatically after LACP timeout. Client device detects LACP timeout after 3sec (in case of short lacp interval), and stops traffic.		

Parent Defect ID:	SLXOS-61510	**Issue ID:**	SLXOS-62106
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2c
Technology Group:	Management	**Technology:**	Software Installation & Upgrade
Symptom:	a) If the device is reloaded, running-configs is not retained with auto persistence enable as dcmd database is not present. b) If the device is not reloaded and do a normal fwdl or fullinstall, no issue will be seen.		
Condition:	If “firmware download + noreboot” is issued and later if the “firmware commit” is done and rebooted the device.		

Parent Defect ID:	SLXOS-62115	**Issue ID:**	SLXOS-62126
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2b
Technology Group:	Management	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	SNMP trap is not sent for Loopback interface which is a VTEP, during cluster bring-up after a reload.		
Condition:	Reload of switch that is in a MCT cluster. SNMP trap is not sent when an interface comes up. Issue is seen when VTEP comes up as part of cluster bring-up after reload.		

Parent Defect ID:	SLXOS-62773	**Issue ID:**	SLXOS-62773
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Some BGP EVPN ND routes are not flushed in BGP EVPN table alone when one MH node comes out from MM and traffic is not getting forwarded for those ND routes		
Condition:	This EVPN ND routes sync issue happens inconsistently when one MH node comes out from MM		

Parent Defect ID:	SLXOS-61178	**Issue ID:**	SLXOS-62976
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3d
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	ICMP - Internet Control Message Protocol
Symptom:	Slowness on the ping responses on SLX.		
Condition:	On SLX node, CPU is busy with the higher priority packets.		

Parent Defect ID:	SLXOS-62671	**Issue ID:**	SLXOS-62995
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.2
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4+ - IPv6 Border Gateway Protocol
Symptom:	Latency of around 250ms to 1second is observed on SLX device.		
Condition:	SLX node has experienced the CPU congestion		

Parent Defect ID:	SLXOS-63052	**Issue ID:**	SLXOS-63052
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	Static Routing (IPv4)
Symptom:	Higher convergence of traffic for primary and backup static nexthops.		
Condition:	When primary nexthop goes DOWN, secondary nexthop takes time to get installed and traffic handoff happens delayed.		

Parent Defect ID:	SLXOS-63118	**Issue ID:**	SLXOS-63118
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4
Technology Group:	Other	**Technology:**	Other
Symptom:	2nd and 3rd BO ports of 8520-48XT and 8520-48Y do not come up when OIR is done and they are connected to Spirent or a SLX 9150 respectively.		
Condition:	When OIR is done on 8520-48XT or 8520-48Y devices.		
Workaround:	Remove and configure the breakout config or reload the device.		

Parent Defect ID:	SLXOS-63121	**Issue ID:**	SLXOS-63121
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4
Technology Group:	Layer 2 Switching	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	"show cluster track" command does not display correct interface status		
Condition:	Interface status is not displayed as 'down' under 'show cluster track' when port-channel becomes down due to the minimum-link criteria not being met.		

Parent Defect ID:	SLXOS-61254	**Issue ID:**	SLXOS-63124
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 18r.1.00ca
Technology Group:	MPLS	**Technology:**	LDP - Label Distribution Protocol
Symptom:	Duplicate LDP Address Withdraw Message sent from LDP for each VC-Peer.		
Condition:	Issue is seen when we do "clear mac-address" under a bridge domain.		

Parent Defect ID:	SLXOS-63182	**Issue ID:**	SLXOS-63182
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4

Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Sometimes the switch reload is seen in a scaled environment.		
Condition:	In scaled environment and BGP PIC configuration is enabled, when routes are learned through BGP and are getting processed.		

Parent Defect ID:	SLXOS-63023	**Issue ID:**	SLXOS-63982
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.2g
Technology Group:	Management	**Technology:**	Software Installation & Upgrade
Symptom:	Device will boot to ONIE on bootrom, and waits for ever.		
Condition:	Doing firmware downgrade from 20.2.3 to 20.1.2 via USB.		
Workaround:	Use methods of firmware download, other than the USB.		

Parent Defect ID:	SLXOS-64409	**Issue ID:**	SLXOS-64606
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4a
Technology Group:	Management	**Technology:**	CLI - Command Line Interface
Symptom:	TPVM configuration is lost when the device reloads with default configuration during firmware update.		
Condition:	Issue happens when "default-config" option is provided in "firmware download" command.		
Workaround:	Execute following commands - "copy default-config startup-config" and then "firmware download" command without "default-config" option.		

Parent Defect ID:	SLXOS-64255	**Issue ID:**	SLXOS-65234
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 18r.1.00j
Technology Group:	Management	**Technology:**	CLI - Command Line Interface
Symptom:	ARP not resolved for the peer entry		
Condition:	When link fault is cleared.		

Parent Defect ID:	SLXOS-65249	**Issue ID:**	SLXOS-65249
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BFD - BiDirectional Forwarding Detection
Symptom:	In SLX 9740, Traffic Convergence takes ~3 seconds.		

Condition:	Nexthop change takes place in ECMP prefixes.

Parent Defect ID:	SLXOS-65321	**Issue ID:**	SLXOS-65321
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	Other
Symptom:	Traffic takes more than 700 msec to converge when the port channel between the border leaf and gateway fails, and the traffic is redirected over the ICL		
Condition:	When one port channel between a border leaf and the gateway is shutdown, the traffic should switch to the ICL. This takes more than 600 msec in the S-N direction.		

Parent Defect ID:	SLXOS-65436	**Issue ID:**	SLXOS-65436
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	Other
Symptom:	Not able to delete a logical interface.		
Condition:	When a new BD/LIF was created after LIF limit is reached.		

Parent Defect ID:	SLXOS-65700	**Issue ID:**	SLXOS-65700
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1
Technology Group:	MPLS	**Technology:**	MPLS VPLS - Virtual Private LAN Services
Symptom:	LACP configured Port channels may flap after clearing MACs.		
Condition:	Executing "clear mac dynamic" command on a Provider Edge node with more than 600 VPLS bridge domain configuration may cause LACP port channels to flap.		
Workaround:	MACs can be cleared one at a time or clear MAC by one VLAN at a time		

Parent Defect ID:	SLXOS-65885	**Issue ID:**	SLXOS-65889
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2ad
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	BGP sessions could flap due to BGP rate-limit thresholds.		

Condition:	BGP control packets may be dropped if BGP CPU rate-limit thresholds are reached in BGP scaling scenarios.

Parent Defect ID:	SLXOS-65909	**Issue ID:**	SLXOS-65909
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	EFA checks if BGP session ESTABLISHED and announces failure in bringing up the session established.		
Condition:	BGP session takes 30+ seconds to become ESTABLISHED. Before that EFA times out and announces failure.		

Parent Defect ID:	SLXOS-66144	**Issue ID:**	SLXOS-66144
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	Other
Symptom:	Traffic takes more than 900 msec in the N-S direction when a port channel between the Gateway and Border Leaf fails. Minimum link is configured over this port channel and the trigger is the shutdown of one interface belonging to the port channel.		
Condition:	Minimum-link is configured between border leaf and gateway. When a port channel member between them is shutdown in the BL side, the PO is expected to fail. The GW should redirect the traffic to the other border leaf. This was seen to take more than 900 ms. The GW is a SLX 9640.		

Parent Defect ID:	SLXOS-65379	**Issue ID:**	SLXOS-66289
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3j
Technology Group:	MPLS	**Technology:**	MPLS VPLS - Virtual Private LAN Services
Symptom:	MPLS encapsulated 'Unicast ICMP with destination MAC starts on 4' traffic fails to forward from 9740(PHP/P) to 9850(PE).		
Condition:	a) Establish VPLS session between 9850 & MLX with adding 9740 as Transit Node. b) Initiate traffic with destination MAC starts with 4 from CE to CE.		

Parent Defect ID:	SLXOS-66290	**Issue ID:**	SLXOS-66290
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1

Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	VRRPv2 - Virtual Router Redundancy Protocol Version 2
Symptom:	SAG mac is not programmed in hardware.		
Condition:	ESI flap on port-channel interface.		

Parent Defect ID:	SLXOS-66291	**Issue ID:**	SLXOS-66291
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Peer group command not accepted under router bgp user vrf		
Condition:	While trying to add peer group for BGP under user vrf.		

Parent Defect ID:	SLXOS-66262	**Issue ID:**	SLXOS-66385
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4a
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	ARP - Address Resolution Protocol
Symptom:	Response is not seen for Neighbor Solicitation		
Condition:	On capturing packets using port mirroring while receiving ICMP6 Neighbor Solicitations at the rate of 1pkt/sec or more, a sporadic miss of Neighbor Advertisements (NA) is seen in the pcap file, though SLX responds with NA for each of them.		

Parent Defect ID:	SLXOS-66494	**Issue ID:**	SLXOS-66494
Severity:	S1 - Critical		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1
Technology Group:	Other	**Technology:**	Other
Symptom:	With FEC mode RS-FEC/FC-FEC configuration, the link is not coming up.		
Condition:	When configuring the "no shutdown" on the port, with FEC mode as RS-FEC /FC-FEC.		

Parent Defect ID:	SLXOS-66686	**Issue ID:**	SLXOS-66686
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1
Technology Group:	Other	**Technology:**	Other
Symptom:	"show efa status" is not getting the status from EFA and throwing the error		
Condition:	While doing multiple EFA upgrade without "no efa deploy", "show efa status" is not getting the status from EFA		

Workaround:	Execute "no efa deploy" before doing the "efa deploy" on the node with already EFA deployed.

Parent Defect ID:	SLXOS-66718	**Issue ID:**	SLXOS-66718
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1
Technology Group:	Other	**Technology:**	Other
Symptom:	Observed the optics removed for all ports.		
Condition:	After multiple device reloads on 9740 device.		

Parent Defect ID:	SLXOS-66716	**Issue ID:**	SLXOS-66727
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4a
Technology Group:	MPLS	**Technology:**	MPLS VPLS - Virtual Private LAN Services
Symptom:	show bridge-domain <BD#> logical-interface" displays the LIF as untagged, when it is configured as a tagged interface. This is cosmetic issue.		
Condition:	This is only cosmetic bug as traffic was working as tagged. When bridge-domain is configured with tagged interface, show command show it as untagged.		
Workaround:	None		

Parent Defect ID:	SLXOS-66738	**Issue ID:**	SLXOS-66738
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1
Technology Group:	Monitoring	**Technology:**	Port Mirroring
Symptom:	In port mirroring configuration if destination interface is a port-channel and source interface is either a port-channel or member of a port-channel then destination port-channel interface goes down.		
Condition:	Issue is seen if in port mirroring configuration destination interface is configured as a port-channel.		

Parent Defect ID:	SLXOS-66740	**Issue ID:**	SLXOS-66740
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BFD - BiDirectional Forwarding Detection
Symptom:	BFD daemon reboot may be seen.		
Condition:	Multiple times add and remove of EPGs from EFA.		

Parent Defect ID:	SLXOS-66741	**Issue ID:**	SLXOS-66741
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	Other
Symptom:	RH entries are exhausting. Utilizing more resources		
Condition:	Enabling Maintenance mode makes RH entries exhaust and utilize more resources		

Parent Defect ID:	SLXOS-66742	**Issue ID:**	SLXOS-66742
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1
Technology Group:	Layer 2 Switching	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	BUM packets failed to go out over CCEP(cluster client endpoint) ports		
Condition:	Below is the sequence of trigger: -Maintenance mode enable -Vlan delete/add against CCEP Interface -Disable Maintenance mode		

Parent Defect ID:	SLXOS-61178	**Issue ID:**	SLXOS-62976
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3d
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	ICMP - Internet Control Message Protocol
Symptom:	Slowness on the ping responses on SLX.		
Condition:	On SLX node, CPU is busy with the higher priority packets.		

Parent Defect ID:	SLXOS-66305	**Issue ID:**	SLXOS-66802
Severity:	S2 – Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4
Technology Group:	Other	**Technology:**	Other
Symptom:	In SLX-OS 9640, other unrelated 1G ports go down when one particular 1G port is reseated.		
Condition:	In SLX-OS 9640, for example, if ports 0/13, 0/14, 0/16, 0/17 have 1G optics and are UP, and when 0/13 optic is reseated, 0/14 and 0/16 also go down.		

Defects Closed with Code Changes

The following software defects were closed in 20.4.1 with a code change as of **April 2022**:

Parent Defect ID:	SLXOS-42488	**Issue ID:**	SLXOS-42488
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Other	**Technology:**	Other
Symptom:	"show running-config ip prefix-list <list-name>" on specific prefix-list sometimes doesnt work		
Condition:	issue is observed during highly scaled scale prefix-list configurations		

Parent Defect ID:	SLXOS-49454	**Issue ID:**	SLXOS-52076
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.1
Technology Group:	Management	**Technology:**	CLI - Command Line Interface
Symptom:	Sometimes, show running-config ip prefix-list <name> takes around 25 mins to display output		
Condition:	Issue is seen when the user is querying for a specific prefix-list while the device has highly scaled prefix list configuration		

Parent Defect ID:	SLXOS-56675	**Issue ID:**	SLXOS-56675
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3
Technology Group:	Other	**Technology:**	Other
Symptom:	WARNING message, Unqualified SFP transceiver for interface Ethernet 0/x is detected.		
Condition:	Insert 100G LR4 optic (EQPT1H4LR4LCL100) optics.		

Parent Defect ID:	SLXOS-57274	**Issue ID:**	SLXOS-57274
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.2
Technology Group:	Management	**Technology:**	CLI - Command Line Interface
Symptom:	On execution of "show run route-map" command with route map name like "show run route-map <route-map-name>" it throws error.		
Condition:	Issue is seen when "show run route-map" command is invoked with route map name.		

Parent Defect ID:	SLXOS-60172	**Issue ID:**	SLXOS-60176
Severity:	S1 - Critical		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3ea
Technology Group:	Other	**Technology:**	Other

Symptom:	We may see flap of any random interface during the bootup time of the device. The device can be SLX 9740, SLX 9250, SLX 8720, SLX 9150.
Condition:	Sometimes Port flap is seen on a device during bootup.

Parent Defect ID:	SLXOS-61120	**Issue ID:**	SLXOS-61167
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3b
Technology Group:	Layer 2 Switching	**Technology:**	VLAN - Virtual LAN
Symptom:	Access to SLX management port is not working.		
Condition:	Ping packet drop is seen if it passes through VLAN before turning back on the mgmt. interface.		

Parent Defect ID:	SLXOS-61209	**Issue ID:**	SLXOS-61209
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.3
Technology Group:	Layer 2 Switching	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	Broadcast, unknown unicast and Multicast traffic loss		
Condition:	Remote client interface shutdown followed by no cluster-client auto and cluster-client auto under local client interface		

Parent Defect ID:	SLXOS-62256	**Issue ID:**	SLXOS-62256
Severity:	S1 - Critical		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.3
Technology Group:	Layer 2 Switching	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	CCEP Port-channel flaps		
Condition:	With more than 96 Port-channels as MCT clients, and traffic running with COS priority of 6 or 7 - when one of the MCT node is reloaded, we see some of the CCEP Port-channels flapping on other MCT node.		

Parent Defect ID:	SLXOS-62863	**Issue ID:**	SLXOS-62863
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	1+ sec of traffic loss is observed during a border leaf reload.		
Condition:	Reloading one of SLX-9740 border leaf's in a MCT configuration		

Parent Defect ID:	SLXOS-62230	**Issue ID:**	SLXOS-62998
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.2c

Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	On SLX 9640, BGP flaps are seen sometimes		
Condition:	In a scaled environment, and when high rate of control packets are processed on CPU, it can lead to lead loss of BGP packets.		

Parent Defect ID:	SLXOS-62353	**Issue ID:**	SLXOS-63106
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2b
Technology Group:	Layer 2 Switching	**Technology:**	VXLAN - Virtual Extensible LAN
Symptom:	VRF traffic loss is greater than 1sec upon spine node reboot.		
Condition:	Upon spine reboot, few BFD sessions from compute nodes to border-leaf flap and traffic loss for 1-2 sec is observed.		

Parent Defect ID:	SLXOS-63253	**Issue ID:**	SLXOS-63253
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4
Technology Group:	Layer 2 Switching	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	MCT Cluster peer-interface Port-channel flaps few times		
Condition:	On reloading one of the border leaf nodes in the MCT configuration, ICL port-channel flaps, while the reloaded node is coming online. This happens when more than 5000 BFD sessions are established over the VxLAN tunnel.		

Parent Defect ID:	SLXOS-63282	**Issue ID:**	SLXOS-63282
Severity:	S1 - Critical		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4
Technology Group:	Monitoring	**Technology:**	Port Mirroring
Symptom:	On SLX 9740, flow based mirroring is not working for flow matching deny rules with the configured ACL		
Condition:	configure mirror action in deny rule , traffic matching deny rule are not mirrored.		

Parent Defect ID:	SLXOS-63289	**Issue ID:**	SLXOS-63289
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4
Technology Group:	Monitoring	**Technology:**	sFlow
Symptom:	Flow based ERSPAN mirroring is not working in the ingress direction.		
Condition:	If the configured ERSPAN id is more than 255.		

Parent Defect ID:	SLXOS-63125	**Issue ID:**	SLXOS-63317
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3g
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	MAC address is not updated properly when there is MAC move between MCT peer nodes multiple times.		
Condition:	In the IP fabric, the MAC move happens between the MCT peer nodes.		

Parent Defect ID:	SLXOS-63941	**Issue ID:**	SLXOS-63960
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.2bb
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Unexpected reload of the switch		
Condition:	During the SNMP walk with 1 M routes learnt from real internet feed, when any route among the learnt routes has a longer BGP AS path attribute.		

Parent Defect ID:	SLXOS-63974	**Issue ID:**	SLXOS-63978
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3g
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	BGP flaps could be seen during high scale of BGP packets to CPU if it hits threshold rate-limit.		
Condition:	BGP flaps could be seen during high scale of BGP packets to CPU if it hits threshold rate-limit.		

Parent Defect ID:	SLXOS-62922	**Issue ID:**	SLXOS-64002
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2d
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Some IPV4 BGP sessions gets deleted only after BGP hold timer expires even though BFD has gone down		
Condition:	When configuring with Extreme Fabric Automation(EFA), and EPG(End Point Group) is removed in the local node. Issue in the symptom is seen on the remote node.		

Parent Defect ID:	SLXOS-64007	**Issue ID:**	SLXOS-64083
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2b
Technology Group:	Layer 2 Switching	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	Port-channel interfaces stay down		
Condition:	On a 8720 MCT, when one of the MCT leaf reloads, port-channel interfaces stay down on one end, as the LACP packets are not being received.		

Parent Defect ID:	SLXOS-64022	**Issue ID:**	SLXOS-64090
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	MAC address is not updated properly when there is MAC move between MCT peer nodes multiple times.		
Condition:	In the IP fabric, the MAC move happens between the MCT peer nodes.		

Parent Defect ID:	SLXOS-63334	**Issue ID:**	SLXOS-64111
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 18r.1.00j
Technology Group:	MPLS	**Technology:**	MPLS VLL - Virtual Leased Line
Symptom:	User may experiences one way traffic over VLL usually during failover to bypass path.		
Condition:	Rarely, hardware fails to delete transit cross-connect, and hardware continues to have stale Label in MPLS forwarding table.		

Parent Defect ID:	SLXOS-64141	**Issue ID:**	SLXOS-64145
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2d
Technology Group:	Management	**Technology:**	Other
Symptom:	In case, when file replay takes place during reboot of the switch and the configuration file contains CLI for Maintenance Mode - "enable-on-reboot", then log "RASLOG SMAN-1004" is generated twice. This indicates system is entering into maintenance Mode.		
Condition:	During system reload, when the configuration file replay takes place as in case of "full-install"		

Parent Defect ID:	SLXOS-63036	**Issue ID:**	SLXOS-64417
Severity:	S3 - Moderate		

Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2b
Technology Group:	Management	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	During bootup, SNMP traps for link status of VE and loopback interfaces are sent even when "snmp trap lnk-status disable" is configured for the interfaces		
Condition:	Issue is seen only during bootup for VE and loopback interfaces that are not shutdown.		

Parent Defect ID:	SLXOS-64508	**Issue ID:**	SLXOS-64516
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4
Technology Group:	Layer 2 Switching	**Technology:**	VXLAN - Virtual Extensible LAN
Symptom:	Broadcast storm across IP Fabric caused by BUM traffic flooding due to Layer 2 loop		
Condition:	Adding another MCT pair into the exiting IP Fabric		

Parent Defect ID:	SLXOS-60949	**Issue ID:**	SLXOS-64600
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 18r.1.00h
Technology Group:	Other	**Technology:**	Other
Symptom:	Tx Errors observed on interfaces		
Condition:	Following different conditions are required to see this issue • oTraffic type • mixed traffic with jumbo frame sizes • Tunneled traffic of MPLS and VPLS • Ingress normal - egress tunneled traffic • Egress port-channels • QoS Port-Speed-Up command configured on the Port-Channels with the max allowed limit		

Parent Defect ID:	SLXOS-64668	**Issue ID:**	SLXOS-64673
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3c_CVR
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	During loop condition, BGP TTL1 packets maybe dropped.		
Condition:	During loop condition, BGP control packets may be classified as TTL1 packets and they are processed from Exception queue and maybe dropped once the threshold is reached.		

Parent Defect ID:	SLXOS-64669	**Issue ID:**	SLXOS-64677
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3c_CVR
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	BGP sessions may flap due to high rate of incoming BGP packets with TTL value 1.		
Condition:	BGP control packets with TTL value 1 may be dropped due to incorrect CPU queue classification with lower rate-limit of 100 pps for BGP protocols packets.		

Parent Defect ID:	SLXOS-64690	**Issue ID:**	SLXOS-64711
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.2c
Technology Group:	Other	**Technology:**	Other
Symptom:	Tx Errors observed on interfaces continuously incrementing at a significant number when monitored over a 24 hour period		
Condition:	Following different conditions are required to see this issue • oTraffic type • mixed traffic with jumbo frame sizes • Tunneled traffic of MPLS and VPLS • Ingress normal - egress tunneled traffic • Egress port-channels • QoS Port-Speed-Up command configured on the Port-Channels with the max allowed limit		

Parent Defect ID:	SLXOS-64211	**Issue ID:**	SLXOS-64722
Severity:	S2 – Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3d
Technology Group:	Layer 2 Switching	**Technology:**	LAG - Link Aggregation Group
Symptom:	Physical Port Laser was not turned OFF when port is made down.		
Condition:	When FEC is configured, physical port Laser was not turned OFF when port is made down		

Parent Defect ID:	SLXOS-64678	**Issue ID:**	SLXOS-64791
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BFD - BiDirectional Forwarding Detection
Symptom:	In 9250/9150/8720/8520 BFD sessions in MCT secondary border leaf node may flap.		

Condition:	While MCT primary border leaf node's cluster comes up after reload.

Parent Defect ID:	SLXOS-64803	**Issue ID:**	SLXOS-64844
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4a
Technology Group:	Layer 2 Switching	**Technology:**	LAG - Link Aggregation Group
Symptom:	LACP LAG continuously flaps with reason 'timeout' or 'peer-out-of-sync'.		
Condition:	When native VLAN is used in the range of 768 to 1023 on port-channel, with 'no switchport tag native' on SLX-9150/9250, port-channel may flap.		

Parent Defect ID:	SLXOS-64706	**Issue ID:**	SLXOS-64848
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2b
Technology Group:	Layer 2 Switching	**Technology:**	VXLAN - Virtual Extensible LAN
Symptom:	ARP/NDs are not resolved for the hosts reachable through one particular VxLAN tunnel (14th tunnel created - Tunnel 32785) in IP Fabric topology.		
Condition:	BUM traffic from Tunnel 32785 is being wrongly interpreted as ICL BUM traffic, and getting dropped at CCEP ports, which is leading to the failure of ARP/ND. Moreover this wrong mapping can cause BUM flooding to fabric side also.		

Parent Defect ID:	SLXOS-64941	**Issue ID:**	SLXOS-64941
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.3
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	SNMP OID extremeBgp4V2PrefixInPrefixes shows "Routes Accepted/Installed + Filtered"		
Condition:	extremeBgp4V2PrefixInPrefixes value is not accurate/confusing, when Filtered value is more than actual received routes.		

Parent Defect ID:	SLXOS-64244	**Issue ID:**	SLXOS-64951
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.2c
Technology Group:	Layer 2 Switching	**Technology:**	UDLD - Uni-Directional Link Detection

Symptom:	UDLD will not come-up between CE(slx) routers across mpls vll networks as UDLD pkts get dropped on transient SLX routers.
Condition:	UDLD will not come-up between CE(slx) routers across mpls vll networks as UDLD pkts get dropped on transient SLX routers(9540/9640/9850).

Parent Defect ID:	SLXOS-64594	**Issue ID:**	SLXOS-64979
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3g
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	Other
Symptom:	May notice traffic latency between end customers and data packets looks lifted to CPU on transit node for processing.		
Condition:	This issue may be seen only on MCT configured topology on SLX 9540 and SLX 9640.		

Parent Defect ID:	SLXOS-64048	**Issue ID:**	SLXOS-65198
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3g
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	Other
Symptom:	May notice traffic latency between end customers and data packets looks lifted to CPU on transit node for processing.		
Condition:	This issue maybe seen only on MCT configured topology on SLX 9540 and SLX 9640.		

Parent Defect ID:	SLXOS-64855	**Issue ID:**	SLXOS-65254
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4
Technology Group:	Security	**Technology:**	AAA - Authentication, Authorization, and Accounting
Symptom:	REST query for show-system-monitor fails		
Condition:	REST query for show-system-monitor from non-admin user		

Parent Defect ID:	SLXOS-64688	**Issue ID:**	SLXOS-65273
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	ARP - Address Resolution Protocol

Symptom:	When the port channel from an MCT node to the CCEP client goes down, the ping to the CCEP client fails, even though there is a path to the CCEP client through the ICL and the other MCT node.
Condition:	There is a CCEP client (Linux box) connected to a pair of MCT nodes through a port channel. A server is able to ping the client through the MCT node-1 and the port channel. When the port channel is shutdown at MCT node-1, the expectation is that the packet will be sent to MCT node-2 through ICL and to the client from there. But it was found the packet was getting dropped at MCT node-2 because it was going over the ICL as a VLAN tagged packet. This is applicable to SLX 9640 and SLX 9540.

Parent Defect ID:	SLXOS-64585	**Issue ID:**	SLXOS-65277
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4
Technology Group:	Management	**Technology:**	Configuration Fundamentals
Symptom:	DCMD module reboot was observed when deletion of VRF configuration was in progress and simultaneously request was made to read the configuration via REST.		
Condition:	The issue was seen during deletion of VRF configuration and simultaneously request was made to read the configuration via REST. This issue was seen rarely.		

Parent Defect ID:	SLXOS-65380	**Issue ID:**	SLXOS-65405
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4a
Technology Group:	Other	**Technology:**	Other
Symptom:	DNX entry for TPVM is missing after device reload with running TPVM		
Condition:	Issue is observed after device reload with running tpvm dnx entries		

Parent Defect ID:	SLXOS-65398	**Issue ID:**	SLXOS-65426
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4
Technology Group:	Layer 2 Switching	**Technology:**	VLAN - Virtual LAN
Symptom:	End point group (EPG) configuration from EFA fails to create new Bridge domain (BD) logical interfaces (LIF) as the system reached maximum allowed Attachment Circuit (AC) LIF scale. EFA displays the following error: %Error: Config not allowed as it will exceed system max allowed AC LIFs..', Error : EndpointGroup Creation failed		

Condition:	BD LIF creation beyond 9087 number fails with error code. This fix allows BD LIF scale to grow till 11,647 limit.

Parent Defect ID:	SLXOS-64783	**Issue ID:**	SLXOS-66047
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3g
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	Other
Symptom:	Traceroute command output not showing response time for some intermediate hops.		
Condition:	Traceroute command output not showing response time for some intermediate hops when destination is reachable via non-management VRF		

Parent Defect ID:	SLXOS-66123	**Issue ID:**	SLXOS-66136
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2d
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BFD - BiDirectional Forwarding Detection
Symptom:	Unexpected reload of router		
Condition:	Unexpected reload of router when BFD sessions are flapped.		

Parent Defect ID:	SLXOS-64995	**Issue ID:**	SLXOS-66153
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2b
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	ARP - Address Resolution Protocol
Symptom:	Some of the BFD sessions are going down		
Condition:	SRIOV ports are connected with Leaf pair in Active-Standby mode. Reload of the Leaf with active SRIOV port causes some of the BFD sessions to go down.		

Parent Defect ID:	SLXOS-66145	**Issue ID:**	SLXOS-66157
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4a
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BFD - BiDirectional Forwarding Detection
Symptom:	Unexpected reload of router		
Condition:	Router unexpectedly reloaded with BFD session flap.		

Parent Defect ID:	SLXOS-66161	**Issue ID:**	SLXOS-66197
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4ab
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BFD - BiDirectional Forwarding Detection
Symptom:	Unexpected reload of router		
Condition:	Unexpected reload of router with BFD configuration		

Parent Defect ID:	SLXOS-63139	**Issue ID:**	SLXOS-66229
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3g
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	Other
Symptom:	Traceroute command output not showing response time for some intermediate hops.		
Condition:	Traceroute command output not showing response time for some intermediate hops when destination is reachable via non-management VRF.		

Parent Defect ID:	SLXOS-66244	**Issue ID:**	SLXOS-66253
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4ab
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	Other
Symptom:	Traffic was getting dropped for one or a few VLANs after restoring from EFA config backup		
Condition:	The customer made an EFA backup. Removed a VRF configuration. Restored the EFA backup.		

Parent Defect ID:	SLXOS-64586	**Issue ID:**	SLXOS-66261
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2b
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	During loop condition, BGP TTL1 packets maybe dropped.		
Condition:	During loop condition, BGP control packets may be classified as TTL1 packets and they are processed from Exception queue and maybe dropped once the threshold is reached.		

Parent Defect ID:	SLXOS-62785	**Issue ID:**	SLXOS-66398
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2d
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	Other
Symptom:	Traffic loss of 2+ seconds observed in border leaf device.		
Condition:	When gateway link failover happens, traffic loss was observed in border leaf.		

Parent Defect ID:	SLXOS-66399	**Issue ID:**	SLXOS-66403
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BFD - BiDirectional Forwarding Detection
Symptom:	Default debug level of BFD is displayed.		
Condition:	On executing show debug all		

Parent Defect ID:	SLXOS-66687	**Issue ID:**	SLXOS-66687
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1
Technology Group:	Security	**Technology:**	HTTP/HTTPS
Symptom:	HTTP server is not accepting the connections and HTTP connection is refused.		
Condition:	HTTP server is not accepting the connections during EFA configuration, or while adding to the device to the EFA fabric in the EFA.		

Defects Closed without Code Changes

The following software defect was closed in 20.4.1 without code change as of **April 2022**.

Parent Defect ID:	SLXOS-46276	**Issue ID:**	SLXOS-46276
Reason Code:	Not Reproducible	**Severity:**	S2 - Major
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	The remote end tunnel retains old VTEP IP when VTEP IP is changed at the local end		
Condition:	When tunnel VTEP IP is changed locally, some of the evpn IMR routes for old VTEP IP are not withdrawn. Hence old tunnel exists at remote end.		
Workaround:	When VTEP IP is modified, please issue "clear bgp evpn neighbor all"		

Parent Defect ID:	SLXOS-46419	**Issue ID:**	SLXOS-46419
Reason Code:	Not Reproducible	**Severity:**	S3 - Moderate
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Monitoring	**Technology:**	Port Mirroring
Symptom:	QoS service-policy configuration is not allowed on a mirror destination port-channel.		
Condition:	Configure a port-channel as mirror destination and configure a service-policy under this port-channel.		
Workaround:	Remove mirror configuration and add service-policy under this port-channel. Reconfigure mirror session with this port-channel as mirror destination.		

Parent Defect ID:	SLXOS-47644	**Issue ID:**	SLXOS-47644
Reason Code:	Not Reproducible	**Severity:**	S2 - Major
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Security	**Technology:**	ACLs - Access Control Lists
Symptom:	OSPF neighbourship doesn't go down after applying IP ACL on the interface		
Condition:	Applying IP ACL after OSPF neighbourship up.		
Workaround:	Clear OSPF neighbourship after IP ACL applied.		

Parent Defect ID:	SLXOS-52329	**Issue ID:**	SLXOS-52329
Reason Code:	Will Not Fix	**Severity:**	S2 - Major
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.1a

Technology Group:	IP Multicast	**Technology:**	IGMP - Internet Group Management Protocol
Symptom:	The IGMP querier node does not receive IGMP joins on Multicast tunnel even though there are receivers present on other LVTEP. This causes IGMP group entry expiry after the time-out.		
Condition:	1. There should be MCT nodes acting as a leaf (LVTEP) and receiver should be connected to CCEP client or CEP port. 2. The MDT Rx path is on one MCT peer and MDT Tx path is on other MCT peer. 3. IGMP Query should be received on Multicast tunnel. 4. IGMP report should land on the peer which is having MDT Rx path.		
Workaround:	If Source or Receiver is connected to one of the MCT nodes, then it is recommended to configure IGMP snooping querier for the vlan or Bridge domain on both the MCT peers.		

Parent Defect ID:	SLXOS-52506	**Issue ID:**	SLXOS-52506
Reason Code:	Will Not Fix	**Severity:**	S2 - Major
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.1a
Technology Group:	Management	**Technology:**	Other
Symptom:	Netconf request to configure ip prefix-list without providing sequence number fails and returns error.		
Condition:	Issue exists only for configuration via Netconf		
Workaround:	Workaround is to provide sequence number value in the Netconf request while configuring ip prefix-list		

Parent Defect ID:	SLXOS-56861	**Issue ID:**	SLXOS-56861
Reason Code:	Not Reproducible	**Severity:**	S3 - Moderate
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.2
Technology Group:	Other	**Technology:**	Other
Symptom:	Sometimes, a unrelated interface can go down when an optic is inserted.		
Condition:	A new optic is inserted in SLX 9740.		

Parent Defect ID:	SLXOS-60682	**Issue ID:**	SLXOS-60682
Reason Code:	Network Tuning	**Severity:**	S3 - Moderate
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.1
Technology Group:	Other	**Technology:**	Other
Symptom:	Interface Link flap is observed.		
Condition:	Speed is configured on the interface		

Parent Defect ID:	SLXOS-60951	**Issue ID:**	SLXOS-61576
Reason Code:	Design Limitation	**Severity:**	S3 - Moderate
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3e

Technology Group:	Layer 2 Switching	**Technology:**	LAG - Link Aggregation Group
Symptom:	MAC address of port-channel INTF changes when system is reloaded after performing un-config and then config of port channel interfaces.		
Condition:	MAC address of port channel interfaces change in below two cases; 1. Without reload - Port-channel interfaces are configured. Some of the port-channel interfaces are un-configured, and configured again without any specific sequence. 2. Port-channel Interfaces config and un-config is done without any particular sequence. Then config is saved and system is reloaded.		
Workaround:	For SLX 9540, SLX 9640 and SLX 9740, Some number of port-channel INTF can be created in the incremental order interface index. (say , port-channel 1, then port-channel 2, …, then port-channel 10). Now, config can be saved, and these port-channel are kind or reserved for future use. With these steps followed, MAC address of port-channel interfaces will not change with reload as well.		

Parent Defect ID:	SLXOS-61371	**Issue ID:**	SLXOS-62218
Reason Code:	Network Tuning	**Severity:**	S2 - Major
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2
Technology Group:	Other	**Technology:**	Other
Symptom:	On SLX 9740, and breakout port cli command on a port-macro group, can cause other ports in same group to flap sometimes.		
Condition:	Issue is seen when the breakout command is configured.		

Parent Defect ID:	SLXOS-62270	**Issue ID:**	SLXOS-62361
Reason Code:	Not Reproducible	**Severity:**	S3 - Moderate
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2c
Technology Group:	Monitoring	**Technology:**	Port Mirroring
Symptom:	When VLAN is configured as source in monitor session , mirroring stops working after rebooting device		
Condition:	Configure flow based mirroring session with VLAN as source		
Workaround:	1)Delete Monitor configuration 2)Remove the ACL binding from the VLAN interface 3)Configure monitor session with VLAN as source 4)Bind L2 ACL on the VLAN interface.		

Parent Defect ID:	SLXOS-62507	**Issue ID:**	SLXOS-62712
Reason Code:	Not Reproducible	**Severity:**	S2 - Major
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2c
Technology Group:	Layer 2 Switching	**Technology:**	VXLAN - Virtual Extensible LAN
Symptom:	HSLagt daemon crash		

Condition:	HSLagt daemon termination is seen when VxLAN tunnel creation and deletion operations happen at very quick interval

Parent Defect ID:	SLXOS-60455	**Issue ID:**	SLXOS-62870
Reason Code:	Feature/Function Not Supported	**Severity:**	S3 - Moderate
Product:	SLX-OS	**Reported in Release:**	SLXOS 18r.1.00ch
Technology Group:	Layer 2 Switching	**Technology:**	xSTP - Spanning Tree Protocols
Symptom:	RPVST flaps on SLX device		
Condition:	when root bridge change occurs without any user intervention		

Parent Defect ID:	SLXOS-62690	**Issue ID:**	SLXOS-62986
Reason Code:	Insufficient Information	**Severity:**	S3 - Moderate
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3d
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	BGP session is down on SLX device		
Condition:	Interface down on SLX due to failure on the LACP BPDU's. This will lead to BGP session down.		

Parent Defect ID:	SLXOS-61558	**Issue ID:**	SLXOS-62992
Reason Code:	Insufficient Information	**Severity:**	S2 - Major
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3d
Technology Group:	Management	**Technology:**	Other
Symptom:	Occasional TPVM CPU spike above 90% noticed for 1-2 sec.		
Condition:	Collecting EFA support-save on TPVM.		

Parent Defect ID:	SLXOS-62722	**Issue ID:**	SLXOS-63001
Reason Code:	Feature/Function Not Supported	**Severity:**	S2 - Major
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3c
Technology Group:	Traffic Management	**Technology:**	QoS - Quality of Service
Symptom:	Packets are egressing with DSCP value as 0 value, irrespective of incoming DSCP value.		
Condition:	In IP fabric environment, packets ingress at the SLX 9150 leaf switch with non-zero DSCP values and egress the SLX 9250 border leaf switch.		

Parent Defect ID:	SLXOS-62849	**Issue ID:**	SLXOS-63004
Reason Code:	Working as Designed	**Severity:**	S2 - Major
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3g
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	May experience 20-60 seconds of traffic loss.		
Condition:	On BGP re-convergence on network with below scale values, where 873k+ bgp ipv4 routes + 136k+ bgp ipv6 routes made to switch other path because of manual shut on working path.		

Parent Defect ID:	SLXOS-62093	**Issue ID:**	SLXOS-63015
Reason Code:	Insufficient Information	**Severity:**	S3 - Moderate
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.2f
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BFD - BiDirectional Forwarding Detection
Symptom:	SLX stops forwarding the Traffic after the unexpected reload		
Condition:	BGP is configured on a SLX node. While processing the BGP packets, sometimes the switch reloads.		
Recovery:	Power cycle the switch.		

Parent Defect ID:	SLXOS-60943	**Issue ID:**	SLXOS-63018
Reason Code:	Feature/Function Not Supported	**Severity:**	S3 - Moderate
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.2g
Technology Group:	Monitoring	**Technology:**	sFlow
Symptom:	Sflow collector is configured for user vrf		
Condition:	Sflow sample reaching sflow collector via default vrf.		

Parent Defect ID:	SLXOS-63092	**Issue ID:**	SLXOS-63092
Reason Code:	Not Reproducible	**Severity:**	S2 - Major
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Convergence times of upto 800 msec is seen when an interface from the Gateway towards the Border Leaf is shut down		
Condition:	There is a port channel between PE router and the Border leaf. The minimum-links is configured in the port channel. One of the physical interfaces in the port channel is shut and the minimum-link configuration brings down the port channel.		

	The convergence time for the traffic from the border leaf towards the gateway is sometimes seen to be in the range of 500-800 msec.
Workaround:	Using only BGP routes and configuring Prefix-Independent-Convergence can provide better convergence times than having static routes.

Parent Defect ID:	SLXOS-63115	**Issue ID:**	SLXOS-63115
Reason Code:	Already Reported	**Severity:**	S2 - Major
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4
Technology Group:	Security	**Technology:**	ACLs - Access Control Lists
Symptom:	On SLX 9740, Ingress ipv6 access-list counters do not increment in ipv6-optimised tcam profile		
Condition:	User has configured to use ipv6-optimised tcam profile and has configured counters for matching ipv6 access-list rules. Issued "clear counters" cli command.		

Parent Defect ID:	SLXOS-62135	**Issue ID:**	SLXOS-64196
Reason Code:	Already Implemented	**Severity:**	S3 - Moderate
Product:	SLX-OS	**Reported in Release:**	SLXOS 18r.1.00b
Technology Group:	Monitoring	**Technology:**	RAS - Reliability, Availability, and Serviceability
Symptom:	Logs indicating flash size usage crossing high boundary		
Condition:	/var/log/hasm.log file size is large, with no impact on functionality		