ExtremeCloud™ Orchestrator Release Notes

Version 3.4.1

9037946-01 Rev AA
January 2024

Copyright © 2024 Extreme Networks, Inc. All rights reserved.

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see: www.extremenetworks.com/about-extreme-networks/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: https://www.extremenetworks.com/support/policies/open-source-declaration/

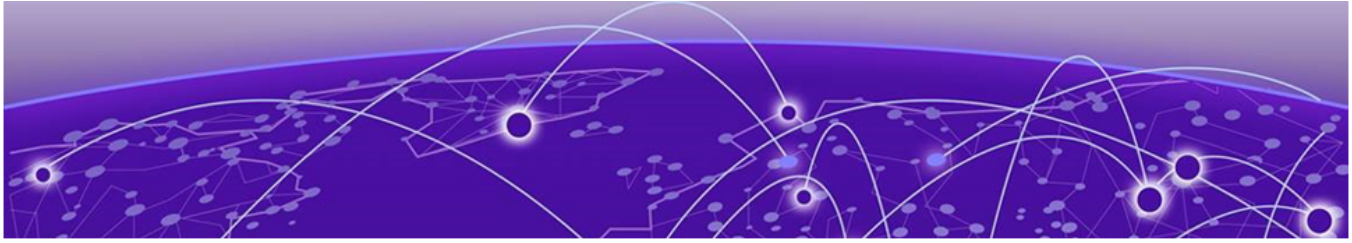


Table of Contents

Release Notes **4**

New In This Release 4

Supported Platforms and Deployment Models for Fabric Skill 5

Supported Platforms and Deployment Models for Visibility Skill 9

XCO Upgrade Prerequisites 11

Known Limitations 12

Known Limitations in Fabric Skill 12

Known Limitations in Visibility Skill 14

Defects Closed with Code Changes 15

Defects Closed with Code Changes in ExtremeCloud Orchestrator 3.4.1 15

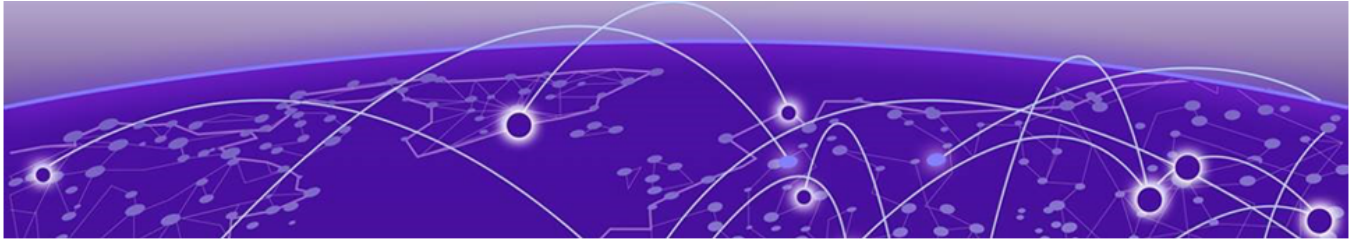
Defects Closed with Code Changes in ExtremeCloud Orchestrator 3.4.0 16

Defects Closed without Code Changes 25

Open Defects 27

Help and Support 37

Subscribe to Product Announcements 37



Release Notes

New In This Release on page 4
Supported Platforms and Deployment Models for Fabric Skill on page 5
Supported Platforms and Deployment Models for Visibility Skill on page 9
XCO Upgrade Prerequisites on page 11
Known Limitations on page 12
Defects Closed with Code Changes on page 15
Defects Closed without Code Changes on page 25
Open Defects on page 27
Help and Support on page 37

New In This Release

ExtremeCloud Orchestrator 3.4.1 resolves an issue through defect fix. For information about XCO deployment, refer to the *ExtremeCloud Orchestrator Deployment Guide, 3.4.0*.

Note
In release 3.2.0 and later, Extreme Fabric Automation (EFA) is referred to as ExtremeCloud Orchestrator (XCO). The terms EFA and XCO refer to the same product and are used interchangeably.

Supported Platforms and Deployment Models for Fabric Skill

Support includes Server, Open Virtual Appliance (OVA), and TPVM deployment models, supported TPVM versions, supported SLX-OS software versions, and supported SLX devices.

Note

- OVA deployment model does not support HA.
- As a best practice, refer to the following Extreme validated support matrices for support platforms and deployment models information.

Table 1: Server Deployment Models

XCO Version	Managed SLX Devices	Multi-Fabric Support	Ubuntu Server Version	Virtual Machine
3.1.x	More than 24	Yes	16.04, 18.04, and 20.04	• CPU: 4 cores • Storage: 64 GB • RAM: 8 GB
3.2.x	More than 24	Yes	18.04 and 20.04	• CPU: 4 cores • Storage: 64 GB • RAM: 8 GB
3.3.x	More than 24	Yes	18.04 and 20.04	• CPU: 4 cores • Storage: 64 GB • RAM: 8 GB
3.4.x	More than 24	Yes	18.04 and 20.04	• CPU: 4 cores • Storage: 64 GB • RAM: 8 GB

Table 2: OVA Deployment Models

XCO Version	Managed SLX Devices	Multi-Fabric Support	Ubuntu Version	Virtual Machine
3.1.x	More than 24	Yes	18.04	• CPU: 4 cores • Storage: 64 GB • RAM: 8 GB
3.2.x	More than 24	Yes	18.04	• CPU: 4 cores • Storage: 64 GB • RAM: 8 GB

Table 2: OVA Deployment Models (continued)

XCO Version	Managed SLX Devices	Multi-Fabric Support	Ubuntu Version	Virtual Machine
3.3.x	More than 24	Yes	20.04 LTS	• CPU: 4 cores • Storage: 64 GB • RAM: 8 GB
3.4.x	More than 24	Yes	20.04 LTS	• CPU: 4 cores • Storage: 64 GB • RAM: 8 GB

Table 3: TPVM Deployment Models

XCO Version	TPVM Deployment	Managed SLX Devices	Multi-Fabric Support	Ubuntu Version	Minimum SLX-OS Version
3.2.x	• SLX 9150 • SLX 9250 • SLX 9740 • Extreme 8520 • Extreme 8720 • Extreme 8820 (20.4.3 and later)	Up to 24	Yes	18.04	20.4.3
3.3.0	• SLX 9150 • SLX 9250 • SLX 9740 • Extreme 8520 • Extreme 8720 • Extreme 8820 (20.4.3 and later)	Up to 24	Yes	20.04 LTS	20.5.2

Table 3: TPVM Deployment Models (continued)

XCO Version	TPVM Deployment	Managed SLX Devices	Multi-Fabric Support	Ubuntu Version	Minimum SLX-OS Version
3.3.1	• SLX 9150 • SLX 9250 • SLX 9740 • Extreme 8520 • Extreme 8720 • Extreme 8820 (20.4.3 and later)	Up to 24	Yes	20.04 LTS	20.5.2a
3.4.x	• SLX 9150 • SLX 9250 • SLX 9740 • Extreme 8520 • Extreme 8720 • Extreme 8820 (20.4.3 and later)	Up to 24	Yes	20.04 LTS	20.5.2a

Table 4: TPVM Software Support

XCO Version	TPVM Version	SLX-OS Version
3.1.0	4.5.6	20.4.2a
3.1.1	4.5.8	20.4.3
3.2.0	4.5.10	20.4.3a
3.2.1	4.5.12	20.5.1
3.3.0	4.6.2	20.5.2
3.3.1	4.6.4	20.5.2a
3.4.0	4.6.6	20.5.3a
3.4.1	4.6.7	20.5.3a

Table 5: IP Fabric Topology Matrix

Device	SLX-OS Release	Leaf	Spine	Super Spine	Border Leaf	Small DC Fabric
SLX 9150	20.2.x, 20.3.x, 20.4.x	✔				✔
SLX 9250	20.2.x, 20.3.x, 20.4.x	✔	✔	✔		✔
SLX 9540	20.2.x, 20.3.x, 20.4.x	✔			✔	
SLX 9640	20.2.x, 20.3.x, 20.4.x				✔	

Table 5: IP Fabric Topology Matrix (continued)

Device	SLX-OS Release	Leaf	Spine	Super Spine	Border Leaf	Small DC Fabric
SLX 9740	20.2.x, 20.3.x, 20.4.x		✔	✔	✔	✔
Extreme 8720	20.3.x, 20.4.x	✔	✔	✔	✔	✔
Extreme 8520	20.3.x, 20.4.x	✔			✔	✔
Extreme 8820	20.4.3		✔	✔	✔	✔

Table 6: XCO or EFA, Neutron, and SLX-OS Compatibility

XCO or EFA Version	Neutron Version	SLX-OS Version
2.5.4, 2.5.5	3.1.1-04	20.3.2d

Supported Platforms and Deployment Models for Visibility Skill

Support includes Server, OVA, and supported devices and software.

Note

- Upgrade from XVM (Extreme Visibility Manager) to XCO is not supported.
- XCO supports only a fixed set of special characters for hostnames. Any additional characters configured in MLX or SLX are reconciled in XCO and can be edited or deleted. Any configuration name must start with an alphanumeric character and can contain a-z A-Z 0-9 _ -.

Table 7: Ubuntu Server Version

XCO Version	Ubuntu Version	Virtual Machine
3.1.x	18.04 and 20.04	Minimum: • CPU: 4 cores • Storage: 128 GB • RAM: 8 GB Recommended: • CPU: 16 cores • Storage: 200 GB • RAM: 32 GB
3.2.x	18.04 and 20.04	Minimum: • CPU: 4 cores • Storage: 128 GB • RAM: 8 GB Recommended: • CPU: 16 cores • Storage: 200 GB • RAM: 32 GB

Table 7: Ubuntu Server Version (continued)

XCO Version	Ubuntu Version	Virtual Machine
3.3.x	18.04 and 20.04	Minimum: • CPU: 4 cores • Storage: 128 GB • RAM: 8 GB Recommended: • CPU: 16 cores • Storage: 200 GB • RAM: 32 GB
3.4.x	18.04 and 20.04	Minimum: • CPU: 4 cores • Storage: 128 GB • RAM: 8 GB Recommended: • CPU: 16 cores • Storage: 200 GB • RAM: 32 GB

Table 8: OVA Deployment Models

XCO Version	Ubuntu Version	Virtual Machine
3.1.x	18.04	Minimum: • CPU: 4 cores • Storage: 64 GB • RAM: 8 GB
3.2.x	18.04	Minimum: • CPU: 4 cores • Storage: 64 GB • RAM: 8 GB

Table 8: OVA Deployment Models (continued)

XCO Version	Ubuntu Version	Virtual Machine
3.3.x	20.04 LTS	Minimum: • CPU: 4 cores • Storage: 64 GB • RAM: 8 GB
3.4.x	20.04 LTS	Minimum: • CPU: 4 cores • Storage: 64 GB • RAM: 8 GB

Table 9: Supported Devices and Software

Device	Supported Software
Extreme 9920	Extreme 9920 software with the NPB application • 21.1.2.x
Extreme Routing MLX Series	• NetIron 6.3.00 patches
Extreme Switching SLX 9140	• SLX-OS 18s.1.03 patches
Extreme Switching SLX 9240	• SLX-OS 18s.1.03 patches

XCO Upgrade Prerequisites

Prerequisites for XCO upgrade process with the default gateway changed:

1. Ensure that no DNS configuration exists under TPVM config and resolv.conf.
2. Presence of management connectivity from SLX and TPVM to external build server image, wherein image is available during SLX and TPVM upgrade process.

If file/etc/sshd/sshd_config is modified to non-default values, then manually readjust the following parameters:

- MaxStartups 30:30:100
- MaxAuthTries 6
- LoginGraceTime 120

Note
The hardening script, extr-granite.py bundled with EFA 2.6.1 will not automatically modify the above mentioned parameters.

Known Limitations

Note the following caveat for this release of ExtremeCloud Orchestrator.

- If the CLOS setup firmware upgrade encounters the error "Cannot start download before the new image is committed", then create a separate group only for the active XCO node and perform the firmware upgrade.

Known Limitations in Fabric Skill

Follow these caveats and limitations when using Fabric Skill.

Standby XCO Down after many unexpected reloads of the Active Node

Symptom	Condition	Workaround

After ~30 failovers the standby was found to be Down.	While testing HA resiliency by forcing a Kernel Panic on the active node	This is a known defect with the Open Source MariaDB 10.6.10 which falls into a core-dump crash loop.
		1. Stop MariaDB service:
		`sudo systemctl stop mariadb.service`
		2. Remove the Galera Cluster Cache:
		`sudo rm -f /apps/efadata/mysql/galera.cache`
		3. Restart MariaDB service:
		`sudo systemctl start mariadb.service`
		4. Confirm if MariaDB has started:
		`systemctl status mariadb`

Quality of Service (QoS) policy service support

- The XCO-driven application of policy is dynamic and can vary depending on the port's role, whether it belongs to a fabric, tenant, port channel, or tenant endpoint group.

Tip
As a best practice, avoid running user-driven policy operations in parallel with fabric, tenant, port channel, and tenant endpoint group operations.

To ensure that the fabric, tenant, port channel, and tenant endpoint group configurations are effective, run the **show** command before proceeding with the policy operations, and vice-versa.

- Before running the force operations, including deletion, ensure that you unbind the policies (QoS) from all the relevant targets (fabric, tenant, port, port channel, and tenant endpoint group) to avoid stale policies (QoS) in the system.
- Before executing the QoS policy bind commands, remove any conflicting or additional OOB (Out of Band) QoS configurations from the switches to ensure that the correct policies are applied to the ports.
- There is no support for a lossless hardware profile. Therefore, you must switch the configuration on SLX devices to a lossy hardware profile before provisioning QoS policies from XCO.
- There is no support for egress QoS maps. While XCO allows the configuration of egress QoS maps, as a best practice, do not configure any egress QoS maps from XCO due to limitations in SLX support of egress QoS maps.

VRF delete from EPG and re-adding VRF to EPG fails intermittently

Symptom	Condition	Workaround
Endpoint group (EPG) update **vrf-add** operation fails with the reason as VRF to be added has conflicting VRF on the switch.	Run EPG update **vrf-add**, **vrf-delete**, and **vrf-add** operation CLI in quick succession: 1. Update EPG for operation **vrf-add**. 2. Update EPG for operation **vrf-delete**. 3. Update the same EPG again with operation **vrf-add** for the same VRF which was deleted in step 2.	Wait of 30 seconds between the EPG update **vrf-add** and vrf-delete operations on the same EPG.

REST operations are not retried (as applicable) during the service boot

Symptom	Condition	Workaround
REST operations are not retried (as applicable) during the service boot up.	After publishing the necessary events on the message bus, the status for the REST operations are nit set automatically.	Manually set the status for all REST operations.

RBAC: XCO shows "export EFA_TOKEN" command suggestion when a tenant user logs in

Symptom	Condition	Workaround
XCO shows a **export EFA_TOKEN** message after a tenant user with RBAC logs in to the system.	When a user is created with the default login shell as sh.	XCO supports only bash shell for login or any other CLI commands. Ensure that bash is specified as the default login shell for all XCO user accounts.

EFA Token command message

Type this in your shell:

export EFA_TOKEN=eyJhbGciOiJSUzI1NiIsImtpZCI6IjEuMCIsInR5cCI6IkpXVCJ9.eyJjb21tb25fbmFtZSI6IkVGQSBUb2tlbiBTZXJ2aWNlIiwidWFzIjpbeyJ0YXJnZXQiOiJFRkEiLCJyb2xlIjoiVlIyLVRudEFkbWluIn1dLCJvcmciOiJFeHRyZW1lIE5ldHdvcmtzIiwidmVyIjoiMS4wIiwiaWQiOiIiLCJleHAiOjE2NDUyNDcxNDIsImp0aSI6IjZjMjA4ZDUxLTkwNzgtMTFlYy1iZjk5LWNhNzk1MDY1YzIwNyIsImlhdCI6MTY0NTE2MDc0MiwiaXNzIjoiRUZBIFRva2VuIFNlcnZpY2UiLCJuYmYiOjE2NDUxNjA3NDIsInN1YiI6InVzZXIyIn0.b7m5PINijeEdNSqnTeE2ZhUrqKLKQAu079vXyBIdgHbXKt9ULfa03vMU1jfBO1qFb1-x0oHmsAQ0pSsF5JLeMaMzMflLf78ktZO8U5IePq72vM5en35IR-DNLyoGIZBeFeG6ZbBMoETzz5vf9OuefgQID3YdjcALr7yllCgDmLVFlgson77yCBpkTK15xm1GRbtL7JKXZzShBE7E3kdW7N71MdM85Gc3r4l-c8sfz7eo06gKrfTq9wXCv4_LVzR6-KRSg6NyLq363WEpcK1A2Hs0Wo3T9TpquYHNaCWA5I1QTsG-RHFdg4kxZP2fQpUp6Bgy1s6k59PVPn4-M-a8lA— Time Elapsed: 4.619465187s —

XCO CLI or REST request with scale config takes longer than 15 minutes fails

Symptom	Condition	Workaround
Tenant2 delete is successful whereas deleting Tenant1 took more than 15 minutes and failed with the following message: Error : service is not available or internal server error has occurred, please try again later Tenant service was running. Tenant1 was not available after the error.	When you try to delete tenants in a single rack small data center deployment configured with scale tenant config	Any CLI or REST tenant operations, and any fabric operations taking more than 15 minutes, will timeout at the client side. The operation completes in the background. Run the **efa tenant show** command to view the actual state of the operation.

Known Limitations in Visibility Skill

Follow these caveats and limitations when using the Visibility Skill.

LAG created when port channel deployment fails

Any changes to ExtremeCloud Orchestrator configuration are reverted when a port channel deployment fails. However, a link aggregation group (LAG) is created on the device. The LAG is immediately deleted, but you can see the creation and deletion of a LAG in the device logs.

MLX UDA profile must be associated with an ingress group if the policy contains a UDA match

(MLX only) When you create an ingress group and associate it with an ingress policy, you must also associate the group with a UDA profile if the ingress policy contains a UDA match. For more information, see ExtremeCloud Orchestrator GUI Admin Guide.

Firmware upgrade requires an absolute path to image locations

In the **Absolute Path** field, enter the complete file path to the location of the firmware image. The following are sample file paths for the various supported devices.

- Extreme 9920 (absolute path to the binary file): /root/TierraOS--NPB.bin
- SLX (absolute directory path where supported image files are located): /root/slxos18s.1.03/slxos18s.1.03a
- MLX (path to the manifest file): XMR-MLX/MLX_npb_06200_mnf.txt

For more information, see ExtremeCloud Orchestrator GUI Admin Guide.

Device discovery

XCO deployed in packet broker mode supports device discovery notifications only for packet broker devices.

Listener policy byte count is incorrect when truncation is enabled

On the Extreme 9920 device, the byte count for truncated packets is the actual byte count seen by the egress ACL before truncation.

Defects Closed with Code Changes

The following defects were closed in ExtremeCloud Orchestrator 3.4.0 and 3.4.1.

Defects Closed with Code Changes in ExtremeCloud Orchestrator 3.4.1

Parent Defect ID:	XCO-9270	Issue ID:	XCO-9270
Product:	XCO	Reported in Release:	EFA 3.3.1
Symptom:	Standby node showing 'down' after continuous node reboot		
Condition:	Manually triggering SLX reload where the active XCO node is running and check the node status after reboot (when it moves to standby mode).		
Workaround:	N/A		
Recovery:	Reboot both active and standby nodes to recover from the situation		

Defects Closed with Code Changes in ExtremeCloud Orchestrator 3.4.0

Parent Defect ID:	XCO-4127	Issue ID:	XCO-4127
Product:	XCO	Reported in Release:	EFA 3.0.0
Symptom:	Ports are not listed in the port-channel creation for SLX NPB devices		
Condition:	Even though the ports are not used in any other configurations, the ports are not listed in the port-channel creation. For these ports, speed is set to auto-negotiation, and ports are not connected with cable.		
Workaround:	For breakout ports, make sure that cables are connected so that port speed will be updated.		
Recovery:	N/A		

Parent Defect ID:	XCO-4146	Issue ID:	XCO-4146
Product:	XCO	Reported in Release:	EFA 2.7.2
Symptom:	The fabric devices continue to remain in cfg-refresh-err state after the tpvm fail over.		

Parent Defect ID:	XCO-4146	Issue ID:	XCO-4146
Condition:	1.Fabric devices are already in cfg-refresh-err state due to LLDP Link down(LD) event. 2. Bring up the LLDP links responsible for the fabric devices to be in cfg-refresh-err state. 3. Execute the TPVM failover by 'tpvm stop' and 'tpvm start' commands during the LLDP Link up (LA) event handling caused by 2.		
Recovery:	1The user triggers LD/LA event by flapping the interface links which are the devices are in the cfg-refreshed state even though DRC wouldn't help out to recover the device to the cfg-sync state and the pending reason is "LA/LD". 1.1. "shutdown" the interface link on the physical link on Devices follow by "efa inventory device udpate --ip <device-ip>", which generates LD events 21.. "no shutdown" the interface link on the physical link on Devices follow by "efa inventory device udpate --ip <device-ip>", which generates LA events 1.3. If the pending config contains "LA" : Execute "efa inventory drift-reconcile execute --ip <device-ip> --reconcile" on the devices which are in cfg-refresh-err /cfg-refreshed state [or] IF the pending config contains "LD,LA" : Execute "efa fabric configure --name <fabric-name>" to clean up the configuration on devices which are in cfg-refresh-err /cfg-refreshed state. [OR] 2. The user reboots the devices without maintenance mode which are the devices are in cfg-refreshed state even though DRC wouldn't help out to recover the device to the cfg-sync state. 2.1. "reload" the switches without out maintenance mode to enable 2.2. Execute "efa inventory drift-reconcile execute --ip <device-ip> --reconcile" on the devices which are in cfg-refresh-err /cfg-refreshed state.		

Parent Defect ID:	XCO-7183	Issue ID:	XCO-7183
Product:	XCO	Reported in Release:	XCO 3.2.2
Symptom:	After changing DNS nameservers in /etc/netplan and running the update-dns.sh --dns-action allow, the following error is seen: (efa:ubuntu)ubuntu@efa:/opt/efa$ sudo /opt/efa/update-dns.sh /opt/efa/update-dns.sh Usage: --help - Show this message --dns-action <'allow'|'disallow'> - Allow host DNS entries to be forwarded to the pods (efa:ubuntu)ubuntu@efa:/opt/efa$ sudo /opt/efa/update-dns.sh --dnsaction allow Unexpected nameserver entry of 127.0.0.53 found in /etc/resolve.conf (efa:ubuntu)ubuntu@efa:/opt/efa$		

Parent Defect ID:	XCO-7183	Issue ID:	XCO-7183
Condition:	In 18.04.6 and 20.04, Ubuntu uses a stub-resolv.conf located in /run/systemd/resolve/stub-resolv.conf . This file is symlink to /etc/resolv.conf in /run/systemd/resolve/. There is another file, resolv.conf which contains the information for DNS from netplan. Additionally, systemd-resolved provides a local DNS stub listener on IP address 127.0.0.53 on the local loopback interface. Programs issuing DNS requests directly,bypassing any local API may be directed to this stub, in order to connect them to systemd-resolved. Note: The best practice is for local programs to use the glibc NSS or bus APIs instead (as described above), as various network resolution concepts (such as link-local addressing, or LLMNR Unicode domains) cannot be mapped to the unicast DNS protocol. We do not recognize the 127.0.0.53 address as valid.		
Workaround:	If updating DNS to allow host entries to be forwarded to the pods using the update-dns.sh script in XCO-3.3.0 on Ubuntu 20.0.4 or 18.0.4-6 or above, follow these steps. 20.0.4 or 18.0.4-6 or above, follow these steps: After netplan is applied and before running update_dns.sh 1. Check if symlink exists, if not directly edit /etc/resolv.conf to netplan ip $ ls -l /etc/resolv.conf lrwxrwxrwx 1 root root 39 Feb 20 2021 /etc/resolv.conf -> ../run/systemd/resolve/stub-resolv.conf <<<symlink exists sbr@sbr-virtual-machine ~ $ 2. Check if it has 127.0.0.53 ip in below files: ~ $ cat /etc/resolv.conf | grep nameserver nameserver 127.0.0.53 sbr@sbr-virtual-machine ~ $ cat /run/systemd/resolve/stub-resolv.conf | grep nameserver nameserver 127.0.0.53 sbr@sbr-virtual-machine ~ $ 3. Edit the following file to add netplan ip for the nameserver and remove 127.0.0.53 sudo vi /run/systemd/resolve/stub-resolv.conf 4. Check if both files are updated. ~ $ cat /run/systemd/resolve/stub-resolv.conf | grep nameserver nameserver 10.10.10.0 sbr@sbr-virtual-machine ~ $ cat /etc/resolv.conf | grep nameserver nameserver 10.10.10.0		

Parent Defect ID:	XCO-7183	Issue ID:	XCO-7183
	sbr@sbr-virtual-machine ~ $ 5. Run update_dns.sh --dns-action allow. 6. Run sudo netplan apply to restore /etc/resolv.conf and /run/systemd/resolve/stub-resolv.conf to its default value of 127.0.0.53.		

Parent Defect ID:	XCO-7955	Issue ID:	XCO-7955
Product:	XCO	Reported in Release:	XCO 3.3.0
Symptom:	When triggering the "Firmware Activate" process, it can lead to either parallel or serial execution, irrespective of the behavior of grouping devices for traffic loss. In cases where auto-commit is enabled, the activation can result in a "Firmware Commit Failed" status on the EFA end, even though the firmware commit has been successfully completed on the device end.		
Condition:	The "Firmware Activate" process is initiated from the user interface, either through the Inventory Page or the Fabric-wide Page, even in the midst of an incomplete operation on a subset of devices. For instance: Device 1 and Device 2 trigger a download with auto-commit enabled from either the Inventory or Fabric-wide Page. Device 3 triggers a download from the Fabric or Inventory Page. Subsequently, Device 1 and Device 2 attempt to continue with the "Activate Download" operation from the inventory or fabric page, resulting in a "Firmware Commit Failed" failure.		
Workaround:	Do not initiate firmware upgrades on other devices until the device completes both the Activate operation and the commit operation.		
Recovery:	Based on the error in the flow sequences, use the following set of commands: "efa inventory debug unblock-from-fwdl" , "efa inventory device firmware-download" to continue with download operation		

Parent Defect ID:	XCO-8070	Issue ID:	XCO-8070
Product:	XCO	Reported in Release:	XCO 3.2.1
Symptom:	'efa system backup' fails with Error : Failed to execute service lock API due to error Role ServiceAdmin does not have permissions to path: /v1/inventory/lockservice, method: POST.		
Condition:	When db error occurs in Rbac during initialization, then return gracefully. Allowing Rbac to do re-initialization. Earlier we were not returning when Db is unavailable/down, hence it was failing to load policies.		

Parent Defect ID:	XCO-8070	Issue ID:	XCO-8070
	Thus, not able to resolve permissions to run command.		

Parent Defect ID:	XCO-8128	Issue ID:	XCO-8128
Product:	XCO	Reported in Release:	XCO 3.2.1
Symptom:	Unable to Create EPG when out of band static-routes with next-hop interface exist		
Condition:	Root cause: There are multiple issues observed when oob static routes are added. (a) When null route is added, inventory table is populated with wrong interface name - tengigabitethernet 0, (b) published vrfupdate event does not contain interface name and nexthoptype value is set to invalid value - 0, (c) when tenant reads the event it writes incomplete information in its db and (d) Tenant does not know how to read back the incomplete back properly.		
Workaround:	Not appilcable.		
Recovery:	1. Remove the static-routes from the vrf config in the device. 2. Update the tenant db vrf_static_route to delete the corresponding stale records (oob_created=1 and nh_type = 0). 3. Create the previously failing new epg-s and confirm that they succeed. 4. Re-add the static-routes in the vrf config in the device.		

Parent Defect ID:	XCO-8200	Issue ID:	XCO-8200
Product:	XCO	Reported in Release:	XCO 3.3.0
Symptom:	SLX Devices are not allowed to execute the same firmware download execution flow, which could result in traffic loss. For example, it is not allowed to choose two Leaf devices from the same MCT pair.		
Condition:	From the User Interface, go to the **Fabric** page & select a few devices. Go to table action and select **Firmware Upgrade** option.		
Workaround:	The user selects the left-side leaf of the MCT pair and triggers firmware download and activation. Similarly, the user selects the right-side leaf of the MCT pair and triggers firmware download and activation.		
Recovery:	Choose another set of devices that will not result in traffic loss and proceed with the firmware download operation.		

Parent Defect ID:	XCO-8232	Issue ID:	XCO-8232
Product:	XCO	Reported in Release:	XCO 3.3.0
Symptom:	Error is observed while updating EFA system CLI setting		

Parent Defect ID:	XCO-8232	Issue ID:	XCO-8232
	Error : error creating directory on remote: Could not chdir to home directory /users/home21/<username>: No such file or directory		
Condition:	While using CLI "efa system settings update --remote-server-ip <ip> --remote-transfer-protocol scp --remote-server-username <username> --remote-server-password <password> --remote-server-directory <remote-server-directory>"		
Workaround:	Use Remote Server which has bash support installed.		
Recovery:	Add bash support and retry the CLI command.		

Parent Defect ID:	XCO-8234	Issue ID:	XCO-8234
Product:	XCO	Reported in Release:	XCO 3.3.0
Symptom:	The fabric alarm and the alarm status update notifications can briefly reflect a small time window where the fabric alarm is cleared when it is actually unhealthy.		
Condition:	This can occur during fabric formation or during any operation where fabric health is degraded due to multiple reasons (example:- spine to leaf link going down, BGP neighborship going down between spine and leaf, etc...). Once a specific device and links are repaired and deemed healthy, the overall fabric alarm may temporarily be cleared although other devices remain unhealthy. Then subsequently the fabric alarm will be corrected and put into an unhealthy state due to the remaining unhealthy devices.		
Workaround:	N/A		
Recovery:	The fabric alarm automatically recovers to the proper state. Its just that the fabric alarm may temporarily be cleared when it is actually not cleared yet.		

Parent Defect ID:	XCO-8267	Issue ID:	XCO-8267
Product:	XCO	Reported in Release:	XCO 3.2.1
Symptom:	Devices successfully finished their backups and took 4 minutes but the completion timeout was set to 3 minutes. Hence we observed "Config Backup timed out for Device" error message.		
Condition:	The monitor process is making rest calls to Inventory every 2 seconds to see if the backup is done yet and after 3 minutes monitor claims failure. Setting the completion timeout greater than the netconf timeout which is 4 minutes and 50 seconds, so that the monitor won't have false positive failure messages.		

Parent Defect ID:	XCO-8289	Issue ID:	XCO-8289
	XCO	Reported in Release:	XCO 3.2.1

Parent Defect ID:	XCO-8289	Issue ID:	XCO-8289
Product:			
Symptom:	After setting breakout port on 9740, the next ports are still shown in 'show-running-config'		
Condition:	On 9740 breakout of port, can see unacceptable lines in efa show-running-config (with 21 broken out, can't have 22 admin state)		

Parent Defect ID:	XCO-8366	Issue ID:	XCO-8366
Product:	XCO	Reported in Release:	XCO 3.3.1
Symptom:	IPv6-Prefix over IPv4-Peer device setting under Inventory service becomes refreshed and gets removed from the device when device is removed from fabric or entire fabric gets deleted. This setting doesn't get applied automatically to the device when it is added back to the fabric or fabric is reconfigured.		
Condition:	1. Configure fabric. 2. Enable IPv6-Prefix over IPv4-Peer device setting from inventory CLI. 3. Remove device from fabric or delete entire fabric. 4. Add device back in fabric or re-configure fabric. Performing Step 4 doesn't configure IPv6-Prefix over IPv4-Peer setting on device and Inventory service keep on identifying drift for the same.		
Recovery:	Run DRC from Inventory service before/after adding device to fabric & reconfiguring fabric		

Parent Defect ID:	XCO-8574	Issue ID:	XCO-8574
Product:	XCO	Reported in Release:	XCO 3.3.0
Symptom:	Delete/Remove route-map was successful even when bindings associated with BGP neighbor. It supposed to deny.		
Condition:	1. Create route-map stanza 2. Configure it on the device 3. Create BGP peer and peer-group with route-map binding 4. Delete the route-map with --seq all		
Workaround:	Remove BGP peer/peer-group association first and then delete/ remove the route-map from Device.		
Recovery:	Re-add the route-map to device again and then follow the workaround above for proper removal.		

Parent Defect ID:	XCO-8698	Issue ID:	XCO-8698
	XCO	Reported in Release:	EFA 2.7.2

Parent Defect ID:	XCO-8698	Issue ID:	XCO-8698
Product:			
Symptom:	Some of the anycast IP configs of existing ports-ctags of an epg have been found to be marked as 'deleted' in XCO's database. Could've been due to some sync issue that existed in 2.7 or previous images. When a port-group-add is performed on this epg with ports from new devices, the command is failed with 503 - Service available error as the tenant service gets a panic. Re-execution of same command succeeds without provisioning anycast configs in the device.		
Condition:	Data corruption: There is no mapping of anycast-ip with VE port in endpoint_group_network_properties_ip table for select VE ports (3 out of 20 to be exact). Instead, a NULL value was seen in device_id and device_port_ip_id column. This is normally done only when port-group-delete is executed, not otherwise. Root cause: there are other associated epg pord's anycast configs marked as deleted in XCO's database. This causes XCO to attempt to prepare configuration for these ports as well, as part of port-gruop-add use case. This use case has a bug in Tenant software and causes a non-fatal panic. this has cascaded to the actual issue customer faced.		
Workaround:	Not applicable		
Recovery:	Not applicable		

Parent Defect ID:	XCO-8700	Issue ID:	XCO-8700
Product:	XCO	Reported in Release:	XCO 3.3.0
Symptom:	GUI upgrade went successful, but device stuck on GUI so can't perform configuration or delete the device.		
Condition:	GUI upgrade went successful, but device stuck on GUI so can't perform configuration or delete the device.		

Parent Defect ID:	XCO-8827	Issue ID:	XCO-8827
Product:	XCO	Reported in Release:	XCO 3.2.1
Symptom:	"efa system backup --remote" failed when password length exceeds 16 chars on the remote server.		
Condition:	System backup was failing due to error in decrypting the password. Hence unable to do scp to remote host.		

Parent Defect ID:	XCO-8831	Issue ID:	XCO-8831
	XCO	Reported in Release:	XCO 3.3.0

Parent Defect ID:	XCO-8831	Issue ID:	XCO-8831
Product:			
Symptom:	XCO Visibility showing non-existent ports on 9920.		
Condition:	When looking at ports on 9920 non-existent ports shows up sometimes.		

Parent Defect ID:	XCO-8935	Issue ID:	XCO-8935
Product:	XCO	Reported in Release:	XCO 3.3.0
Symptom:	Delete/Remove route-map from Device was successful even when bindings associated with BGP neighbor. It supposed to deny.		
Condition:	1. Create route-map stanza. 2. Configure it on the device. 3. Create BGP peer and peer-group with route-map binding. 4. Update route-map with operation remove-device.		
Workaround:	Remove BGP peer/peer-group association first and then delete/ remove the route-map from Device		
Recovery:	Re-add the route-map to device again and then follow the workaround above for proper removal.		

Parent Defect ID:	XCO-8936	Issue ID:	XCO-8936
Product:	XCO	Reported in Release:	XCO 3.3.0
Symptom:	Delete or remove prefix-list from Device was successful even when bindings associated with BGP neighbor. It supposed to deny.		
Condition:	1. Create prefix-list. 2. Create route-map. 3. Create route-map-match and associate prefix created in Step 1 with route-map created in Step 2. 4. Associate/advertise prefix-list/route-map in bgp peer-group. 5. Delete or Remove Prefix-list from Device created in Step 1.		
Workaround:	Remove BGP peer/peer-group association first and then delete/ remove the prefix-list from Device.		
Recovery:	Re-add the prefix-list to device again and then follow the workaround above for proper removal.		

Parent Defect ID:	XCO-8975	Issue ID:	XCO-8975
	XCO	Reported in Release:	XCO 3.3.1

Parent Defect ID:	XCO-8975	Issue ID:	XCO-8975
Product:			
Symptom:	ICL Expansion - Fabric Event 'Link Add (LA)' Not Shown for All Switches.		
Condition:	LA should come on both device d1, d2 (or) if this is not feasible, then the PR changes solves the issue by having additional checks on fabric LA handling specific to mct devices.		

Parent Defect ID:	XCO-9323	Issue ID:	XCO-9323
Product:	XCO	Reported in Release:	XCO 3.3.0
Symptom:	GUI for Device Ports status when Group by "Name" doesn't match		
Condition:	GUI for Device Ports status when Group by "Name" doesn't match		

Defects Closed without Code Changes

The following defects are closed without code changes in ExtremeCloud Orchestrator 3.4.0.

Parent Defect ID:	XCO-5263	Issue ID:	XCO-5263
Reason Code:	Already Reported		
Product:	XCO	Reported in Release:	EFA 3.1.0
Symptom:	Failed to report telemetry not streamed from device		
Condition:	When SLX device is discovered from XCO and statistics are getting streamed using telemetry service. Device is not sending statistics using telemetry service.		
Workaround:	Select the individual device and verify the statistics are streaming from device.		

Parent Defect ID:	XCO-8072	Issue ID:	XCO-8072
Reason Code:	Insufficient Information		
Product:	XCO	Reported in Release:	XCO 3.3.0
Symptom:	When configuring an OOB QoS map of traffic-class-cos type without DP value provided on SLX, after device update, the entry showed up on EFA with DP value of 4.		
Condition:	When configuring an OOB QoS map of traffic-class-cos type without DP value provided on SLX, after device update, the entry showed up on EFA with DP value of 4.		

Parent Defect ID:	XCO-8072	Issue ID:	XCO-8072
Workaround:	No workaround for this OOB entry.		
Recovery:	Delete this OOB entry from SLX device side.		

Parent Defect ID:	XCO-8131	Issue ID:	XCO-8131
Reason Code:	Not a Software Defect		
Product:	XCO	Reported in Release:	XCO 3.2.0
Symptom:	RMA command giving the error in EFA		
Condition:	RMA command giving the error in EFA		
Workaround:	After replacing with new device use same port pairs connection which were used before replacement and also If ports are in shutdown state, bring the ports up and re-run RMA.		
Recovery:	After replacing with new device use same port pairs connection which were used before replacement and also If ports are in shutdown state, bring the ports up and re-run RMA.		

Parent Defect ID:	XCO-8403	Issue ID:	XCO-8403
Reason Code:	Already Reported		
Product:	XCO	Reported in Release:	XCO 3.2.1
Symptom:	When adding SLX devices to fabric with add-bulk it fails		
Condition:	Add SLX 8820 device(while keeping all ports admin down) to fabric using add-bulk command and see if it fails		
Workaround:	Upgrade to 3.3.0 or above to have "auto admin enable feature" support for SLX 8820 device or enable all ports admin up and the try to add to fabric using add-bulk		
Recovery:	Upgrade to 3.3.0 or above to have "auto admin enable feature" support for SLX 8820 device or enable all ports admin up and the try to add to fabric using add-bulk		

Parent Defect ID:	XCO-8423	Issue ID:	XCO-8423
Reason Code:	Not Applicable		
Product:	XCO	Reported in Release:	XCO 3.2.1
Symptom:	Disk high usage and EFA is down on standby TPVM		
Workaround:	efactl clean commands is used to clean up the disk.		
Recovery:	efactl clean commands is used to clean up the disk.		

Open Defects

There are no open defects for ExtremeCloud Orchestrator 3.4.1 and the following defects are open in ExtremeCloud Orchestrator 3.4.0.

Parent Defect ID:	XCO-3445	Issue ID:	XCO-3445
Product:	XCO	Reported in Release:	EFA 3.0.0
Symptom:	DRC will not identify the drift and hence will not reconcile the drifted configuration		
Condition:	Below are the steps to reproduce the issue: 1. Configure multi rack Non-CLOS fabric. 2. Manually remove the below set of configurations on device under: router-bgp no neighbor 172.x.x.x password xxxx no neighbor 172.x.x.x update-source loopback 1 no neighbor 172.x.x.x peer-group overlay-ebgp-group address-family l2vpn evpn no retain route-target all 3. Run "efa inventory drift-reconcile execute --ip <device-ip>"		
Recovery:	Manually reconfigure the removed configurations from the device		

Parent Defect ID:	XCO-3471	Issue ID:	XCO-3471
Product:	XCO	Reported in Release:	EFA 3.1.0
Symptom:	Stale BGP Peer-group entry configured under router BGP on SLX Border leaf and Spine devices with none of the BGP neighbors linked with the Peer group.		

Parent Defect ID:	XCO-3471	Issue ID:	XCO-3471
Condition:	1. Create a 3-stage CLOS fabric, add devices with MCT leaf, spine, and border-leaf and configure the fabric. 2. Convert the 3-stage CLOS fabric to a 5-stage CLOS fabric using the fabric migrate command. "efa fabric migrate --type "3-to-5-stage" --source-fabric <source-fabric> --destination-3-stage-leaf-spine-pod <pod-name> --destination-3-stage-border-leaf-pod <pod-name>" 3. Add super-spine POD devices to the migrated 5-stage CLOS fabric. 4. Disconnect the BorderLeaf to Spine links and reconnect the BorderLeaf to Super-Spine links. 5. Configure the migrated 5-stage CLOS fabric.		
Recovery:	Manually delete the stale BGP peer-groups from both the Border Leaf and Spine devices		

Parent Defect ID:	XCO-4128	Issue ID:	XCO-4128
Product:	XCO	Reported in Release:	EFA 3.0.0
Symptom:	Port-channel partial configuration are present on device for SLX NPB devices		
Condition:	Port-channel configuration failed from UI, on device still the partial configuration is present.		
Workaround:	Make sure that all the configuration information are correctly populated from UI so that configuration will not fail on device.		
Recovery:	Login to SLX CLI and delete the given port channel and click on refresh configuration on XCO UI from device action list.		

Parent Defect ID:	XCO-4129	Issue ID:	XCO-4129
Product:	XCO	Reported in Release:	EFA 3.0.0
Symptom:	Disable of vn-tag header strip and enabling of 802.1BR header strip fails from XCO GUI for SLX NPB		
Condition:	When vn-tag header strip is enabled on an interface, disabling the vn-tag header strip and enabling the 802.1BR header strip in a single operation fails from XCO GUI.		

Parent Defect ID:	XCO-4129	Issue ID:	XCO-4129
Workaround:	Disable the vn-tag header strip in first operation (save the port update) and then edit port again for enabling 802.1BR header strip option.		
Recovery:	N/A		

Parent Defect ID:	XCO-6964	Issue ID:	XCO-6964
Product:	XCO	Reported in Release:	XCO 3.2.0
Symptom:	Upgrade was successful but a Failed message appears at the end of upgrade.. message is "Status: Failed"		
Condition:	Upgrade XCO with latest build. Issue is seen only on customer setup.		

Parent Defect ID:	XCO-7100	Issue ID:	XCO-7100
Product:	XCO	Reported in Release:	XCO 3.2.0
Symptom:	"Target TPVM Version" Does not display until new TPVM is already installed.		
Condition:	During the TPVM upgrade, "Target TPVM Version" gets updated late in the workflow.		
Recovery:	The correct Target TPVM version gets updated after the new version is installed.		

Parent Defect ID:	XCO-8191	Issue ID:	XCO-8191
Product:	XCO	Reported in Release:	XCO 3.3.0
Symptom:	If you run concurrent epg update commands operation as port-group-add or vrf-add on bridge-domain EPGs that are associated with more than one ctag, one or some of the commands may fail with error "Save for device failed".		
Condition:	This is observed more often when more than 3 concurrent EPG port-group-add commands with non-conflicting ports and non-overlapping ctag-range are executed. Occasionally, configuration information that is pushed by one command is not used properly to prepare command recipe for another, causing the failure of one command.		

Parent Defect ID:	XCO-8191	Issue ID:	XCO-8191
Workaround:	Rerunning the failing command will succeed. The error is intermittent and does not cause permanent changes. XCO state information is not affected at any point.		
Recovery:	No recovery is required as no state change is done as part of this failure.		

Parent Defect ID:	XCO-8550	Issue ID:	XCO-8550
Product:	XCO	Reported in Release:	XCO 3.3.0
Symptom:	IPV6 deployment failing with default GW errors even IPv6 XCO server can reach to default Gateway.		
Condition:	IPv6 deployment is failed in below condition. Failed condition- default proto static metric 1024 nexthop via 2600:3c01:e000:e2::2 dev eth0 weight 1 expecting the below pattern - fe80::/64 dev veth0a9acd23 proto kernel metric 256 pref medium default via 2620:100:c:e085:20c:29ff:fee1:3ec1 dev ens160 metric 1024 pref medium		
Workaround:	User has to add the default route using below command- sudo ip -6 route add default via <IPv6 address of default gw> dev <exit interface> example: sudo ip -6 route add default via fc00::5:204:96ff:fed6:f288 dev eth0		

Parent Defect ID:	XCO-8735	Issue ID:	XCO-8735
Product:	XCO	Reported in Release:	XCO 3.3.0
Symptom:	Inventory and device page showing different firmware version.		
Condition:	Post firmware upgrade, Inventory and device page showing different firmware version.		
Workaround:	Post device discovery, device page shows correct firmware ware version.		

Parent Defect ID:	XCO-8829	Issue ID:	XCO-8829
Product:	XCO	Reported in Release:	XCO 3.2.1
Symptom:	New firmware-host registry fails when single quote is used in the password.		

Parent Defect ID:	XCO-8829	Issue ID:	XCO-8829
Condition:	Single quote is used in the password.		
Workaround:	Use the password with no single quote.		

Parent Defect ID:	XCO-9137	Issue ID:	XCO-9137
Product:	XCO	Reported in Release:	XCO 3.3.0
Symptom:	EFA upgrade from release 2.7.2 to 3.3.0		
Condition:	When DNS was removed before upgrade.		
Workaround:	DNS configuration should not be changed between upgrades.		
Recovery:	If DNS config removed, after upgrade to EFA 3.3.0 use update_dns.sh script to disallow DNS using following steps: 1. Bash update-dns.sh --dns-action disallow. 2. Get the coredns pod name using k3s kubectl get pods -n kube-system. 3. Restart Coredns pod using k3s kubectl delete pod <coredns pod name> -n kube-system. 4. Wait for few mins or Restart All efa pods using: sudo efactl stop. sudo efactl start.		

Parent Defect ID:	XCO-9178	Issue ID:	XCO-9178
Product:	XCO	Reported in Release:	XCO 3.4.0
Symptom:	When a device is removed from fabric which has QoS configuration, not all QoS configuration is removed from the device and EFA.		
Condition:	Device is deleted from fabric		
Workaround:	User needs to unbind the policies (QoS) from all the relevant targets (fabric/tenant/port/po) before executing the fabric device delete to avoid the stale policies(QoS) in the system.		

Parent Defect ID:	XCO-9190	Issue ID:	XCO-9190
	XCO	Reported in Release:	XCO 3.3.0

Parent Defect ID:	XCO-9190	Issue ID:	XCO-9190
Product:			
Symptom:	VM GUI Library matches shows 2 devices when only 1 device discovered.		
Condition:	Remove all the devices and discover only one device.		

Parent Defect ID:	XCO-9195	Issue ID:	XCO-9195
Product:	XCO	Reported in Release:	XCO 3.3.0
Symptom:	XCO3.3 VM GUI won't allow library copy for matches.		
Condition:	Go to Library page using XCO GUI and try to make a copy using edit option.		

Parent Defect ID:	XCO-9217	Issue ID:	XCO-9217
Product:	XCO	Reported in Release:	XCO 3.3.0
Symptom:	CLI for **`efactl restart`** throwing retrying and failed messages on customer setup only.		
Condition:	Run the CLI **`efactl restart`** command on GTAC setup and user can see the failed pop-up trace even those pods restart completed successfully.		

Parent Defect ID:	XCO-9224	Issue ID:	XCO-9224
Product:	XCO	Reported in Release:	XCO 3.4.0
Symptom:	QoS application is not taking place after changing interface switch port modes or changing the interface from L2 to L3 or vice-a-versa through OOB (out of band) means.		
Condition:	Modifying the switchport mode followed by executing auto DRC.		
Recovery:	Remove all OOB Interface configuration and restore the configuration to the original EFA configured values and re-run DRC.		

Parent Defect ID:	XCO-9270	Issue ID:	XCO-9270
Product:	XCO	Reported in Release:	XCO 3.3.1
Symptom:	Standby node showing 'down' after node reboot		

Parent Defect ID:	XCO-9270	Issue ID:	XCO-9270
Condition:	Trigger SLX reload using below command where the active XCO node is running and check the node status after reboot (when it becomes standby) echo c >/proc/sysrq-trigger		
Recovery:	Reboot both active and standby nodes to recover from the situation		

Parent Defect ID:	XCO-9284	Issue ID:	XCO-9284
Product:	XCO	Reported in Release:	XCO 3.4.0
Symptom:	Copy default-config to startup-config with maintenance mode enabled will remove all config including QoS policies on a device. Further running DRC does not properly re-install all QoS configuration.		
Recovery:	Remove the device from inventory then register the device back.		

Parent Defect ID:	XCO-9291	Issue ID:	XCO-9291
Product:	XCO	Reported in Release:	XCO 3.4.0
Symptom:	The fabric internal ports QoS profile is not getting applied on fabric internal ports when Leaf devices are converted from single-homed to multi-homed by adding new Leaf device.		
Condition:	The fabric internal ports QoS profile is not getting applied on fabric internal ports when Leaf devices are converted from single-homed to multi-homed by adding new Leaf device.		
Workaround:	User can issue unbind of fabric internal port QoS profile and rebind the fabric internal port QoS profile using below commands. Unbind Fabric internal ports QoS profile: efa policy qos profile unbind --name <profile_name> --fabric <fabric_name> --port fabric-internal Bind Fabric internal ports QoS profile: efa policy qos profile bind --name <profile_name> --fabric <fabric_name> --port fabric-internal		
Recovery:	User can issue unbind of fabric internal port QoS profile and rebind the fabric internal port QoS profile using below commands. Unbind Fabric internal ports QoS profile: efa policy qos profile unbind --name <profile_name> --fabric <fabric_name> --port fabric-internal Bind Fabric internal ports QoS profile: efa policy qos profile bind --name <profile_name> --fabric <fabric_name> --port fabric-internal		

Parent Defect ID:	XCO-9331	Issue ID:	XCO-9331
	XCO	Reported in Release:	XCO 3.4.0

Parent Defect ID:	XCO-9331	Issue ID:	XCO-9331
Product:			
Symptom:	If a tenant interface level qos profile binding exist on a port channel and the port channel is removed from the device via OOB (Out Of Band) triggering DRC will not re-install the Tenant level interface binding.		
Condition:	Removing a Port Channel from a device via OOB (Out of Band) and triggering DRC.		
Workaround:	Once the port channel is restored by the DRC process on the device the user will need to re-apply/rebind the desired QoS profile on the tenant interface (port channel) using efa policy qos profile bind --name <profile_name> --tenant <tenant_name> --po <port channel ID>		
Recovery:	Once the port channel is restored by the DRC process on the device the user will need to re-apply/rebind the desired QoS profile on the tenant interface (port channel) using efa policy qos profile bind --name <profile_name> --tenant <tenant_name> --po <port channel ID>		

Parent Defect ID:	XCO-9336	Issue ID:	XCO-9336
Product:	XCO	Reported in Release:	XCO 3.4.0
Symptom:	Inventory device delete is not removing qos config on the spine device		
Condition:	Device deletion from inventory which has QoS configuration		
Workaround:	User needs to unbind the policies (QoS) from all the relevant targets (fabric/tenant/port/po) before running the inventory device delete.		
Recovery:	User needs to unbind the policies (QoS) from all the relevant targets (fabric/tenant/port/po). After this user needs to delete the leftover QoS configuration from SLX.		

Parent Defect ID:	XCO-9341	Issue ID:	XCO-9341
Product:	XCO	Reported in Release:	XCO 3.2.1
Symptom:	App state for one of the border leaf shows 'cfg-refresh-error'.		

Parent Defect ID:	XCO-9341	Issue ID:	XCO-9341
Condition:	Due to some reason if mariadb restarts on active XCO node, "Error : dial tcp <xco-ip>:3306: connect: connection refused; invalid transaction; invalid transaction" is seen for 'efa fabric show' command. After db connection is successful, the app state for one of the border leaf shows 'cfg-refresh-error'.		
Recovery:	To update the app-state for the device, the below recovery steps can be followed: 1. On SLX: shut MCT ports. 2. On XCO: efa inventory device update –ip <device-ip>. 3. On SLX:, no shut MCT ports. 4. On XCO: efa inventory device update –ip <device-ip>.		

Parent Defect ID:	XCO-9354	Issue ID:	XCO-9354
Product:	XCO	Reported in Release:	XCO 3.3.1
Symptom:	Threshold monitor configuration for monitor types(lif, bfd-session, vxlan-tunnel, mac-table) failed when we configure thru XCO to SLX device(starting from SLX version - 20.5.3).		
Condition:	Use XCO 3.3.1 and SLX version 20.5.3 and try the following cases: 1. Set monitor threshold for lif, bfd-session, vxlan-tunnel, mac-table thru XCO failed only when we use count/interval fields. 2. Unset monitor threshold for lif, bfd-session, vxlan-tunnel, mac-table thru XCO failed. Here Unset logic tries to clear all fields including count/interval fields by default.		
Workaround:	1. Set monitor threshold for types lif, bfd-session, vxlan-tunnel, & mac-table thru XCO without count/interval fields. 2. Unset can't be done by XCO. Instead it can be unset directly in SLX using the following commands: no threshold-monitor <monitor-type> Or use XCO 3.3.1 with SLX version 20.5.2a for functioning without any issue.		

Parent Defect ID:	XCO-9362	Issue ID:	XCO-9362
Product:	XCO	Reported in Release:	XCO 3.4.0
Symptom:	The fabric internal ports QoS profile is not getting applied on intended ports: 1) When a new device is being added to CLOS fabric and fabric is configured. 2) When a new rack is added to non-CLOS fabric and fabric is configured.		

Parent Defect ID:	XCO-9362	Issue ID:	XCO-9362
Condition:	Pre-condition: Fabric internal ports QoS profile is already applied on a fabric (CLOS or non-CLOS). Issue will be seen: 1) When a new device is being added to CLOS fabric and fabric is configured. 2) When a new rack is added to non-CLOS fabric and fabric is configured		
Workaround:	User can issue unbind of fabric internal port QoS profile and rebind the fabric internal port QoS profile using below commands. Unbind Fabric internal QoS profile: efa policy qos profile unbind --name <profile_name> --fabric <fabric_name> --port fabric-internal Bind Fabric internal QoS profile: efa policy qos profile bind --name <profile_name> --fabric <fabric_name> --port fabric-internal		
Recovery:	User can issue unbind of fabric internal port QoS profile and rebind the fabric internal port QoS profile using below commands. Unbind Fabric internal QoS profile: efa policy qos profile unbind --name <profile_name> --fabric <fabric_name> --port fabric-internal Bind Fabric internal QoS profile: efa policy qos profile bind --name <profile_name> --fabric <fabric_name> --port fabric-internal		

Parent Defect ID:	XCO-9363	Issue ID:	XCO-9363
Product:	XCO	Reported in Release:	XCO 3.4.0
Symptom:	Tenant and Tenant Interface QoS policy information is not fully removed from EFA DB and SLX device when the tenant delete with --force option is specified.		
Condition:	Issue is observed when user issues the command 'efa tenant delete --name <tenant_name> --force'		
Workaround:	This is covered in the targeted Generic Release notes (item) User needs to unbind the policies (QoS) from all the relevant targets (fabric/tenant/port/port channel/tenant endpoint group) before executing the force operations including delete to avoid the stale policies(QoS) in the system.		

Parent Defect ID:	XCO-9381	Issue ID:	XCO-9381
Product:	XCO	Reported in Release:	EFA 2.7.2
Symptom:	9740 devices with breakout port configured, DRC fails for even numbered port.		

Parent Defect ID:	XCO-9381	Issue ID:	XCO-9381
Condition:	If XCO is upgraded from previous version to 3.2.0 version.		
Workaround:	Perform fresh install followed by reconfiguration of breakout ports and its respective configuration.		

Help and Support

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: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2800. 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 Product Announcements

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

1. Go to The Hub.
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.

4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

You can modify your product selections or unsubscribe at any time.