



# ExtremeCloud™ Orchestrator Release Notes

3.2.0

9037731-00 Rev AB  
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/company/legal/trademarks](http://www.extremenetworks.com/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

---

<b>Release Notes.....</b>	<b>4</b>
New In This Release.....	4
Evolution of EFA and XVM into XCO.....	4
Supported Platforms and Deployment Models for Fabric Skill.....	9
Supported Platforms and Deployment Models for Visibility Skill.....	12
XCO Upgrade Prerequisites.....	13
Known Limitations.....	13
Known Limitations in Fabric Skill.....	13
Known Limitations in Visibility Skill.....	16
Defects Closed with Code Changes .....	17
Defects Closed without Code Changes.....	28
Open Defects.....	33
Help and Support.....	44
Subscribe to Product Announcements.....	44



# Release Notes

---

- [New In This Release](#) on page 4
- [Supported Platforms and Deployment Models for Fabric Skill](#) on page 9
- [Supported Platforms and Deployment Models for Visibility Skill](#) on page 12
- [XCO Upgrade Prerequisites](#) on page 13
- [Known Limitations](#) on page 13
- [Defects Closed with Code Changes](#) on page 17
- [Defects Closed without Code Changes](#) on page 28
- [Open Defects](#) on page 33
- [Help and Support](#) on page 44

## New In This Release

---

ExtremeCloud Orchestrator 3.2.0 provides the following features and improvements. For information about XCO deployment, refer to the [ExtremeCloud Orchestrator Deployment Guide, 3.2.0](#).

## Evolution of EFA and XVM into XCO



### Note

From release 3.2.0 onwards, 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.

ExtremeCloud™ Orchestrator is a comprehensive microservice based, cloud-native solution that provides organizations the ability to visualize at a workspace level using the user interface or shift to the orchestration level to integrate and automate the network infrastructure through APIs.

XCO integrates Extreme Fabric Automation (EFA) and Extreme Visibility Manager (XVM) solutions:

- EFA: Automates life-cycle management that includes design, deployment, operation, and refresh of IP fabric networks.
- XVM: Manages network packet broker (NPB) and visibility solution.

For more information, refer to the [ExtremeCloud Orchestrator CLI Administration Guide, 3.2.0](#).

**Table 1: Features and improvements**

Feature	Description
Certificate Management enhancement Part 3	<p>Procedure to update the password of a new user in XCO.</p> <p>Update to third-party certificates</p> <p>Host Authentication certificates running on port 8079</p> <p>Update to the renewal script</p> <p>For more information, refer to the <a href="#">ExtremeCloud Orchestrator CLI Administration Guide, 3.2.0</a>.</p>
BUM traffic Local bias support for LVTEP	<p>Procedure to configure hardware profile to limit the IPv6 prefix to 64.</p> <p>For more information, refer to the <a href="#">ExtremeCloud Orchestrator CLI Administration Guide, 3.2.0</a>.</p>
Log files customization support	<p>Procedure to configure or unconfigure and customize log files to fit system resources.</p> <p>For more information, refer to the <a href="#">ExtremeCloud Orchestrator CLI Administration Guide, 3.2.0</a>.</p>
Tenant : EPG : Network : ICMP Redirect Enable or Disable	<p>Procedure to configure ICMP Redirect Enable or Disable.</p> <p>For more information, refer to the <a href="#">ExtremeCloud Orchestrator CLI Administration Guide, 3.2.0</a>.</p> <p>For SLX platform support information, refer to SLX-OS documentation.</p>
XCO log streaming and filtering	<p>Additional filtering capability for logging streams, notification terminology, additional notification filtering, and sub-filter commands.</p> <p>For more information, refer to the <a href="#">ExtremeCloud Orchestrator CLI Administration Guide, 3.2.0</a>.</p>
Pure IPv6 Support	<p>Updated the topic with dual IP mode supported northbound CLIs content.</p> <p>For more information, refer to the <a href="#">ExtremeCloud Orchestrator CLI Administration Guide, 3.2.0</a>.</p> <hr/> <p>Use only IPv6 address to configure on the node interfaces when deploying XCO.</p> <p>For more information, refer to the <a href="#">ExtremeCloud Orchestrator Deployment Guide, 3.2.0</a>.</p>

**Table 1: Features and improvements (continued)**

Feature	Description
Configuration for IPv6 prefixes restricted to 64	New information on backup and restore content for IPv6 support. For more information, refer to the <a href="#">ExtremeCloud Orchestrator CLI Administration Guide, 3.2.0</a> .
	Procedure to configure hardware profile to limit the IPv6 prefix to 64. For more information, refer to the <a href="#">ExtremeCloud Orchestrator CLI Administration Guide, 3.2.0</a> .
Infra and deployment enhancements	Support for accessing supportsave without logging in to XCO. For more information, refer to the <a href="#">ExtremeCloud Orchestrator CLI Administration Guide, 3.2.0</a> .
	Use of auto-reboot options for TPVM incremental upgrade. For more information, refer to the <a href="#">ExtremeCloud Orchestrator Deployment Guide, 3.2.0</a> .
	Changes to OVA root user login. For more information, refer to the <a href="#">ExtremeCloud Orchestrator Deployment Guide, 3.2.0</a> .
Inventory and Fabric Service enhancements	Update to Fabric Settings in Active Fabric: Small Data Center Fabric and Fabric Settings in Active Fabric: Clos Fabric tables for BGP multihop. Update to procedure on BGP multihop on an active fabric, fabric configuration using force option, and Linux exit codes. For more information, refer to the <a href="#">ExtremeCloud Orchestrator CLI Administration Guide, 3.2.0</a> .
BGP ADD-PATH	Procedure to configure additional paths on Tenant BGP peer and BGP peer group. For more information, refer to the <a href="#">ExtremeCloud Orchestrator CLI Administration Guide, 3.2.0</a> .
Health Support for Fabric Service	Fabric and device health status with sample output. For more information, refer to the <a href="#">ExtremeCloud Orchestrator CLI Administration Guide, 3.2.0</a> .

**Table 1: Features and improvements (continued)**

Feature	Description
XCO Alarm Management	Information on XCO alarms, alarm inventory, status change notifications, and alarm commands. For more information, refer to the <a href="#">ExtremeCloud Orchestrator CLI Administration Guide, 3.2.0</a> .
Evolution of EFA and XVM to XCO	Information on evolution of EFA and XVM to XCO, support and integration information, and XCO architecture. For more information, refer to the <a href="#">ExtremeCloud Orchestrator CLI Administration Guide, 3.2.0</a> .
Additional external authentication option	Information on another external XCO user authentication option. For more information, refer to the <a href="#">ExtremeCloud Orchestrator Security Guide, 3.2.0</a> .
API update for XCO user roles	API update for assigning XCO user roles. For more information, refer to the <a href="#">ExtremeCloud Orchestrator Security Guide, 3.2.0</a> .
System hardening for CIS-CAT assessments	Improvements to system hardening information. For more information, refer to the <a href="#">ExtremeCloud Orchestrator Security Guide, 3.2.0</a> .
Common landing page	The dashboard or the common landing page provides an overview of system health. For more information, refer to the <a href="#">ExtremeCloud Orchestrator GUI Administration Guide, 3.2.0</a> .
Fabric management	ExtremeCloud Orchestrator automates and orchestrates SLX IP fabrics through CLI and user interface. For more information, refer to the <a href="#">ExtremeCloud Orchestrator GUI Administration Guide, 3.2.0</a> .
Network essential configurations	ExtremeCloud Orchestrator supports network essential configurations that are required for creating and configuring fabric networks. For more information, refer to the <a href="#">ExtremeCloud Orchestrator GUI Administration Guide, 3.2.0</a> .

**Table 1: Features and improvements (continued)**

Feature	Description
Support Save	ExtremeCloud Orchestrator supports support save logs collection for troubleshooting. For more information, refer to the <a href="#">ExtremeCloud Orchestrator GUI Administration Guide, 3.2.0</a> .
Bulk device inventory download	ExtremeCloud Orchestrator supports downloading of bulk device inventory. For more information, refer to the <a href="#">ExtremeCloud Orchestrator GUI Administration Guide, 3.2.0</a> .
SLX optical statistics	ExtremeCloud Orchestrator supports optical statistics for SLX devices. For more information, refer to the <a href="#">ExtremeCloud Orchestrator GUI Administration Guide, 3.2.0</a> .
User management enhancements	ExtremeCloud Orchestrator supports user management enhancements such as add and edit host user. For more information, refer to the <a href="#">ExtremeCloud Orchestrator GUI Administration Guide, 3.2.0</a> .
Role Based Access Control (RBAC)	Role Based Access Control (RBAC) defines the capabilities that a user account has based on the assigned role. For more information, refer to the <a href="#">ExtremeCloud Orchestrator GUI Administration Guide, 3.2.0</a> .

For more information, see [Defects Closed with Code Changes](#) on page 17.



## 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

As a best practice, refer to the following Extreme validated support matrices for support platforms and deployment models information.

**Table 2: Server Deployment Models**

XCO Version	Managed SLX Devices	Multi-Fabric Support	Ubuntu Server Version	Virtual Machine
2.7.x, 3.0.0	More than 24	Yes	16.04, 18.04	<ul style="list-style-type: none"> <li>CPU: 4 cores</li> <li>Storage: 64 GB</li> <li>RAM: 8 GB</li> </ul>
3.1.x	More than 24	Yes	16.04, 18.04, and 20.04	<ul style="list-style-type: none"> <li>CPU: 4 cores</li> <li>Storage: 64 GB</li> <li>RAM: 8 GB</li> </ul>
3.2.0	More than 24	Yes	18.04 and 20.04	<ul style="list-style-type: none"> <li>CPU: 4 cores</li> <li>Storage: 64 GB</li> <li>RAM: 8 GB</li> </ul>

**Table 3: OVA Deployment Models**

XCO Version	Managed SLX Devices	Multi-Fabric Support	Ubuntu Version	Virtual Machine
2.7.x, 3.0.0, and 3.1.x	More than 24	Yes	18.04	<ul style="list-style-type: none"> <li>CPU: 4 cores</li> <li>Storage: 64 GB</li> <li>RAM: 8 GB</li> </ul>
3.2.0	More than 24	Yes	18.04	<ul style="list-style-type: none"> <li>CPU: 4 cores</li> <li>Storage: 64 GB</li> <li>RAM: 8 GB</li> </ul>

**Table 4: TPVM Deployment Models**

XCO Version	TPVM Deployment	Managed SLX Devices	Multi-Fabric Support	Ubuntu Version	Minimum SLX-OS Version
2.7.x	<ul style="list-style-type: none"> <li>SLX 9150</li> <li>SLX 9250</li> <li>SLX 9740</li> </ul>	Up to 24	Yes	18.04	20.4.1

**Table 4: TPVM Deployment Models (continued)**

XCO Version	TPVM Deployment	Managed SLX Devices	Multi-Fabric Support	Ubuntu Version	Minimum SLX-OS Version
	<ul style="list-style-type: none"> <li>Extreme 8520</li> <li>Extreme 8720</li> </ul>				
3.0.x	<ul style="list-style-type: none"> <li>SLX 9150</li> <li>SLX 9250</li> <li>SLX 9740</li> <li>Extreme 8520</li> <li>Extreme 8720</li> </ul>	Up to 24	Yes	18.04	20.4.2
3.1.x	<ul style="list-style-type: none"> <li>SLX 9150</li> <li>SLX 9250</li> <li>SLX 9740</li> <li>Extreme 8520</li> <li>Extreme 8720</li> <li>Extreme 8820 (20.4.3 onwards only)</li> </ul>	Up to 24	Yes	18.04	20.4.2
3.2.0	<ul style="list-style-type: none"> <li>SLX 9150</li> <li>SLX 9250</li> <li>SLX 9740</li> <li>Extreme 8520</li> <li>Extreme 8720</li> <li>Extreme 8820 (20.4.3 onwards only)</li> </ul>	Up to 24	Yes	18.04	20.4.3

**Table 5: TPVM Software Support**

XCO Version	TPVM Version	SLX-OS Version
2.5.4	4.3.0	20.3.2d
2.5.5		
2.6.0	4.4.0	20.3.4/4a
2.6.1		
2.7.0	4.5.0	20.4.1
2.7.2	4.5.1	20.4.1b
3.0.0	4.5.3	20.4.2
3.1.0	4.5.6	20.4.2a

**Table 5: TPVM Software Support (continued)**

XCO Version	TPVM Version	SLX-OS Version
3.1.1	4.5.8	20.4.3
3.2.0	4.5.10	20.4.3a

**Table 6: 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				✓	
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 7: 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 names. 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 8: Ubuntu Server Version**

XCO Version	Ubuntu Version	Virtual Machine
3.1.x	18.04 and 20.04	Minimum: <ul style="list-style-type: none"><li>• CPU: 4 cores</li><li>• Storage: 128 GB</li><li>• RAM: 8 GB</li></ul> Recommended: <ul style="list-style-type: none"><li>• CPU: 16 cores</li><li>• Storage: 200 GB</li><li>• RAM: 32 GB</li></ul>
3.2.0	18.04 and 20.04	Minimum: <ul style="list-style-type: none"><li>• CPU: 4 cores</li><li>• Storage: 128 GB</li><li>• RAM: 8 GB</li></ul> Recommended: <ul style="list-style-type: none"><li>• CPU: 16 cores</li><li>• Storage: 200 GB</li><li>• RAM: 32 GB</li></ul>

**Table 9: OVA Deployment Models**

XCO Version	Ubuntu Version	Virtual Machine
3.1.x	18.04	Minimum: <ul style="list-style-type: none"><li>• CPU: 4 cores</li><li>• Storage: 64 GB</li><li>• RAM: 8 GB</li></ul>
3.2.0	18.04	Minimum: <ul style="list-style-type: none"><li>• CPU: 4 cores</li><li>• Storage: 64 GB</li></ul>

**Table 9: OVA Deployment Models (continued)**

XCO Version	Ubuntu Version	Virtual Machine
		<ul style="list-style-type: none"> <li>RAM: 8 GB</li> </ul>

**Table 10: Supported Devices and Software**

Device	Supported Software
Extreme 9920	Extreme 9920 software with the NPB application <ul style="list-style-type: none"> <li>21.1.2.x</li> </ul>
Extreme Routing MLX Series	<ul style="list-style-type: none"> <li>NetIron 6.3.00 patches</li> </ul>
Extreme Switching SLX 9140	<ul style="list-style-type: none"> <li>SLX-OS 18s.1.03 patches</li> </ul>
Extreme Switching SLX 9240	<ul style="list-style-type: none"> <li>SLX-OS 18s.1.03 patches</li> </ul>

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

## Known Limitations in Fabric Skill

Follow these caveats and limitations when using Fabric Skill.

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

Symptom	Condition	Workaround
Endpoint group (EPG) update <b>vrf-add</b> operation fails with the reason as VRF to be added has conflicting VRF on the switch.	Run EPG update <b>vrf-add</b> , <b>vrf-delete</b> , and <b>vrf-add</b> operation CLI in quick succession: <ol style="list-style-type: none"> <li>1. Update EPG for operation <b>vrf-add</b>.</li> <li>2. Update EPG for operation <b>vrf-delete</b>.</li> <li>3. Update the same EPG again with operation <b>vrf-add</b> for the same VRF which was deleted in step 2.</li> </ol>	Wait of 30 seconds between the EPG update <b>vrf-add</b> 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.	The status are not set for all the REST operations AFTER publishing all the necessary events on the message bus.	For all the REST operations, set the status AFTER publishing all the necessary events on the message bus.

RBAC: XCO shows "export EFA\_TOKEN" command suggestion when a tenant user logs in

Symptom	Condition	Workaround
<p>XCO shows the following message after a tenant user with RBAC logs in to the system: Please type this in your shell:</p> <pre> <b>export</b> <b>EFA_TOKEN</b>=eyJhbGciOiJSUzI1NiIsImtpZCI6IjEuMCIsInR5cCI6IkpXVCJ9.eyJjb2l0b25lbnR5cCI6IjE6IiwidWFzIjpbeyJ0YXJzZXQiOiJFRkeiLCJyb2x1IjoieVlIyLVRudE</pre>	<p>When a user is created with the default login shell as sh.</p>	<p>XCO supports only bash shell for login or any other CLI commands.</p>

*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 <b>efa tenant show</b> 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 Administration Guide, 3.2.0](#).

*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 Administration Guide, 3.2.0](#).

*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 resolved in ExtremeCloud Orchestrator 3.2.0.

<b>Parent Defect ID:</b>	XCO-3435	<b>Issue ID:</b>	XCO-3435
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 2.5.0
<b>Symptom:</b>	Add Device Failed because ASN used in border leaf showing conflict		
<b>Condition:</b>	If there are more than one pair of Leaf/border leaf devices then devices which are getting added first will get the first available ASN in ascending order and in subsequent addition of devices if one of device is trying to allocate the same ASN because of brownfield scenario then EFA will throw an error of conflicting ASN		
<b>Workaround:</b>	Add the devices to fabric in the following sequence 1)First add devices that have preconfigured configs 2)Add remaining devices that don't have any configs stored		
<b>Recovery:</b>	Removing the devices and adding the devices again to fabric in following sequence 1)First add devices that have preconfigured configs 2)Add remaining unconfigured devices.		

<b>Parent Defect ID:</b>	XCO-3459	<b>Issue ID:</b>	XCO-3459
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 2.7.0
<b>Symptom:</b>	After EFA installation, when the date on the host is moved back in time, the certificate renewal process doesn't complete and EFA doesn't work even after restoring the date back.		

<b>Parent Defect ID:</b>	XCO-3460	<b>Issue ID:</b>	XCO-3460
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 2.5.5
<b>Symptom:</b>	kubernetes command <code>k3s kubectl get pods -n efa</code> will show some pods in "ImagePullBackOff" state.		
<b>Condition:</b>	when node Disk Space is full and pods are in evicted state, after freeing up space and executing <code>efactl start</code> or on next restart of pod.		

<b>Parent Defect ID:</b>	XCO-3460	<b>Issue ID:</b>	XCO-3460
<b>Workaround:</b>	Check for expected Disk space as mentioned in system requirements.		
<b>Recovery:</b>	<ol style="list-style-type: none"> <li>1. Check if we have enough disk space as mentioned in system requirements,</li> <li>2. On the install dir , change to docker_images and import the images using following command k3s ctr image import docker_k3s_images.tar</li> <li>3. execute efactl start</li> </ol>		

<b>Parent Defect ID:</b>	XCO-3478	<b>Issue ID:</b>	XCO-3478
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 2.7.2
<b>Symptom:</b>	passwords for users extreme and efainternal are set to never expire.		

<b>Parent Defect ID:</b>	XCO-3479	<b>Issue ID:</b>	XCO-3479
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.1.0
<b>Symptom:</b>	EFA health status is not turning to green if the device is removed from inventory and the device had previously generated alerts.		
<b>Condition:</b>	Removing the device from inventory		
<b>Workaround:</b>	<p>There are two workarounds:</p> <ol style="list-style-type: none"> <li>1. Remove the health.gob following the below steps sudo systemctl stop monitor sudo systemctl status monitor sudo rm /apps/efadata/misc/health.gob sudo systemctl start monitor</li> <li>2. Add the device back</li> </ol>		
<b>Recovery:</b>	The health status can be changed to green by following the steps mentioned in workaround.		

<b>Parent Defect ID:</b>	XCO-3968	<b>Issue ID:</b>	XCO-3968
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 2.4.2
<b>Symptom:</b>	Single node deployment fails with 'DNS resolution failed.'		

<b>Parent Defect ID:</b>	XCO-3968	<b>Issue ID:</b>	XCO-3968
<b>Condition:</b>	After a multi-node deployment and then un-deployment is done on a server, if single-node deployment is tried on the same server, the installer exits with the error, 'DNS resolution failed.'		
<b>Workaround:</b>	After un-deployment of the multi-node installation, perform a reboot of the server/TPVM.		

<b>Parent Defect ID:</b>	XCO-4136	<b>Issue ID:</b>	XCO-4136
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.1.0
<b>Symptom:</b>	The intermediate session expired popup in the XCO user interface		
<b>Condition:</b>	When the user session is active for one hour, the user will see a session expiry popup.		
<b>Workaround:</b>	Set the higher value for the user token expiry using "efa auth settings token update" CLI. The default access token expiry value is 1 hour. Example: efa auth settings token update --type=ACCESS --hours=2 --minutes=30		
<b>Recovery:</b>	The user has to click OK on the popup and the user session will be reauthenticated automatically.		

<b>Parent Defect ID:</b>	XCO-4147	<b>Issue ID:</b>	XCO-4147
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.1.0
<b>Symptom:</b>	The Bridge domain will show the pw-profile as default rather than the actual value 'Tenant-profile'. This is even after the DRC and the EFA will show bridge domain configurations as drifted.		
<b>Condition:</b>	<p>On BR-SLX9540, BR-SLX9640, SLX9740-40C, SLX9740-80C</p> <ol style="list-style-type: none"> <li>1. Configure a fabric and create a BD based tenant, vrf and Port channel under the tenant</li> <li>2. Configure L3 EPG under the BD based tenant using the vrf and Port channel created in step 1.</li> <li>3. Step 2 will result in 'Tenant-profile' pw-profile configuration under the Bridge domain corresponding to the Tenant ctag.</li> <li>4. Delete the port channel which has the associated LIF to the BD (discussed in step 3) on the switch.</li> </ol> <p>OR</p> <p>Delete the LIF present in the Port channel or Ethernet Port that is associated with the BD (discussed in step 3) on the switch.</p> <ol style="list-style-type: none"> <li>5. Execute the DRC for the switch using CLI 'efa inventory drift-reconcile execute --ip &lt;ip-address&gt; --reconcile'</li> <li>6. Step 5 will result in 'default' pw-profile configuration instead of 'Tenant-profile' under the Bridge domain corresponding to the Tenant ctag and EPG ctags will remain in 'cfg-refreshed' state.</li> </ol> <p>Note: The issue is reproducible on BR-SLX9540, BR-SLX9640, SLX9740-40C, SLX9740-80C platforms only.</p>		

<b>Parent Defect ID:</b>	XCO-4147	<b>Issue ID:</b>	XCO-4147
<b>Workaround:</b>	Do not delete the Port channel or LIF associated with the Port channel or the Ethernet Port		
<b>Recovery:</b>	Execute DRC the second time to reconcile the bridge domain to the original state.		

<b>Parent Defect ID:</b>	XCO-4150	<b>Issue ID:</b>	XCO-4150
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 2.7.0
<b>Symptom:</b>	Traffic dashboard is accessible on port 8080 without any username and password.		
<b>Workaround:</b>	Restart iptables service on the node for closing 8080 port to be accessed from outside. sudo systemctl restart efa-iptables.service		

<b>Parent Defect ID:</b>	XCO-4154	<b>Issue ID:</b>	XCO-4154
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 2.7.2
<b>Symptom:</b>	Fabric devices continue to remain in cfg-refresh-err state even though the links between the MCT pair are brought up after the reload		
<b>Condition:</b>	<ol style="list-style-type: none"> <li>1. Configure a single rack(MCT Pair) Non-CLOS fabric with the SLX devices</li> <li>2. All links between the MCT pair are brought down</li> <li>3. "efa fabric show" output indicates the devices with the app-sate set as "cfg-refresh-err"</li> <li>4. Reload the SLX devices</li> <li>5. There are connectivity issues towards the SLX from EFA after reload</li> </ol>		
<b>Recovery:</b>	<ol style="list-style-type: none"> <li>1. Fix the network connectivity issue between EFA and the SLX devices</li> <li>2. Execute "lldp disable" followed by "lldp enable" under the physical interfaces interconnecting the MCT pair</li> <li>3. Execute "efa inventory device update --ip &lt;device-ip&gt;" on the MCT pair</li> </ol>		

<b>Parent Defect ID:</b>	XCO-4156	<b>Issue ID:</b>	XCO-4156
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.1.0
<b>Symptom:</b>	<p>Port-group add operation on a Layer-3 EPG of a bridge-domain enabled tenant that shares cttag with other EPGs may fail. on certain conditions with the error:</p> <p>Device: &lt;device-1-IP&gt; Ctag: &lt;ctag&gt; Anycast &lt;IP-1&gt; subnet is conflicting with already configured Ve 4097 : Anycast &lt;IP-1&gt; on the device &lt;device-1&gt;</p>		

<b>Parent Defect ID:</b>	XCO-4156	<b>Issue ID:</b>	XCO-4156
<b>Condition:</b>	<ol style="list-style-type: none"> <li>1. Configure two layer-3 EPGs with shared ctags and with ports from different SLX devices that are connected as MCT pair</li> <li>2. Do an EPG port-group-delete update operation on one EPG to remove all its ports</li> <li>3. Re-add the same ports back to the EPG</li> </ol> <p>The step 3 will fail with the symptom mentioned above.</p>		
<b>Workaround:</b>	Ensure that the layer-3 EPGs that share ctags are provisioned with all the ports upfront at the time of EPG create time itself		
<b>Recovery:</b>	None		

<b>Parent Defect ID:</b>	XCO-4158	<b>Issue ID:</b>	XCO-4158
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.1.0
<b>Symptom:</b>	Creating a SNMP community with a view that is not configured in EFA may be allowed.		
<b>Condition:</b>	A SNMP view created directly on the SLX can be used as the view associated with a SNMP community, even when the view is not in EFA's view list.		
<b>Workaround:</b>	When creating SNMP communities, consult the SLX configuration to see if any out of band views were created or ensure all view are created by EFA.		
<b>Recovery:</b>	When using an out of band view, creating the view in EFA will take ownership of the view on a specific OID or the community can be changed to use a different view name that is not out of band.		

<b>Parent Defect ID:</b>	XCO-4160	<b>Issue ID:</b>	XCO-4160
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 2.7.0
<b>Symptom:</b>	After node-replacement with multiaccess subinterfaces, EFA is not accessible through VIP.		
<b>Condition:</b>	When new TPVM is installed for node-replacement, if new hostname was different from the older one with the same IP.		
<b>Recovery:</b>	In /etc/keepalived/keepalived.conf on the standby node, update the multiaccess IP and restart the keepalived service.		

<b>Parent Defect ID:</b>	XCO-4164	<b>Issue ID:</b>	XCO-4164
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.1.0
<b>Symptom:</b>	Syslog messages are not seen for SLX (NPB) devices in the XCO user interface.		
<b>Condition:</b>	When the SLX device already has a secured Syslog configuration and then discovers the same device in XCO.		

<b>Parent Defect ID:</b>	XCO-4164	<b>Issue ID:</b>	XCO-4164
<b>Workaround:</b>	Clear the secured Syslog configuration on the SLX NPB device before discovering it in XCO.		
<b>Recovery:</b>	Clear the secured Syslog configuration on the SLX NPB device and rediscover the device.		

<b>Parent Defect ID:</b>	XCO-4165	<b>Issue ID:</b>	XCO-4165
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.1.0
<b>Symptom:</b>	'efa tenant show' command fails with error 500.		
<b>Condition:</b>	A user is assigned multiple tenant admin roles.		
<b>Workaround:</b>	Use 'efa tenant show --name=' to view tenant details.		

<b>Parent Defect ID:</b>	XCO-4168	<b>Issue ID:</b>	XCO-4168
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.1.0
<b>Symptom:</b>	Ingress group is not updating correctly on NPB device version 21.1.2.3		
<b>Condition:</b>	When there is an ingress group associated with given policy exists without any inner/outer tunnel information present and other ingress group which is also associated with same policy with inner/outer tunnel configuration is being updated, the update of 2nd ingress group is not happening.		
<b>Workaround:</b>	Delete ingress group with inner/outer tunnel information and add it back with updated configuration.		
<b>Recovery:</b>	Delete ingress group with inner/outer tunnel information and add it back with updated configuration.		

<b>Parent Defect ID:</b>	XCO-4169	<b>Issue ID:</b>	XCO-4169
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.1.0
<b>Symptom:</b>	For fabric installation, the password reset of a local user having tenant admin role displays an error message related to the permission.		
<b>Condition:</b>	Perform password reset of a local user having a dynamic tenant administrator role.		
<b>Workaround:</b>	Don't create the local user having a dynamic tenant administrator role.		

<b>Parent Defect ID:</b>	XCO-4174	<b>Issue ID:</b>	XCO-4174
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.1.0
<b>Symptom:</b>	For fabric installation, the tenant user logout displays an error message related to the permission.		

<b>Parent Defect ID:</b>	XCO-4174	<b>Issue ID:</b>	XCO-4174
<b>Condition:</b>	Perform logout for a user having a dynamic tenant administrator role.		
<b>Recovery:</b>	The user can ignore the error message as the user will be logged out successfully in spite of the error.		

<b>Parent Defect ID:</b>	XCO-4182	<b>Issue ID:</b>	XCO-4182
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.0.0
<b>Symptom:</b>	rabbitmq log files keep growing and eventually exhausting the disk space.		
<b>Condition:</b>	rabbitmq pod logs which are present after failover are not purged. The fix cleans up logs that are not from the current running pod and older than 5 days. The cleanup is triggered once on start of efa-monitor service and then repeated every 5 days.		
<b>Workaround:</b>	Delete the rabbitmq logs manually at /apps/efa_logs/rabbitmq/ on TPVM and /var/log/efa/rabbitmq/ on server.		

<b>Parent Defect ID:</b>	XCO-4185	<b>Issue ID:</b>	XCO-4185
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 2.7.0
<b>Symptom:</b>	Unable to add notifications subscribers by FQDN.		
<b>Condition:</b>	This issue arises when XCO is installed prior to the configuration of a DNS name server. The fix allows the user to run a command after installation and after the DNS server is configured that allows the XCO services to use host names. See the Admin Guide for details under the section, "Configure DNS Name Server access".		
<b>Workaround:</b>	Requires XCO to be reinstalled after the DNS server was configured.		

<b>Parent Defect ID:</b>	XCO-4202	<b>Issue ID:</b>	XCO-4202
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.1.0
<b>Symptom:</b>	Rule match (ACL) is reconciled with zero DSCP value		
<b>Condition:</b>	When rule match is set with only with default protocol (IPv6/IPv4), and device is discovered from XCO, it is reconciled with DSCP value 0 (zero) in XCO.		

<b>Parent Defect ID:</b>	XCO-4202	<b>Issue ID:</b>	XCO-4202
<b>Workaround:</b>	While editing the rule match, user needs to be cautioned to clear the DSCP value of 0 (zero) in the form so that it will not be pushed to device.		
<b>Recovery:</b>	If the DSCP value zero is configured on the device, user can edit the rule match and clear the DSCP value and push it to device.		

<b>Parent Defect ID:</b>	XCO-4204	<b>Issue ID:</b>	XCO-4204
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.1.0
<b>Symptom:</b>	An incorrect error message is shown to the EFA user when the user tries to add an SLX device (with an expired password) to the fabric, using the below command: "efa fabric device add --name <fabric name> --rack <rackname> --ip <ip>--username <value> --password <value>"		
<b>Condition:</b>	<ol style="list-style-type: none"> <li>1. Make slx password expire by configuring the below on the SLX # show running-config password-attributes password-attributes force-default-password-change password-attributes max-password-age 30.</li> <li>2. Modify the date on SLX past 30 days so that it expires.</li> <li>3. Try to use device registration in EFA using the command "efa fabric device add". Observe the error message displayed is not complete or meaningful.</li> </ol>		
<b>Workaround:</b>	Check for password attribute configuration # show running-config password-attributes password-attributes force-default-password-change password-attributes max-password-age 30. Remove the above configuration so the password does not expire.		
<b>Recovery:</b>	There are 2 recoveries: <ol style="list-style-type: none"> <li>1. Login to switch through management IP and change password and use that changed password to add device to the fabric using the below CLI efa fabric device add --name fab2 --rack room1-rack1 --ip 10.20.246.5 --username admin --password &lt;changed password&gt;</li> <li>2. Reset the device to default configuration so the default credentials can be used in the below CLI efa fabric device add --name fab2 --rack room1-rack1 --ip 10.20.246.5 --username admin --password &lt;default password&gt;</li> </ol>		

<b>Parent Defect ID:</b>	XCO-4772	<b>Issue ID:</b>	XCO-4772
	XCO	<b>Reported in Release:</b>	EFA 2.7.0



Parent Defect ID:	XCO-4772	Issue ID:	XCO-4772
Product:			
Symptom:	SLX stuck in locked status and can not be unlocked		

Parent Defect ID:	XCO-5042	Issue ID:	XCO-5042
Product:	XCO	Reported in Release:	EFA 3.1.0
Symptom:	.Update libc6 package in XCO 3.2		

Parent Defect ID:	XCO-5044	Issue ID:	XCO-5044
Product:	XCO	Reported in Release:	EFA 3.1.0
Symptom:	Current TPVM Version doesn't hold after TPVM upgrade		

Parent Defect ID:	XCO-5167	Issue ID:	XCO-5167
Product:	XCO	Reported in Release:	EFA 2.7.2
Symptom:	EFA shows some VRF in "UNSTABLE" and "cfg-refreshed" state after manual DRC check.		
Condition:	In EFA, Configure VRF with default IPv6 static route(::/0) and assign the VRF to EPG and then execute manual DRC followed by "efa tenant vrf show" and "efa tenant epg show".		

Parent Defect ID:	XCO-5219	Issue ID:	XCO-5219
Product:	XCO	Reported in Release:	EFA 3.0.1
Symptom:	efa-change-hostname does not change the TPVM hostname on the running config of SLX		

Parent Defect ID:	XCO-5220	Issue ID:	XCO-5220
Product:	XCO	Reported in Release:	EFA 3.0.0
Symptom:	PODs moving to CrashLoopBack state		

Parent Defect ID:	XCO-5247	Issue ID:	XCO-5247
	XCO	Reported in Release:	EFA 3.1.0

<b>Parent Defect ID:</b>	XCO-5247	<b>Issue ID:</b>	XCO-5247
<b>Product:</b>			
<b>Symptom:</b>	EFA logout displays error after EFA restore.		
<b>Condition:</b>	EFA logout displays an error that 'Logout Failed' after EFA restore.		

<b>Parent Defect ID:</b>	XCO-5252	<b>Issue ID:</b>	XCO-5252
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.0.1
<b>Symptom:</b>	Drift-reconcile failure during SLX-OS upgrade to 20.4.2ac		
<b>Condition:</b>	DRC triggered during FWDL is skipped but in efa cli it is reported as DRC failed.		
<b>Workaround:</b>	Upgrade to EFA3.2.0.		
<b>Recovery:</b>	Not applicable.		

<b>Parent Defect ID:</b>	XCO-5486	<b>Issue ID:</b>	XCO-5486
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.1.1
<b>Symptom:</b>	VZW XCO-VM 3.1.1 cannot plot the policy graphs on dashboard or troubleshooting page		

<b>Parent Defect ID:</b>	XCO-5657	<b>Issue ID:</b>	XCO-5657
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.0.0
<b>Symptom:</b>	EFA PODs moves to evicted state.		
<b>Condition:</b>	When the disk utilization reaches 85%, EFA PODs moves to Evicted state and EFA login fails.		
<b>Workaround:</b>	Clean up the disk space and load the docker_k3s images.		

<b>Parent Defect ID:</b>	XCO-5740	<b>Issue ID:</b>	XCO-5740
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.1.1
<b>Symptom:</b>	SLX Box is rebooted when refresh configuration is run from XCO GUI.		
<b>Condition:</b>	Run refresh configuration for SLX box from XCO GUI		
<b>Workaround:</b>	NA		
<b>Recovery:</b>	NA		

<b>Parent Defect ID:</b>	XCO-5758	<b>Issue ID:</b>	XCO-5758
	XCO	<b>Reported in Release:</b>	XCO 3.1.x

<b>Parent Defect ID:</b>	XCO-5758	<b>Issue ID:</b>	XCO-5758
<b>Product:</b>			
<b>Symptom:</b>	<p>On fresh installation of EFA/XCO on Ubuntu 20.04 LTS, deployment fails while installing glusterFS with the following error.</p> <p>Dependency libnl-3-200 is not installed.</p> <p>Errors were encountered while processing:</p> <pre>libnl-route-3-200:amd64 libibverbs1:amd64 librdmacm1:amd64 ibverbs-providers:amd64</pre> <p>dpkg: dependency problems prevent configuration of libnl-route-3-200:amd64:</p> <p>libnl-route-3-200:amd64 depends on libnl-3-200 (= 3.4.0-1); however: Package libnl-3-200 is not installed.</p>		

<b>Parent Defect ID:</b>	XCO-5930	<b>Issue ID:</b>	XCO-5930
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.0.1
<b>Symptom:</b>	<p>Snmp community creation without view will fail after device registration is done but before the device persist to add the default view efav3View to the DB.</p> <p>The fix is to move the creation of default view to the beginning of device persist to reduce the time delay.</p>		
<b>Condition:</b>	<p>Snmp community creation without view will fail after device registration is done but before the device persist to add the default view efav3View to the DB.</p>		
<b>Workaround:</b>	<p>After fix, the time delay between device registration and creation of default view is much reduced. If it still happens, wait a while after device is registered to create snmp community.</p>		
<b>Recovery:</b>	<p>After fix, the time delay between device registration and creation of default view is much reduced. If it still happens, wait a while after device is registered to create snmp community.</p>		

<b>Parent Defect ID:</b>	XCO-6318	<b>Issue ID:</b>	XCO-6318
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.1.1
<b>Symptom:</b>	<p>User logged into XCO gets logged out every hour irrespective of user is active on GUI or not.</p>		

<b>Parent Defect ID:</b>	XCO-6359	<b>Issue ID:</b>	XCO-6359
	XCO	<b>Reported in Release:</b>	EFA 3.1.1

<b>Parent Defect ID:</b>	XCO-6359	<b>Issue ID:</b>	XCO-6359
<b>Product:</b>			
<b>Symptom:</b>	User cannot scroll policy rules in troubleshooting and monitoring page when there are multiple rules.		

<b>Parent Defect ID:</b>	XCO-6396	<b>Issue ID:</b>	XCO-6396
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.1.1
<b>Symptom:</b>	GUI can't create user profile with verizon wireless email-ids with ""		

## Defects Closed without Code Changes

The following defects were closed without code changes in ExtremeCloud Orchestrator 3.2.0.

<b>Parent Defect ID:</b>	XCO-3443	<b>Issue ID:</b>	XCO-3443
<b>Reason Code:</b>	Working as Designed		
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.1.0
<b>Symptom:</b>	After fresh installation of XCO or after IP change, browser shows the 'Certificate is not Valid'.		
<b>Workaround:</b>	Add EFA CA to the trust store in the browser. Incase of an IP change, regenerate the EFA server certificate using CLI. Refer to Administration guide for details.		

<b>Parent Defect ID:</b>	XCO-4137	<b>Issue ID:</b>	XCO-4137
<b>Reason Code:</b>	Insufficient Information		
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 2.5.5
<b>Symptom:</b>	EFA can not connect to SLX switch until a reload is performed Case		

<b>Parent Defect ID:</b>	XCO-4139	<b>Issue ID:</b>	XCO-4139
<b>Reason Code:</b>	Insufficient Information		
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 2.7.2

<b>Parent Defect ID:</b>	XCO-4139	<b>Issue ID:</b>	XCO-4139
<b>Symptom:</b>	In a CLOS fabric, multiple fabric ports belonging to different fabric devices can have the same IP address assigned incorrectly. For example: interface ethernet 0/x on device D1 and ethernet 0/y on device D2 can have an ip-address 10.1.1.1/31 assigned.		
<b>Recovery:</b>	<ol style="list-style-type: none"> <li>1. Disable the LLDP protocol under the interfaces ethernet 0/x on D1 and ethernet 0/y on D2</li> <li>2. Execute "efa inventory device update --ip &lt;device-ip&gt;" for both D1 and D2</li> <li>3. Execute "efa fabric configure --name &lt;fabric-name&gt;"</li> </ol>		

<b>Parent Defect ID:</b>	XCO-4141	<b>Issue ID:</b>	XCO-4141
<b>Reason Code:</b>	Insufficient Information		
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 2.7.1
<b>Symptom:</b>	EPG update with operation vrf-delete fails with reason record not found.		
<b>Condition:</b>	<ol style="list-style-type: none"> <li>1. Create L3 EPG with vrf1</li> <li>2. In the background trigger inventory device update</li> <li>3. Execute EPG update vrf-delete/add consecutively.</li> <li>4. Inv.vrf_created for vrf1 is received with reason: manual update, hence its gets vrf1 gets added as oob_Created vrf. and same gets consumed in the vrf-add operation.</li> <li>5. One of the vrf-delete fails with the reason: record not found</li> </ol>		
<b>Recovery:</b>	<ol style="list-style-type: none"> <li>1. Delete EPG</li> <li>2. Manually delete VRF from the device.</li> </ol>		

<b>Parent Defect ID:</b>	XCO-4145	<b>Issue ID:</b>	XCO-4145
<b>Reason Code:</b>	Insufficient Information		
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.0.0
<b>Symptom:</b>	Firmware-download progress is stuck in state 'Device Reload Completed'		

<b>Parent Defect ID:</b>	XCO-4151	<b>Issue ID:</b>	XCO-4151
<b>Reason Code:</b>	Already Reported		
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.0.0

<b>Parent Defect ID:</b>	XCO-4151	<b>Issue ID:</b>	XCO-4151
<b>Symptom:</b>	Certificate Expiry warning is shown on 'efa login' after certificate has expired.		
<b>Workaround:</b>	Renew EFA server certificate.		

<b>Parent Defect ID:</b>	XCO-4155	<b>Issue ID:</b>	XCO-4155
<b>Reason Code:</b>	Already Implemented		
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.1.0
<b>Symptom:</b>	Renewal of K3s server certificate fails after a time-shift.		
<b>Condition:</b>	K3s CA certificate has been renewed and immediately K3s server certificate renewal is tried again.		
<b>Workaround:</b>	During K3s CA certificate renewal, the K3s server certificate is generated as well. If the time-shift is very quick, then wait for few hours and then retry the same operation again.		

<b>Parent Defect ID:</b>	XCO-4178	<b>Issue ID:</b>	XCO-4178
<b>Reason Code:</b>	Not Applicable		
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.0.0
<b>Symptom:</b>	SLX not sending NTP traps		

<b>Parent Defect ID:</b>	XCO-4186	<b>Issue ID:</b>	XCO-4186
<b>Reason Code:</b>	Not Reproducible		
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.0.0
<b>Symptom:</b>	Unable to logon to EFA due to no resources found in efa namespace		

<b>Parent Defect ID:</b>	XCO-4191	<b>Issue ID:</b>	XCO-4191
<b>Reason Code:</b>	Insufficient Information		
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 2.7.0
<b>Symptom:</b>	Device reporting as going through firmware download when trying to update epg		

<b>Parent Defect ID:</b>	XCO-4414	<b>Issue ID:</b>	XCO-4414
	Already Implemented		

<b>Parent Defect ID:</b>	XCO-4414	<b>Issue ID:</b>	XCO-4414
<b>Reason Code:</b>			
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 2.5.5
<b>Symptom:</b>	Port adding to EPG is failing		

<b>Parent Defect ID:</b>	XCO-5237	<b>Issue ID:</b>	XCO-5237
<b>Reason Code:</b>	Not Reproducible		
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.0.1
<b>Symptom:</b>	EFA - After TPVM incremental upgrades (4.5.6>>4.5.7) and followed by SLX reloads the EFA application intermittently fails		

<b>Parent Defect ID:</b>	XCO-5614	<b>Issue ID:</b>	XCO-5614
<b>Reason Code:</b>	Already Implemented		
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.0.1
<b>Symptom:</b>	EFA login failed for about 30 minutes after EFA restore backup		

<b>Parent Defect ID:</b>	XCO-5621	<b>Issue ID:</b>	XCO-5621
<b>Reason Code:</b>	Not a Software Defect		
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.0.0
<b>Symptom:</b>	Port-channel config lost after applying the workaround for the defect: 67907		

<b>Parent Defect ID:</b>	XCO-5622	<b>Issue ID:</b>	XCO-5622
<b>Reason Code:</b>	Not a Software Defect		
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.0.0
<b>Symptom:</b>	CNIS 1.8: Vlan/epg configuration inconsistency between EFA and SLX		

<b>Parent Defect ID:</b>	XCO-5923	<b>Issue ID:</b>	XCO-5923
<b>Reason Code:</b>	Working as Designed		
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.0.0
<b>Symptom:</b>	EFA Tenant Update is not working properly[ bgp listen-limit for particular vrf is not getting updated].		

<b>Parent Defect ID:</b>	XCO-5925	<b>Issue ID:</b>	XCO-5925
	Already Implemented		

<b>Parent Defect ID:</b>	XCO-5925	<b>Issue ID:</b>	XCO-5925
<b>Reason Code:</b>			
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.1.0
<b>Symptom:</b>	breakout ports found together with parent interface, DRC fails		

<b>Parent Defect ID:</b>	XCO-5928	<b>Issue ID:</b>	XCO-5928
<b>Reason Code:</b>	Already Implemented		
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.1.0
<b>Symptom:</b>	Health-Check DRC Removed Cluster Peer Configuration		

<b>Parent Defect ID:</b>	XCO-5933	<b>Issue ID:</b>	XCO-5933
<b>Reason Code:</b>	Already Implemented		
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 2.5.4
<b>Symptom:</b>	Standby EFA is showing as down and also Backup is not happening		

<b>Parent Defect ID:</b>	XCO-5935	<b>Issue ID:</b>	XCO-5935
<b>Reason Code:</b>	Insufficient Information		
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 2.7.0
<b>Symptom:</b>	EFA failed to register the SLX nodes		

<b>Parent Defect ID:</b>	XCO-5936	<b>Issue ID:</b>	XCO-5936
<b>Reason Code:</b>	Already Implemented		
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 2.7.0
<b>Symptom:</b>	kubelet Readiness probe failed: Failed to read status file /status/status.json		
<b>Condition:</b>	This particular issue of liveness/readiness probe failure and the subsequent calico-kube-controller crashloop was caused by the file permission issue.		
<b>Workaround:</b>	The issue has been fixed as a part of the updated hardening script with the tpvm release 4.5.10.		
<b>Recovery:</b>	EFA redeploy.		

<b>Parent Defect ID:</b>	XCO-6212	<b>Issue ID:</b>	XCO-6212
	Working as Designed		



<b>Parent Defect ID:</b>	XCO-6212	<b>Issue ID:</b>	XCO-6212
<b>Reason Code:</b>			
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.1.1
<b>Symptom:</b>	EFA tenant creation intermittently fails after initial fabric creation - ports are not available		

<b>Parent Defect ID:</b>	XCO-6430	<b>Issue ID:</b>	XCO-6430
<b>Reason Code:</b>	Not Applicable		
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 2.7.0
<b>Symptom:</b>	.EFA 2.7.0 after spine node reload EFA is non-operational		

## Open Defects

The following defects are open in ExtremeCloud Orchestrator 3.2.0.

<b>Parent Defect ID:</b>	XCO-3438	<b>Issue ID:</b>	XCO-3438
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 2.7.0
<b>Symptom:</b>	When endpoint group create or update operation REST requests of multiple endpoint groups each with 50+ ctags are issued concurrently, one or two of the requests may fail with "Error 1452: Cannot add or update a child row: a foreign key constraint fails" or with an error indicating database timeout or an error indicating failure of network property delete.		
<b>Condition:</b>	When multiple endpoint group requests are processed concurrently, some of the database requests initiated by EFA may cause database to abort one of the request with the above mentioned error		
<b>Workaround:</b>	Execute the commands sequentially		
<b>Recovery:</b>	EFA database and SLX device configurations are always not affected by this error and hence no recovery is required. The failed commands shall be rerun sequentially to successful completion of the expected operations		

<b>Parent Defect ID:</b>	XCO-3445	<b>Issue ID:</b>	XCO-3445
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.0.0
<b>Symptom:</b>	DRC will not identify the drift and hence will not reconcile the drifted configuration		

<b>Parent Defect ID:</b>	XCO-3445	<b>Issue ID:</b>	XCO-3445
<b>Condition:</b>	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. Execute "efa inventory drift-reconcile execute --ip <device-ip>"		
<b>Recovery:</b>	Manually reconfigure the removed configurations from the device		

<b>Parent Defect ID:</b>	XCO-3448	<b>Issue ID:</b>	XCO-3448
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.0.0
<b>Symptom:</b>	Super spine devices continue to remain in cfg-refreshed state even after the invalid topology connections (i.e. superspine to superspine connections) are removed by disabling the LLDP links between the super spine devices followed by a DRC (Drift and Reconcile)		
<b>Condition:</b>	Below are the steps to reproduce the issue 1. Configure a 5-stage CLOS fabric 2. Enable the LLDP link(s) between the superspine devices 3. App state of superspine devices moves to cfg-refresh-error 4. Disable the LLDP link(s) (which were enabled in step 2) between the superspine devices 5. App state of superspine devices moves to cfg-refreshed 6. Execute "efa inventory drift-reconcile execute --ip <device-ip> --reconcile" for the super-spine devices		
<b>Recovery:</b>	Execute "efa fabric configure --name <fabirc-name>" so that the superspine devices move to cfg-in-sync state		

<b>Parent Defect ID:</b>	XCO-3458	<b>Issue ID:</b>	XCO-3458
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.1.0
<b>Symptom:</b>	Port breakout fails for SLX devices with "generic message error". On device new split ports are created.		
<b>Recovery:</b>	login to SLX CLI and remove the breakout of port using these steps: Run following commands configuration terminal hardware connector <slot/interface> breakout mode <4x10g/4x25g>		

<b>Parent Defect ID:</b>	XCO-3458	<b>Issue ID:</b>	XCO-3458
	<p>no breakout  e.g. if the port 0/50 got this issue, following are the commands to run after login to CLI</p> <pre>Freedom7-Bng# configure t Entering configuration mode terminal Freedom7-Bng(config)# hardware Freedom7-Bng(config-hardware)# connector 0/50 Freedom7-Bng(config-connector-0/50)# breakout mode 4x10g Freedom7-Bng(config-connector-0/50)# no breakout</pre>		

<b>Parent Defect ID:</b>	XCO-3471	<b>Issue ID:</b>	XCO-3471
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.1.0
<b>Symptom:</b>	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.		
<b>Condition:</b>	<ol style="list-style-type: none"> <li>1. Create a 3-stage CLOS fabric, add devices with MCT leaf, spine, and border-leaf and configure the fabric</li> <li>2. Convert the 3-stage CLOS fabric to a 5-stage CLOS fabric using the fabric migrate command  <pre>"efa fabric migrate --type "3-to-5-stage" --source-fabric &lt;source-fabric&gt; --destination-3-stage-leaf-spine-pod &lt;pod-name&gt; --destination-3-stage-border-leaf-pod &lt;pod-name&gt;"</pre> </li> <li>3. Add super-spine POD devices to the migrated 5-stage CLOS fabric</li> <li>4. Disconnect the BorderLeaf to Spine links and reconnect the BorderLeaf to Super-Spine links</li> <li>5. Configure the migrated 5-stage CLOS fabric</li> </ol>		
<b>Recovery:</b>	Manually delete the stale BGP peer-groups from both the Border Leaf and Spine devices		

<b>Parent Defect ID:</b>	XCO-3472	<b>Issue ID:</b>	XCO-3472
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.1.0
<b>Symptom:</b>	XCO IP/VIP change is not updated on device for telemetry/streaming and syslog		
<b>Condition:</b>	Once the XCO is installed and devices are discovered in Visibility installation, if the XCO node IP/VIP changes, those are not updated on device for receiving the statistics and syslog.		

<b>Parent Defect ID:</b>	XCO-3472	<b>Issue ID:</b>	XCO-3472
<b>Workaround:</b>	Change the XCO IP/VIP before discovering the devices.		
<b>Recovery:</b>	Required to delete and add all devices again after the IP/VIP of XCO is changed.		

<b>Parent Defect ID:</b>	XCO-4127	<b>Issue ID:</b>	XCO-4127
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.0.0
<b>Symptom:</b>	Ports are not listed in the port-channel creation for SLX NPB devices		
<b>Condition:</b>	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.		
<b>Workaround:</b>	For breakout ports, make sure that cables are connected so that port speed will be updated.		
<b>Recovery:</b>	NA		

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

<b>Parent Defect ID:</b>	XCO-4129	<b>Issue ID:</b>	XCO-4129
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.0.0
<b>Symptom:</b>	Disable of vn-tag header strip and enabling of 802.1BR header strip fails from XCO GUI for SLX NPB		
<b>Condition:</b>	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.		

<b>Parent Defect ID:</b>	XCO-4129	<b>Issue ID:</b>	XCO-4129
<b>Workaround:</b>	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.		
<b>Recovery:</b>	NA		

<b>Parent Defect ID:</b>	XCO-4146	<b>Issue ID:</b>	XCO-4146
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 2.7.2
<b>Symptom:</b>	The fabric devices continue to remain in cfg-refresh-err state after the tpvm fail over.		
<b>Condition:</b>	<ol style="list-style-type: none"> <li>1. Fabric devices are already in cfg-refresh-err state due to LLDP Link down(LD) event.</li> <li>2. Bring up the LLDP links responsible for the fabric devices to be in cfg-refresh-err state.</li> <li>3. Execute the TPVM failover by 'tpvm stop' and 'tpvm start' commands during the LLDP Link up (LA) event handling caused by 2.</li> </ol>		
<b>Recovery:</b>	<p>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".</p> <ol style="list-style-type: none"> <li>1.1. "shutdown" the interface link on the physical link on Devices follow by "efa inventory device update --ip &lt;device-ip&gt;", which generates LD events</li> <li>2.1. "no shutdown" the interface link on the physical link on Devices follow by "efa inventory device update --ip &lt;device-ip&gt;", which generates LA events</li> <li>1.3. If the pending config contains "LA" : Execute "efa inventory drift-reconcile execute --ip &lt;device-ip&gt; --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 &lt;fabric-name&gt;" to clean up the configuration on devices which are in cfg-refresh-err /cfg-refreshed state.</li> </ol> <p>[OR]</p> <ol style="list-style-type: none"> <li>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.</li> <li>2.1. "reload" the switches without out maintenance mode to enable</li> <li>2.2. Execute "efa inventory drift-reconcile execute --ip &lt;device-ip&gt; --reconcile" on the devices which are in cfg-refresh-err /cfg-refreshed state.</li> </ol>		

<b>Parent Defect ID:</b>	XCO-4180	<b>Issue ID:</b>	XCO-4180
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.0.0
<b>Symptom:</b>	Http Login/Logout Raslogs repeatedly observed on device side, after CLI execution.		

<b>Parent Defect ID:</b>	XCO-4180	<b>Issue ID:</b>	XCO-4180
<b>Condition:</b>	During Ntp create/delete operation, few repeated logs are observed on device.		
<b>Workaround:</b>	On device side we can configure Raslog to suppress/ignore logs. logging raslog message SEC-1206 suppress //to suppress logging raslog console CRITICAL //to discard other types and show only critical		
<b>Recovery:</b>	It is a non-functional issue and has no impact on the overall system operations.		

<b>Parent Defect ID:</b>	XCO-5235	<b>Issue ID:</b>	XCO-5235
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.1.0
<b>Symptom:</b>	High Memory utilization by litestream process		
<b>Condition:</b>	Condition not known.		
<b>Workaround:</b>	Not Applicable		
<b>Recovery:</b>	Following steps need to be followed. 1. Check for litestream process on active using ps aux   grep litestream 2. Use following command to restart. systemctl restart litestream.		

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

<b>Parent Defect ID:</b>	XCO-5788	<b>Issue ID:</b>	XCO-5788
<b>Product:</b>	XCO	<b>Reported in Release:</b>	XCO 3.2.0
<b>Symptom:</b>	Preparing for a fabric-wide firmware download either through CLI or the XCO GUI results in an incorrect grouping of leaf and border-leaf devices where the MCT peers are placed in the same firmware download group.		

<b>Parent Defect ID:</b>	XCO-5788	<b>Issue ID:</b>	XCO-5788
<b>Condition:</b>	A timing window exists where immediately performing a fabric-wide firmware download through the XCO GUI or preparing for a fabric-wide firmware download through the CLI right after adding devices to a fabric and configuring the fabric can result in an incorrect firmware download grouping of leaf and border-leaf devices.		
<b>Workaround:</b>	If a fabric-wide firmware download is to be performed right after adding devices to and configuring the fabric, then use "efa inventory device discovery-time list --fabric <fabric name>" to poll for the completion of the fabric configuration. Every device in the fabric should have a "FabricConfigure" reason listed in order to proceed with the fabric-wide firmware download preparation and execution.		
<b>Recovery:</b>	None		

<b>Parent Defect ID:</b>	XCO-5795	<b>Issue ID:</b>	XCO-5795
<b>Product:</b>	XCO	<b>Reported in Release:</b>	XCO 3.2.0
<b>Symptom:</b>	The data in the previous page has the ethernet interfaces as well as other interfaces even though the page is supposed to contain only the ethernet interfaces		
<b>Condition:</b>	<p>Below are the steps to reproduce the issue:</p> <ol style="list-style-type: none"> <li>1. In the XCO GUI Device Inventory view, the user selects the "Network Essentials" options from the row action menu.</li> <li>2. The user navigates to page next page</li> <li>2. And then comes back to the previous page</li> </ol>		

<b>Parent Defect ID:</b>	XCO-5931	<b>Issue ID:</b>	XCO-5931
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.0.1
<b>Symptom:</b>	Firmware Not Committed" but "Firmware Download Show Overall Status" shows "Device Update In Progress		
<b>Condition:</b>	<p>For the firmware download workflow, it will perform the FWDL on each device as prescribed by the grouping and then finally do a "quick" device update (device links only) for all devices that have participated in the FWDL.</p> <p>The purpose of the device links only update is to ensure the fabric configurations are in-sync after the FWDL workflow has completed since devices were rebooted to activate the new firmware.</p> <p>In this customer case they only did a FWDL of a single device, but the workflow is the same... a device links only update will be performed at the end.</p> <p>The firmware download show command contains the individual device's status in the table and the "Overall Status" at the bottom reflects EFA's overall status of the FWDL workflow which includes the Device links only update.</p>		

<b>Parent Defect ID:</b>	XCO-5931	<b>Issue ID:</b>	XCO-5931
<b>Workaround:</b>	The user must poll for the Overall Status Completion to proceed for another FWDL workflow prepare/execute.		
<b>Recovery:</b>	Not applicable.		

<b>Parent Defect ID:</b>	XCO-5990	<b>Issue ID:</b>	XCO-5990
<b>Product:</b>	XCO	<b>Reported in Release:</b>	XCO 3.2.0
<b>Symptom:</b>	A detailed progress bar (with upgrade state) is not available in the Device Inventory view.		
<b>Condition:</b>	<p>Below are the steps to reproduce:</p> <ol style="list-style-type: none"> <li>1. In XCO GUI, the user opens the option for Fabric Topology view for a fabric</li> <li>2. In Fabric Topology View, the user chooses the option of "Upgrade Fabric" from "Fabric Actions".</li> <li>3. The "Fabric Upgrade" form is visible. The user selects an upgrade with or without the "auto-commit" option.</li> <li>4. Once the user confirms the upgrade, the progress bar is visible in the "Fabric Topology" view.</li> <li>5. While the firmware download is in progress the user switches to the "Device Inventory" view and searches for the device upgraded.</li> </ol>		

<b>Parent Defect ID:</b>	XCO-5993	<b>Issue ID:</b>	XCO-5993
<b>Product:</b>	XCO	<b>Reported in Release:</b>	XCO 3.2.0
<b>Symptom:</b>	The notifications show "Devices Upgrade Ongoing" instead of "Devices Restore Ongoing"		
<b>Condition:</b>	<p>Below are the steps to reproduce the issue:</p> <ol style="list-style-type: none"> <li>1. In GUI XCO, the user opens the "Fabric Topology" view for a fabric.</li> <li>2. The user selects the "Upgrade Firmware" option from the "Fabric Actions"</li> <li>3. The Firmware Upgrade form is visible. The user selects the firmware upgrade of fabric with no "Auto Commit" option.</li> <li>4. Once the upgrade is initiated, the Fabric Topology view shows the progress bar and state of the operation.</li> <li>5. The user waits for the download to be completed and for the progress bar to show around 80% completion. Fabric Commit and Restore options will be available.</li> <li>6. The user selects the Restore option</li> </ol>		

<b>Parent Defect ID:</b>	XCO-6054	<b>Issue ID:</b>	XCO-6054
	XCO	<b>Reported in Release:</b>	XCO 3.2.0



<b>Parent Defect ID:</b>	XCO-6054	<b>Issue ID:</b>	XCO-6054
<b>Product:</b>			
<b>Symptom:</b>	Once the firmware upgrade is completed, the progress bar will show around 80% completion since the user has not chosen the auto-commit option during the firmware upgrade.		
<b>Condition:</b>	<p>Below are the steps to reproduce the issue:</p> <ol style="list-style-type: none"> <li>1. In XCO GUI user navigates to the Topology view of a fabric</li> <li>2. The user chooses the "Firmware Upgrade" option under "Fabric Actions".</li> <li>3. Firmware Upgrade form is visible. The user chooses to perform firmware download with "Activate" and no "Auto Commit" option.</li> <li>4. The user confirms the upgrade options.</li> <li>5. The user will be able to see the progress of the ongoing upgrade operation.</li> </ol>		

<b>Parent Defect ID:</b>	XCO-6070	<b>Issue ID:</b>	XCO-6070
<b>Product:</b>	XCO	<b>Reported in Release:</b>	XCO 3.2.0
<b>Symptom:</b>	A detailed progress bar status is not showing under the "Device Inventory" view but is visible only under the "Fabric Topology" view or "Fabric Device" view.		
<b>Condition:</b>	<p>Below are the steps to reproduce:</p> <ol style="list-style-type: none"> <li>1. In XCO GUI, the user opens the "Device Inventory" view.</li> <li>2. The user selects devices from a fabric and clicks on the "Upgrade Firmware" option from the table action menu.</li> <li>3. The "Fabric Upgrade" form is visible. The user selects an upgrade for the selected devices.</li> <li>4. Once the user confirms the upgrade, a progress bar is visible in the "Device Inventory" view.</li> <li>5. The user changes the page and comes back to the same page. The progress bar is not visible.</li> <li>6. The user switches to the "Fabric Topology" view for the fabric of the particular devices. The progress bar is visible.</li> </ol>		

<b>Parent Defect ID:</b>	XCO-6172	<b>Issue ID:</b>	XCO-6172
	XCO	<b>Reported in Release:</b>	XCO 3.2.0

<b>Parent Defect ID:</b>	XCO-6172	<b>Issue ID:</b>	XCO-6172
<b>Product:</b>			
<b>Symptom:</b>	SLX currently doesn't support configuring both IPv4 and IPv6 DNS together. When both IPv4 and IPv6 DNS are configured during tpvm deployment, only one trusted peer config takes effect.		
<b>Workaround:</b>	The best practice is to use IPV4 DNS for XCO deployment.		

<b>Parent Defect ID:</b>	XCO-6189	<b>Issue ID:</b>	XCO-6189
<b>Product:</b>	XCO	<b>Reported in Release:</b>	XCO 3.2.0
<b>Symptom:</b>	SLX currently doesn't support configuring both IPv4 and IPv6 trusted peers together. When both IPv4 and IPv6 trusted-peers are configured after tpvm deploy, only one trusted peer config takes effect.		
<b>Workaround:</b>	The best practice is to use IPV4 trusted peer for XCO deployment.		

<b>Parent Defect ID:</b>	XCO-6355	<b>Issue ID:</b>	XCO-6355
<b>Product:</b>	XCO	<b>Reported in Release:</b>	XCO 3.2.0
<b>Symptom:</b>	<p>When all spine devices are prepared for a firmware download in the same group, a validation error will be returned stating that the last operational spine cannot be added.</p> <p>This validation error can be bypassed by first adding all but one spine in the default group, then finally adding the last spine in the default group.</p>		
<b>Workaround:</b>	<p>Through CLI, prepare all devices by IP address using the force parameter. "efa inventory device firmware-download prepare add --ip &lt;comma separated list of device IPs&gt; --firmware-host &lt;registered firmware-host IP address&gt; --firmware-directory &lt;firmware distribution path&gt; --force".</p> <p>This will enable all devices in the fabric to be prepared for a simultaneous firmware-download where traffic loss is expected.</p>		
<b>Recovery:</b>	None		

<b>Parent Defect ID:</b>	XCO-6360	<b>Issue ID:</b>	XCO-6360
	XCO	<b>Reported in Release:</b>	EFA 3.1.1

<b>Parent Defect ID:</b>	XCO-6360	<b>Issue ID:</b>	XCO-6360
<b>Product:</b>			
<b>Symptom:</b>	Few Important system logs are not seen in XCO UI.		
<b>Condition:</b>	Device is discovered from XCO and some of cards are removed/ inserted in device.		

<b>Parent Defect ID:</b>	XCO-6398	<b>Issue ID:</b>	XCO-6398
<b>Product:</b>	XCO	<b>Reported in Release:</b>	XCO 3.2.0
<b>Symptom:</b>	Logs for monitor service and efa-monitor service are not available.		
<b>Condition:</b>	If the user runs 'efactl clean', the services do not write to logs anymore.		
<b>Workaround:</b>	Restart the specific services on all nodes of XCO after running 'efactl clean'. sudo systemctl restart monitor sudo systemctl restart efamonitor		

<b>Parent Defect ID:</b>	XCO-6429	<b>Issue ID:</b>	XCO-6429
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.1.1
<b>Symptom:</b>	ACL hits displayed on stats table while it should maintain its position during stats update		
<b>Condition:</b>	ACL hits dynamically keep moving around and it can't track of hits.		
<b>Workaround:</b>	Sequence number is implemented and rest of the things will be fixed in next release.		

<b>Parent Defect ID:</b>	EFA-16128	<b>Issue ID:</b>	XCO-6466
<b>Product:</b>	XCO	<b>Reported in Release:</b>	EFA 3.1.1
<b>Symptom:</b>	Full IPv4/IPv6 address are not seen for policy rules.		
<b>Condition:</b>	When user launch troubleshoot and monitor page to select the rules.		
<b>Workaround:</b>	Mouse over tip is provided so that user can get the complete address.		
<b>Recovery:</b>	NA		

<b>Parent Defect ID:</b>	XCO-6510	<b>Issue ID:</b>	XCO-6510
<b>Product:</b>	XCO	<b>Reported in Release:</b>	XCO 3.2.0
<b>Symptom:</b>	The "Network Essentials" option is listed as a device action for the NPB device and a blank page is opened when the user clicks on that.		

<b>Parent Defect ID:</b>	XCO-6510	<b>Issue ID:</b>	XCO-6510
<b>Condition:</b>	NPB device is discovered in XCO and user clicks on the device action (for the NPB device) from the inventory page.		
<b>Workaround:</b>	Don't select the networks essentials for NPB devices from device inventory page.		

## 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 2826. For the support phone number in your country, visit: [www.extremenetworks.com/support/contact](http://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.