Extreme Fabric Automation Release Notes

3.1.0

9037631-00 Rev AB
January 2024

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

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/

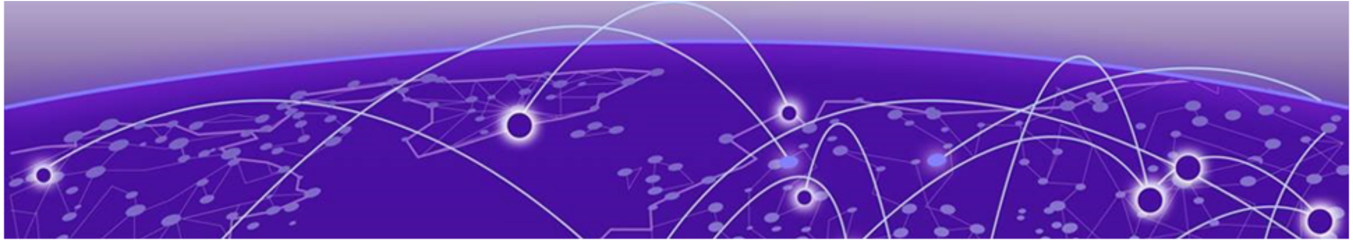

Table of Contents

Release Notes

New In This Release

Extreme Fabric Automation 3.1.0 provides the following features and improvements.

Table 1: Features and improvements

Feature	Description
Certificate Management	Describes K3s CA certificates renewal and modified efa certificate device install command. For more information, refer to the *Extreme Fabric Automation Administration Guide, 3.1.0*.
EFA Inventory and Fabric Service Enhancements	Describes migration of 3-Stage Clos to 5-Stage Clos fabric. For more information, refer to the *Extreme Fabric Automation Administration Guide, 3.1.0*.
L2 and L3 Services Features and Improvements	Describes the tenant service feature enhancements. For more information, refer to the *Extreme Fabric Automation Administration Guide, 3.1.0*.
Health and Fault Management	Describes the unified health and fault management system in EFA. For more information, refer to the *Extreme Fabric Automation Administration Guide, 3.1.0*.

Table 1: Features and improvements (continued)

Feature	Description
BGP Standard Community-list and Extended community-list	Describes the Route map match and Set community list configuration in EFA. For more information, refer to the *Extreme Fabric Automation Administration Guide, 3.1.0*.
Northbound IPv6 support for EFA O and M	Describes the additional virtual IP support for IPv6 during EFA installation or upgrade. For more information, refer to the *Extreme Fabric Automation Administration Guide, 3.1.0*.
EFA installer enhancements	Describes EFA installer support for a packet and fabric suites. For more information, refer to the *Extreme Fabric Automation Deployment Guide, 3.1.0*.
	EFA installer support for TPVM deployments. For more information, refer to the *Extreme Fabric Automation Deployment Guide, 3.1.0*.
Infrastructure and deployment enhancements	Describes single CLI commands supported on SLX for HA deployment. For more information, refer to the *Extreme Fabric Automation Deployment Guide, 3.1.0*.
TACACS configuration	Describes TACACS configuration using CLI. For more information, refer to the *Extreme Fabric Automation Security Guide, 3.1.0*.
Security hardening for SLX	Describes security hardening for SLX. For more information, refer to the *Extreme Fabric Automation Security Guide, 3.1.0*.
Visibility management support	As part of EFA 3.1.0, Visibility management support has been added. This is currently a controlled release and not generally available. For any questions, contact your local Account Team.

For more information, see Defects Closed with Code Changes on page 15.

Supported Platforms and Deployment Models for Fabric Manager

Support includes bare metal, OVA, and TPVM deployment models, supported TPVM versions, supported SLX-OS software versions, and supported SLX devices.

Table 2: Bare Metal Deployment Models

EFA Version	Deployment	Managed SLX Devices	Multi-Fabric Support	Ubuntu Version	Virtual Machine
2.7.x, 3.0.0, and 3.1.0	External server (bare metal)	More than 24	Yes	16.04, 18.04, and 20.04	• CPU: 4 cores • Storage: 64 GB • RAM: 8 GB

Table 3: OVA Deployment Models

EFA Version	Deployment	Managed SLX Devices	Multi-Fabric Support	Ubuntu Version	Virtual Machine
2.7.x, 3.0.0, and 3.1.0	External server (OVA)	More than 24	Yes	18.04	• CPU: 4 cores • Storage: 64 GB • RAM: 8 GB

Table 4: TPVM Deployment Models

EFA Version	TPVM Deployment	Managed SLX Devices	Multi-Fabric Support	Ubuntu Version	Minimum SLX-OS Version
2.7.x	• SLX 9150 • SLX 9250 • SLX 9740 • Extreme 8520 • Extreme 8720	Up to 24	Yes	18.04	20.4.1
3.0.x	• SLX 9150 • SLX 9250 • SLX 9740 • Extreme 8520 • Extreme 8720	Up to 24	Yes	18.04	20.4.2
3.1.x	• SLX 9150 • SLX 9250 • SLX 9740	Up to 24	Yes	18.04	20.4.2

Table 4: TPVM Deployment Models (continued)

EFA Version	TPVM Deployment	Managed SLX Devices	Multi-Fabric Support	Ubuntu Version	Minimum SLX-OS Version
	• Extreme 8520 • Extreme 8720				

Table 5: TPVM Software Support

TPVM Version	SLX-OS 20.2.3 d/e/f	SLX-OS 20.3.2	SLX-OS 20.3.2a	SLX-OS 20.3.2b	SLX-OS 20.3.2c	SLX-OS 20.3.2d	SLX-OS 20.3.4/4a	SLX-OS 20.4.1	SLX-OS 20.4.1b	SLX-OS 20.4.2/2a	Ubuntu Version	EFA Version
4.2.4	Yes	No	No	No	No	No	No	No	No	No	18.04	2.4.x
4.2.5	No	Yes	Yes	No	No	No	No	No	No	No	18.04	2.4.x, 2.5.0
4.2.5	No	No	No	Yes	No	No	No	No	No	No	18.04	2.5.1, 2.5.2
4.2.5	No	No	No	No	Yes	No	No	No	No	No	18.04	2.5.3
4.3.0	No	No	No	No	No	Yes	No	No	No	No	18.04	2.5.4, 2.5.5
4.4.0	No	No	No	No	No	No	Yes	No	No	No	18.04	2.6.0, 2.6.1
4.5.0	No	No	No	No	No	No	No	Yes	No	No	18.04	2.7.0
4.5.1	No	No	No	No	No	No	No	No	Yes	No	18.04	2.7.2
4.5.3	No	No	No	No	No	No	No	No	No	Yes (only with 20.4.2)	18.04	3.0.0
4.5.6	No	No	No	No	No	No	No	No	No	Yes	20.04	3.1.0

Note

The seamless TPVM upgrade feature is not available in SLX 20.2.3f.

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	✔			✔	

Table 6: IP Fabric Topology Matrix (continued)

Device	SLX-OS Release	Leaf	Spine	Super Spine	Border Leaf	Small DC Fabric
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	✔			✔	✔

Table 7: EFA, Neutron, and SLX-OS Compatibility

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: • CPU: 4 cores • Storage: 128 GB • RAM: 8 GB Recommended: • CPU: 16 cores • Storage: 200 GB • RAM: 32 GB
3.2.0	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 9: OVA Deployment Models

XCO Version	Ubuntu Version	Virtual Machine
3.1.x	18.04	Minimum: • CPU: 4 cores • Storage: 64 GB • RAM: 8 GB
3.2.0	18.04	Minimum: • CPU: 4 cores • Storage: 64 GB

Table 9: OVA Deployment Models (continued)

XCO Version	Ubuntu Version	Virtual Machine
		• RAM: 8 GB

Table 10: 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

EFA Upgrade Prerequisites

Prerequisites for EFA upgrade process with the default gateway changed:

1. Ensure that no DNS configuration exists under TPVM config and resolve.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 bundled with EFA 2.6.1 will not automatically modify the above mentioned parameters.

Known Limitations

Known Limitations in EFA

This topic covers several caveats and limitations when using Extreme Fabric Automation.

Provided VNI: 1006 already consumed in fabric

Symptom	Condition	Workaround
Endpoint group (EPG) create fails with VNI resource not being available in the fabric.	Run EPG create, delete, and re-create CLI in quick succession: 1. Create EPG or Networks with user-provided VNI parameter. 2. Delete the EPG. 3. Create the EPG again with the same parameters as in step 1.	Provide a wait of 30 seconds between the create and delete CLI on the same EPG.

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.

vrf_route_target_mapping error while creating EPG (after VRF delete)

Symptom	Condition	Workaround
When VRF is added and deleted to or from and Endpoint Group, in quick succession, multiple times, events received from inventory service can get interleaved with the commands. This causes EFA command execution path to find database entries that are yet to be deleted due to previous command run.	Issue is observed when **`vrf-add`** and **`vrf-delete`** operations are run multiple times on Endpoint Group in quick succession.	Wait for a few minutes before running the **`vrf-add`** again on Endpoint Group.

Inventory device update fails to change device table router-ip field

Symptom	Condition	Workaround
If the router-id is changed on the device (add, delete, or modified), the device table router-ip field does not change after you do inventory device update.	It is found that inventory did detect the diff and generate the RouterBgpUpdatedMsg to Tenant. Tenant did not handle this message.	Add hook in the RouterBgpUpdatedMsg on tenant handler to set the RouterIP. This enables the tenant DB to have the same value with the device after update.

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

Symptom	Condition	Workaround
EFA shows the following message after a tenant user with RBAC logs in to the system: Please type this in your shell: `export EFA_TOKEN=eyJhbGciOiJSUzI1NiIsImtpZCI6IjEuMCIsInR5cCI6IkpXVCJ9.eyJjb21tb25fbmFtZSI6IkVGQSBUb2tlbiBTZXJ2aWNlIiwidWFzIjpbeyJ0YXJnZXQiOiJFRkEiLCJyb2xlIjoiVlIyLVRudEFkbWluIn1dLCJvcmciOiJFeHRyZW1lIE5ldHdvcmtzIiwidmVyIjoiMS4wIiwiaWQiOiIiLCJleHAiOjE2NDUyNDcxNDIsImp0aSI6IjZjMjA4ZDUxLTkwNzgtMTFlYy1iZjk5LWNhNzk1MDY1YzIwNyIsImlhdCI6MTY0NTE2MDc0MiwiaXNzIjoiRUZBIFRva2VuIFNlcnZpY2UiLCJuYmYiOjE2NDUxNjA3NDIsInN1YiI6InVzZXIyIn0.b7m5PINijeEdNSqnTeE2ZhUrqKLKQAu079vXyBIdgHbXKt9ULfa03vMU1jfBO1qFb1-x0oHmsAQ0pSsF5JLeMaMzMflLf78ktZO8U5IePq72vM5en35IR-DNLyoGIZBeFeG6ZbBMoETzz5vf9OuefgQID3YdjcALr7yllCgDmLVFlgson77yCBpkTK15xm1GRbtL7JKXZzShBE7E3kdW7N71MdM85Gc3r4l-c8sfz7eo06gKrfTq9wXCv4_LVzR6-KRSg6NyLq363WEpcK1A2Hs0Wo3T9TpquYHNaCWA5I1QTsG-RHFdg4kxZP2fQpUp6Bgy1s6k59PVPn4-M-a8lA— Time Elapsed: 4.619465187s —`	When a user is created with the default login shell as sh.	EFA supports only bash shell for login or any other CLI commands.

EFA 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 XVM

This topic describes several caveats and limitations that you must follow when using the Extreme Visibility Manager (XVM).

LAG created when port channel deployment fails

Any changes to the Visibility Manager 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.

Egress group configuration cannot be updated during migration

During the migration of MLX configuration to an Extreme 9920 device, you cannot change the configuration of an egress group. After migration is complete, you can change the configuration on the Extreme 9920 device, including the mapping of multiple egress to an egress group.

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 Extreme Visibility Manager Administration and User Guide, 6.1.0.

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.

- 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 Extreme Visibility Manager Administration and User Guide, 6.1.0.

A device can be managed by only one instance of VM

Before adding a device, ensure that it is not managed by any other instance of Visibility Manager. For more information, see Extreme Visibility Manager Administration and User Guide, 6.1.0.

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.

LACP LAG is not supported for Extreme 9920 devices

Although the option to select LACP LAG appears in the **Create Port Channel** page, the option is grayed out. Only static LAG is supported.

Only one region is supported

The Visibility Manager supports creation and management of only one region.

Defects Closed with Code Changes

The following defects were resolved in Extreme Fabric Automation 3.1.1.

Parent Defect ID:	EFA-16044	Issue ID:	EFA-16044
Product:	Extreme Fabric Automation	Reported in Release:	EFA 3.1.0
Symptom:	Firmware upgrade of MLX device is in continuous progress state		
Condition:	Execute the firmware upgrade on an MLX 32-slot device		

Parent Defect ID:	EFA-16060	Issue ID:	EFA-16060
Product:	Extreme Fabric Automation	Reported in Release:	EFA 3.1.0
Symptom:	EFA installer logs incorrect iptables location.		
Condition:	Observed in Ubuntu 20.x and newer versions.		

Parent Defect ID:	EFA-16065	Issue ID:	EFA-16065
Product:	Extreme Fabric Automation	Reported in Release:	EFA 3.1.0

Symptom:	Error messages shown in XCO GUI "Something went wrong" is giving the wrong information to costumers when ports are not reachable.
Condition:	When the port 8078 is not reachable, XCO is giving wrong error in GUI which is misleading to customer.

Parent Defect ID:	EFA-16074	Issue ID:	EFA-16074
Product:	Extreme Fabric Automation	Reported in Release:	EFA 3.1.0
Symptom:	SLX 9140/9240 devices are in continuous progress state when discovered in XCO 3.1		
Condition:	CLI Parsing of policy causing the panic issue in XCO due to which the device will be in continuous progress state.		

Parent Defect ID:	EFA-16077	Issue ID:	EFA-16077
Product:	Extreme Fabric Automation	Reported in Release:	EFA 3.1.0
Symptom:	With XCO 3.1, not able to discover the 9920 NPB device.		
Condition:	If the 9920 NPB device is running with software version 21.1.2.4, XCO 3.1 is not able to discover the device.		

Defects Closed without Code Changes

No defects were closed without code changes in this release of the software.

Open Defects

The following defects are open in Extreme Fabric Automation 3.1.1.

Parent Defect ID:	XCO-3438	Issue ID:	XCO-3438
Product:	XCO	Reported in Release:	EFA 2.7.0
Symptom:	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.		
Condition:	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.		

Workaround:	Execute the commands sequentially.
Recovery:	EFA database and SLX device configurations are not always affected by this error and hence no recovery is required. The failed commands shall be rerun sequentially to successful completion of the expected operations.

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

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. Execute "efa inventory drift-reconcile execute --ip <device-ip>".		
Recovery:	Manually reconfigure the removed configurations from the device.		

Parent Defect ID:	XCO-3448	Issue ID:	XCO-3448
Product:	XCO	Reported in Release:	EFA 3.0.0
Symptom:	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).		

Condition:	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.
Recovery:	Execute "efa fabric configure --name <fabirc-name>" so that the superspine devices move to cfg-in-sync state.

Parent Defect ID:	XCO-3460	Issue ID:	XCO-3460
Product:	XCO	Reported in Release:	EFA 2.5.5
Symptom:	kubernetes command k3s kubectl get pods -n efa will show some pods in "ImagePullBackOff" state.		
Condition:	when node Disk Space is full and pods are in evicted state, after freeing up space and executing efactl start or on next restart of pod.		
Workaround:	Check for expected Disk space as mentioned in system requirements.		
Recovery:	1. Check if we have enough disk space as mentioned in system requirements, 2. On the install dir , change to docker_images and import the images using following command: k3s ctr image import docker_k3s_images.tar 3. 3. Execute efactl start		

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.		

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:	EFA-4127	Issue ID:	EFA-4127
Product:	Extreme Fabric Automation	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:	NA		

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 is correctly populated from UI so that configuration will not fail on device.		
Recovery:	Login to SLX CLI and delete the given port channel and refresh configuration on XCO UI.		

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.
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:	NA

Parent Defect ID:	XCO-4136	Issue ID:	XCO-4136
Product:	XCO	Reported in Release:	EFA 3.1.0
Symptom:	The intermediate session expired popup in the XCO user interface.		
Condition:	When the user session is active for one hour, the user will see a session expiry popup.		
Workaround:	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.		
Recovery:	The user has to click OK on the popup and the user session will be reauthenticated automatically.		

Parent Defect ID:	XCO-4139	Issue ID:	XCO-4139
Product:	XCO	Reported in Release:	EFA 2.7.2
Symptom	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.		
Recovery:	1. Disable the LLDP protocol under the interfaces ethernet 0/x on D1 and ethernet 0/y on D2. 2. Execute "efa inventory device update --ip <device-ip>" for both D1 and D2. 3. Execute "efa fabric configure --name <fabric-name>".		

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.		

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:	Execute "efa inventory drift-reconcile execute --ip <device-ip> --reconcile" on the devices which are in cfg-refresh-err state.

Parent Defect ID:	XCO-4154	Issue ID:	XCO-4154
Product:	XCO	Reported in Release:	EFA 2.7.2
Symptom:	Fabric devices continue to remain in cfg-refresh-err state even though the links between the MCT pair are brought up after the reload.		
Condition:	1. Configure a single rack (MCT Pair) Non-CLOS fabric with the SLX devices. 2. All links between the MCT pair are brought down. 3. "efa fabric show" output indicates the devices with the app-sate set as "cfg-refresh-err". 4. Reload the SLX devices. 5. There are connectivity issues towards the SLX from EFA after reload.		
Recovery:	1. Fix the network connectivity issue between EFA and the SLX devices. 2. Execute "lldp disable" followed by "lldp enable" under the physical interfaces interconnecting the MCT pair. 3. Execute "efa inventory device update --ip <device-ip>" on the MCT pair.		

Parent Defect ID:	XCO-4155	Issue ID:	XCO-4155
Product:	XCO	Reported in Release:	EFA 3.1.0
Symptom:	Renewal of K3s server certificate fails after a time-shift.		
Condition:	K3s CA certificate has been renewed and immediately K3s server certificate renewal is tried again.		
Workaround:	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.		

	XCO-4156	Issue ID:	XCO-4156
Parent Defect ID:	XCO	Reported in Release:	EFA 3.1.0

Symptom:	Port-group add operation on a Layer-3 EPG of a bridge-domain enabled tenant that shares ctag with other EPGs may fail. on certain conditions with the error: Device: <device-1-IP> Ctag: <ctag> Anycast <IP-1> subnet is conflicting with already configured Ve 4097 : Anycast <IP-1> on the device <device-1>
Condition:	1. Configure two layer-3 EPGs with shared ctags and with ports from different SLX devices that are connected as MCT pair. 2. Do an EPG port-group-delete update operation on one EPG to remove all its ports. 3. Re-add the same ports back to the EPG. The step 3 will fail with the symptom mentioned above.
Workaround:	Ensure that the layer-3 EPGs that share ctags are provisioned with all the ports upfront at the time of EPG create time itself.
Recovery:	None

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

Parent Defect ID:	XCO-4164	Issue ID:	XCO-4164
Product:	XCO	Reported in Release:	EFA 3.1.0
Symptom:	Syslog messages are not seen for SLX (NPB) devices in the XCO user interface.		
Condition:	When the SLX device already has a secured Syslog configuration and then discovers the same device in XCO.		
Workaround:	Clear the secured Syslog configuration on the SLX NPB device before discovering it in XCO.		
Recovery:	Clear the secured Syslog configuration on the SLX NPB device and rediscover the device.		

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

	XCO-4168	Issue ID:	XCO-4168

Parent Defect ID:			
Product:	XCO	Reported in Release:	EFA 3.1.0
Symptom:	Ingress group is not updating correctly on NPB device version 21.1.2.3		
Condition:	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.		
Workaround:	Delete ingress group with inner/outer tunnel information and add it back with updated configuration.		
Recovery:	Delete ingress group with inner/outer tunnel information and add it back with updated configuration.		

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

Parent Defect ID:	XCO-4174	Issue ID:	XCO-4174
Product:	XCO	Reported in Release:	EFA 3.1.0
Symptom:	For fabric installation, the tenant user logout displays an error message related to the permission.		
Condition:	Perform logout for a user having a dynamic tenant administrator role.		
Recovery:	The user can ignore the error message as the user will be logged out successfully in spite of the error.		

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

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.