Extreme Fabric Automation Release Notes

3.0.1

9037508-01 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/

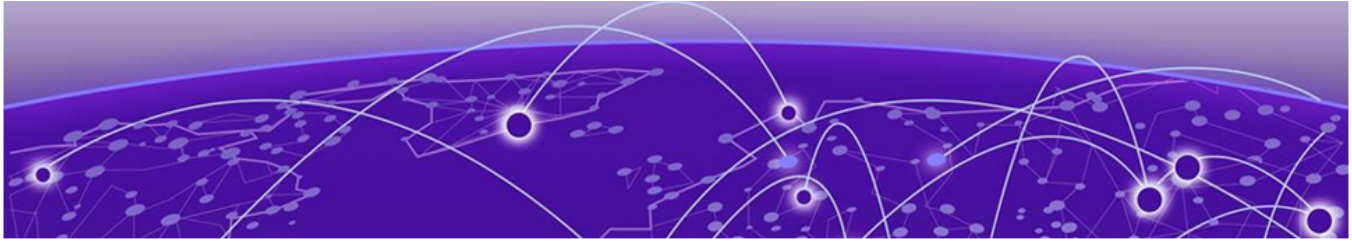
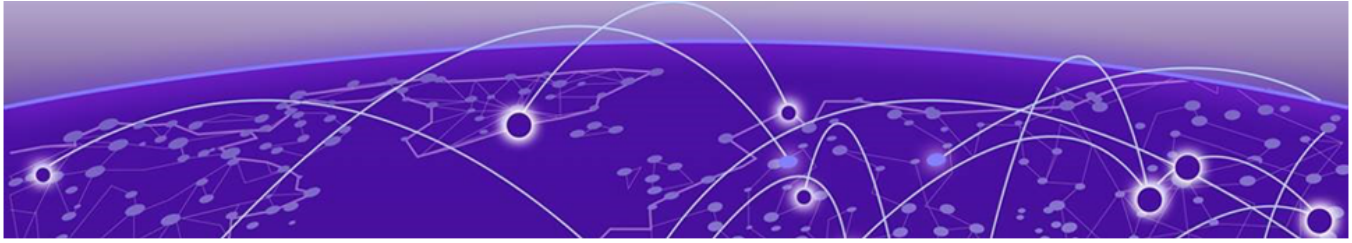


Table of Contents



Release Notes

Supported Platforms and Deployment Models

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

Table 1: Bare Metal Deployment Models

EFA Version	Deployment	Managed SLX Devices	Multi-Fabric Support	Ubuntu Version	Server Requirements
2.6.x, 2.7.x, 3.0.0, 3.0.1	External server (bare metal)	More than 24	Yes	16.04 and 18.04	• CPU: 4 cores • Storage: 50 GB • RAM: 8 GB

Table 2: OVA Deployment Models

EFA Version	Deployment	Managed SLX Devices	Multi-Fabric Support	Ubuntu Version	Server Requirements
2.6.x (Secure mode), 2.7.x, 3.0.0, 3.0.1	External server (OVA)	More than 24	Yes	18.04	• CPU: 4 cores • Storage: 50 GB • RAM: 8 GB

Table 3: TPVM Deployment Models

EFA Version	TPVM Deployment	Managed SLX Devices	Multi-Fabric Support	Ubuntu Version	Minimum SLX-OS Version
2.6.x	• SLX 9150 • SLX 9250 • SLX 9740 • Extreme 8520 • Extreme 8720	Up to 24	Yes	18.04	20.3.4
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	Up to 24	Yes	18.04	20.4.2

Table 3: 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 4: TPVM Software Support

TPVM Version	SLX-OS 20.2.3d/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	SLX-OS 20.4.2ab	Ubuntu Version	EFA Version
4.2.4	Yes	No	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	No	18.04	2.4.x, 2.5.0
4.2.5	No	No	No	Yes	No	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	No	18.04	2.5.3
4.3.0	No	No	No	No	No	Yes	No	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	No	18.04	2.6.0, 2.6.1
4.5.0	No	No	No	No	No	No	No	Yes	No	No	No	18.04	2.7.0
4.5.1	No	No	No	No	No	No	No	No	Yes	No	No	18.04	2.7.2
4.5.3	No	No	No	No	No	No	No	No	No	Yes	No	18.04	3.0.0
4.5.6	No	No	No	No	No	No	No	No	No	No	Yes	18.04	3.0.1

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

Table 5: IP Fabric Topology Matrix

Device	SLX-OS Release	Leaf	Spine	Super Spine	Border Leaf	Small DC Fabric
SLX 9150	20.1.x, 20.2.x, 20.3.x, 20.4.x	✔				✔
SLX 9250	20.1.x, 20.2.x, 20.3.x, 20.4.x	✔	✔	✔		✔
SLX 9540	20.1.x, 20.2.x, 20.3.x, 20.4.x	✔			✔	
SLX 9640	20.1.x, 20.2.x, 20.3.x, 20.4.x				✔	

Table 5: IP Fabric Topology Matrix (continued)

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

Table 6: 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

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

Note the following caveat for this release of Extreme Fabric Automation.

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

Defects Closed with Code Changes

The following defects, which were previously disclosed as open, were resolved in Extreme Fabric Automation 3.0.1.

Parent Defect ID:	EFA-15472	Issue ID:	EFA-15472
Severity:	S2 – Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 3.0.0
Symptom:	Supportsave has incomplete log files or missing information.		
Condition:	When user is logged in to efa through command line, then supportsave should have valid content for the device locks and running configuration.		

Parent Defect ID:	EFA-15691	Issue ID:	EFA-15691
Severity:	S1 – Critical		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 3.0.0
Symptom:	No resources found in efa namespace		
Condition:	After a double fault or active reload after reboot of standby		

Parent Defect ID:	EFA-16008	Issue ID:	XCO-4182
Severity:	S3 – Medium		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 3.0.0
Symptom:	RabbitMQ logs from terminated instances are not being purged or archived via logrotate		
Condition:	Cleanup older rabbitmq pod logs which are present after failover. This cleanups logs that are not from the current running pod, older than 5 days.		
Workaround:	Delete the rabbitmq logs manually at /apps/efa_logs/rabbitmq/ on TPVM and /var/log/efa/rabbitmq/ on server.		

Open Defects

The following defects are open in Extreme Fabric Automation 3.0.1.

Parent Defect ID:	EFA-9570	Issue ID:	EFA-9570
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.0

Parent Defect ID:	EFA-9570	Issue ID:	EFA-9570
Symptom:	Add Device Failed because ASN used in border leaf showing conflict		
Condition:	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		
Workaround:	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		
Recovery:	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.		

Parent Defect ID:	EFA-10062	Issue ID:	EFA-10062
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.0
Symptom:	Removing a device from Inventory does not clean up breakout configuration on interfaces that are part of port channels.		
Condition:	This condition occurs when there is breakout configuration present on device that is being deleted from Inventory, such that those breakout configurations are on interfaces that are part of port-channels		
Workaround:	Manually remove the breakout configuration, if required.		
Recovery:	Manually remove the breakout configuration, if required.		

Parent Defect ID:	EFA-10063	Issue ID:	EFA-10063
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.0
Symptom:	Deleting device from EFA Inventory does not bring up the interface to admin state 'up' after unconfiguring breakout configuration		
Condition:	This condition occurs when there is a breakout configuration present on the device that is being deleted from EFA Inventory		

Parent Defect ID:	EFA-10063	Issue ID:	EFA-10063
Workaround:	Manually bring the admin-state up on the interface, if required		
Recovery:	Manually bring the admin-state up on the interface, if required		

Parent Defect ID:	EFA-12784	Issue ID:	EFA-12784
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.7.0
Symptom:	After fabric configure if lldp links on slx devices are manually made no shut, "efa fabric debug config-gen-reason --name <fabric-name> --device <device-ip>" will display added entries for device. After sometime even if devices are shown as cfg-in-sync in "efa fabric show", "efa fabric debug config-gen-reason --name <fabric-name> --device <device-ip>" will display the added lldp entries. Again if other lldp links of the same device are added, "efa fabric debug config-gen-reason <>" command will display the previously added entries along with the newly added lldp entries.		
Condition:	1) Create and configure clos/non-clos fabric 2) Add new lldp links between any two devices of the fabric 3) Execute "efa inventory device update", followed by "efa fabric show" and "efa fabric debug config-gen-reason" 4) Again add new lldp links between the same devices of the fabric 5) Execute "efa inventory device update", followed by "efa fabric show" and "efa fabric debug config-gen-reason" 6) LLDP entries added in both step (2) and step (4) are displayed in "efa fabric debug config-gen-reason"		
Recovery:	The inconsistency between the output of "efa fabric show" and "efa fabric debug config-gen-reason" has no functional impact. Subsequent execution of "efa fabric configure" command will bring the consistency in the outputs.		

Parent Defect ID:	EFA-12792	Issue ID:	EFA-12792
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.7.0
Symptom:	Considering D1 and D2 are the connected fabric devices when the "ip address" configuration is removed from a fabric interface of D1, the device D2 will be marked as cfg-refreshed		

Parent Defect ID:	EFA-12792	Issue ID:	EFA-12792
Condition:	Below are the steps to reproduce the issue: 1) D1 and D2 are the connected fabric devices. "ip address" configuration from a fabric interface is removed manually from the fabric device D1 2) Trigger DRC on the device D1 or re-configure the ip address (removed in step 1) on the fabric device D1 3) Fabric device D2 connected to the device D1 will move to cfg-refreshed state		
Workaround:			
Recovery:	Either wait for auto-update or manually perform inventory update. CLI to perform manual recovery "efa inventory device update --ip <remoted-device-ip>" Note: The app state of the device D2 will be marked as cfg-in-sync in the subsequent cycle of inventory device update which is auto-triggered every 30 minutes.		

Parent Defect ID:	EFA-13124	Issue ID:	EFA-13124
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	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 can 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 can 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 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		

Parent Defect ID:	EFA-13171	Issue ID:	EFA-13171
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.7.0

Parent Defect ID:	EFA-13171	Issue ID:	EFA-13171
Symptom:	After fabric configure, when neighbor device goes down or comes up, based on how other devices are connected to it, events are triggered on the affected (connected) devices where few validations are done and errors if found are stored for each device. These errors can be seen in "efa fabric error show --name <fabric-name>" output. If DRC is performed on any of these devices having errors and if drift and reconcile are success, then the device will be shown as cfg in-sync state in "efa fabric show" output but errors will continue to exist for the device in "efa fabric error show" output Note: The inconsistency between the output of "efa fabric show" and "efa fabric error show" has no functional impact.		
Condition:	1) Create and configure clos 2) Bring one of the leaf node down (i.e. reload the device) 3) The affected (connected) devices will move to 'cfg refresh error' that can be seen in "efa fabric show" output and the actual errors can be seen in "efa fabric error show --name <fabric-name>" output 4) Perform DRC with reconcile option on one of the device in 'cfg refresh error' by executing "efa inventory drift-reconcile execute --ip <deviceIP> --reconcile" 5) If DRC is succeeds, then the "efa fabric show" output displays the above device (which was in 'cfg refresh error' state) in "cfg in-sync" state and "efa fabric error show" output will continue to display the errors that were seen for the same device in step (3)		
Recovery:	Subsequent execution of "efa fabric configure" command will bring consistency in the outputs.		

Parent Defect ID:	EFA-13178	Issue ID:	EFA-13178
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.7.0
Symptom:	Fabric configuration failed to reconcile when DRC was on-going and user initiated a EFA backup		
Condition:	EFA's backup needs to stop services to ensure that the database is in quiet state, so that the backup is consistent.		
Workaround:	Users should run a backup after the devices are completed going through DRC		
Recovery:	Recovery would be to run DRC operation on that device again after the backup is completed.		

Parent Defect ID:	EFA-13339	Issue ID:	EFA-13339
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.7.0

Parent Defect ID:	EFA-13339	Issue ID:	EFA-13339
Symptom:	The EFA notification service does not send a syslog alert message when an EFA inventory device firmware-download operation fails.		
Condition:	The user attempts to prepare a device for a firmware download using "efa inventory device firmware-download prepare add --ip <device IP>" when the device's management connectivity is unreachable.		
Workaround:	Although the syslog alert message is not available, both the CLI and REST response contain an appropriate error message about the reason for the firmware-download prepare error and the device's connectivity issue.		
Recovery:	None		

Parent Defect ID:	EFA-14289	Issue ID:	EFA-14289
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 3.0.0
Symptom:	When BGP or Static Prefix Independent Convergence is configured as disabled, Drift and Reconcile will not address a drifted state.		
Condition:	The condition is that Prefix Independent Convergence is configured as the default value of disabled on EFA, but the SLX has drifted off of the default value into enabled.		
Workaround:	Prefix Independent Convergence reconcile failure can be worked around by configuring as enabled or by avoiding configuring SLX manually off of the default disabled state.		
Recovery:	Prefix Independent Convergence drift must be reconciled on the SLX device.		

Parent Defect ID:	EFA-14407	Issue ID:	EFA-14407
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	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)		

Parent Defect ID:	EFA-14407	Issue ID:	EFA-14407
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 <fabric-name>" so that the superspine devices move to cfg-in-sync state		

Parent Defect ID:	EFA-14474	Issue ID:	EFA-14474
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 3.0.0
Symptom:	During the device removal from fabric, the ip and ipv6 access-list configurations are not removed from the device		
Condition:	Below are the steps to reproduce the issue: 1) Configure 5-stage CLOS fabric 2) Create EPG of type port-profile on the spine/super spine devices along with port-profile ACLs 3) Remove spine/super spine device from fabric		
Recovery:	Manually remove the stale ip/ipv6 ACLs from the device		

Parent Defect ID:	EFA-14667	Issue ID:	EFA-14667
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 3.0.0
Symptom:	In a 5-stage clos, if border-leaf is not connected to super-spine and it is connected to one/more spine devices, validation succeeds without any error and fabric comes up		

Parent Defect ID:	EFA-14667	Issue ID:	EFA-14667
Condition:	1) Create a 5-stage clos fabric with border-leaf node connected to one/ more spine devices and not connected to super-spine node 2) Configure fabric		
Recovery:	Separate the bordel-leaf from spine pod and connect directly to the super-spine pod		

Parent Defect ID:	EFA-14687	Issue ID:	EFA-14687
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	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:	EFA-14283	Issue ID:	EFA-14283
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 3.0.0
Symptom:	When the BGP peers are created with update source IPv6 values that are not in a compressed format or which have capitals in them (Example: fd00:1:950::A and fd00:1:950::0) followed by the execution of the DRC, then the bgp peers transition to cfg-refreshed state		
Condition:	Steps to reproduce: 1. Create a bgp peer with update source ip in non compressed format or with capitals 2. Do an inventory DRC with drift only 3. The bgp peers get into a refreshed state because of the update source ip mismatch		

Parent Defect ID:	EFA-14283	Issue ID:	EFA-14283
Workaround:	Create the bgp peers with compressed update source ips and without capitals		
Recovery:	Delete the bgp peer through EFA and recreate it through EFA using compressed update source ips and without capitals		

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.