Extreme Fabric Automation Release Notes

2.6.0

9037267-00 Rev AC
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/

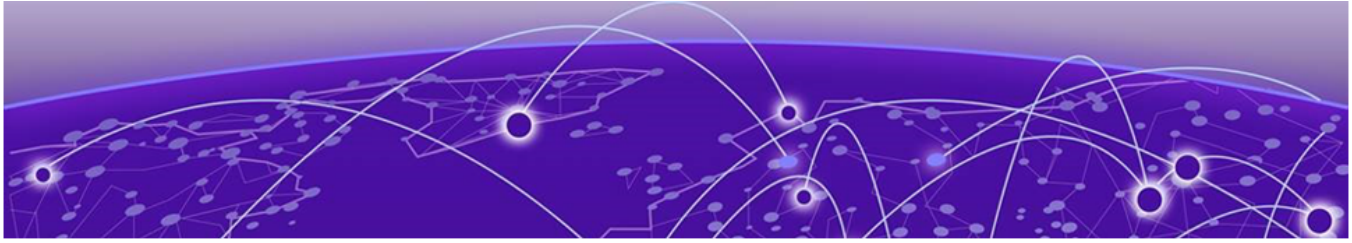

Table of Contents

Release Notes

New In This Release

Extreme Fabric Automation 2.6.0 provides the following features and improvements.

Table 1: Features and Improvements

Feature	Description
Non-Clos Topology: Dynamic ICL	Describes procedure to configure dynamic Inter-Chassis Link (ICL) in small data centers. For more information, see the Extreme Fabric Automation Administration Guide, 2.6.0.
IP prefix list and route map features	Describes procedure to configure IP prefix list and route map. For more information, see the Extreme Fabric Automation Administration Guide, 2.6.0.
IP prefix list and route map features	Update the topic with Policy Service introduction. For more information, see the Extreme Fabric Automation Administration Guide, 2.6.0.
IP prefix list and route map features	Updated the service list with Policy Service. For more information, see the Extreme Fabric Automation Administration Guide, 2.6.0.

Table 1: Features and Improvements (continued)

Feature	Description
BGP Peer: IP prefix list and route map	Describes procedure to configure route map attributes. For more information, see the Extreme Fabric Automation Administration Guide, 2.6.0.
VRF: Advertise Address VRF: Advertise Static-Network VRF: Advertise Aggregate Address	Decribes procedure to configure Advertise Network, Static- Network and Aggregate Address on Tenant VRF. For more information, see the Extreme Fabric Automation Administration Guide, 2.6.0.
BGP Peer/Peer-Group: remove-private-as and default-originate	Describes procedure to configure remove-private-as and default-originate on BGP Peer and Peer- Group. For more information, see the Extreme Fabric Automation Administration Guide, 2.6.0.
5-stage Clos Solution Validation	Updated with 5-stage Clos fabric topology diagram. For more information, see the Extreme Fabric Automation Administration Guide, 2.6.0.
IP Pprefix list and route map features	Updated the topic with Drift and Reconcile (DRC), Idempotency for IP prefix list and route map configurations. For more information, see the Extreme Fabric Automation Administration Guide, 2.6.0.
Support to configure BGP dynamic listen-limit value to '1024' from EFA	Updated the topic with the BGP dynamic listen-limit value. For more information, see the Extreme Fabric Automation Administration Guide, 2.6.0.
EFA login to the switch with different user names triggering as a security violation on the switch	Updated the topic with a step to install the certificates on devices. For more information, see the Extreme Fabric Automation Administration Guide, 2.6.0.
Multi Node: VIP hostname change failed to change log server on the device post completion	Updated the topic with a note. For more information, see the Extreme Fabric Automation Administration Guide, 2.6.0.

For more information, see Defects Closed with Code Changes on page 8.

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 2: Bare Metal Deployment Models

EFA Version	Deployment	Managed SLX Devices	Multi-Fabric Support	Ubuntu Version	Server Requirements
2.4.x, 2.5.x, and 2.6.x	External server (bare metal)	More than 24	Yes	16.04 and 18.04	• CPU: 4 cores • Storage: 50 GB • RAM: 8 GB

Table 3: OVA Deployment Models

EFA Version	Deployment	Managed SLX Devices	Multi-Fabric Support	Ubuntu Version	Server Requirements
2.4.x, 2.5.x, 2.6.x (Secure mode)	External server (OVA)	More than 24	Yes	18.04	• CPU: 4 cores • Storage: 50 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
2.4.x	• SLX 9150 • SLX 9250 • SLX 9740	Up to 24	Yes	18.04	20.2.2b
2.5.x	• SLX 9150 • SLX 9250 • SLX 9740	Up to 24	Yes	18.04	20.2.3.f
2.6.x	• SLX 9150 • SLX 9250 • SLX 9740	Up to 24	Yes	18.04	20.3.4

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 20.2.3d/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	Ubuntu Version	EFA Version
4.2.4	Yes	No	No	No	No	No	No	18.04	2.4.x
4.2.5	No	Yes	Yes	No	No	No	No	18.04	2.4.x, 2.5.0
4.2.5	No	No	No	Yes	No	No	No	18.04	2.5.1, 2.5.2
4.2.5	No	No	No	No	Yes	No	No	18.04	2.5.3
4.3.0	No	No	No	No	No	Yes	No	18.04	2.5.4, 2.5.5
4.4.0	No	No	No	No	No	No	Yes	18.04	2.6.0

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	20.1.x, 20.2.x, 20.3.x	✔				✔
SLX 9250	20.1.x, 20.2.x, 20.3.x	✔	✔	✔		✔
SLX 9540	20.1.x, 20.2.x, 20.3.x	✔			✔	
SLX 9640	20.1.x, 20.2.x, 20.3.x				✔	
SLX 9740	20.2.x, 20.3.x		✔	✔	✔	✔

Table 6: IP Fabric Topology Matrix (continued)

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

Known Limitations

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

- When the backup routing is enabled at the fabric level, the backup routing BGP neighbors are automatically created by the EFA during the creation of VRF on the SLX devices. User will not be able to enable route-map and other BGP attributes on the backup routing BGP neighbors.
- 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 2.6.0.

Parent Defect ID:	EFA-5592	Issue ID:	EFA-5592
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.2.0
Symptom:	Certificates need to be manually imported on replaced equipment in-order to perform RMA.		

Parent Defect ID:	EFA-5592	Issue ID:	EFA-5592
Condition:	RMA/replaced equipment will not have ssh key and auth certificate, in-order to replay the configuration on new switch user needs to import the certificates manually.		
Workaround:	import certificate manually efa certificates device install --ips x,y --certType		

Parent Defect ID:	EFA-8297	Issue ID:	EFA-8297
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.4.0
Symptom:	EPG update anycast-ip-delete operation succeeded for deletion of provisioned anycast-ip for admin-down device. This issue is observed only if an update anycast-ip-add operation is performed after device is put in admin down state and the new config is in non-provisioned state followed by anycast-ip-delete operation for already configured anycast-ip.		
Condition:	Steps to reproduce issue: 1) Configure EPG with anycast-ip (ipv4/ipv6) 2) Make one device admin-down 3) Anycast-ip update-add new anycast-ip (ipv6/ipv4) 4) Update-delete provisioned anycast-ip configured in step-1 (ipv4/ipv6) Step (4) should fail as IP is already configured on the device and trying to delete it should fail as part of APS.		
Workaround:	No workaround for this.		
Recovery:	Recovery can be done by configuring EPG again with the required configuration using efa or cleaning device config for anycast-ip on the switch.		

Parent Defect ID:	EFA-8448	Issue ID:	EFA-8448
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.4.0
Symptom:	When the ports provided by the user in “tenant update port-delete operation” contains all the ports owned by the port-channel, the PO goes into delete pending state. However, the ports are not deleted from the PO. They get deleted from the tenant though.		
Condition:	This issue is seen when the ports provided by the user in “tenant update port-delete operation” contains all the ports owned by the port-channel resulting in an empty PO.		

Parent Defect ID:	EFA-8448	Issue ID:	EFA-8448
Workaround:	User needs to provide ports for “tenant update port-delete operation” which do not result in an empty PO i.e. PO needs to have at least 1 member port.		
Recovery:	Add the ports back using "tenant port-add operation" so that the port-channel has at least 1 member port. The use "efa configure tenant port-channel" to bring the po back to stable state.		

Parent Defect ID:	EFA-9645	Issue ID:	EFA-9645
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.0
Symptom:	When the fabric setting is updated with this particular password "password$\n", md5 password doesn't get configured on the backup routing neighbors that was already created.		
Condition:	1. Configure fabric 2. Create tenant, po, vrf and epg 3. Update fabric setting with "password$\n" and configure fabric 4. MD5 password is not configured on backup routing neighbors under BGP address family ipv4/ipv6 vrf		
Workaround:	Update the fabric setting with any other password combination that does not include "$\n" combination.		
Recovery:	Update the fabric setting with any other password combination that does not include "$\n" combination.		

Parent Defect ID:	EFA-9813	Issue ID:	EFA-9813
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.4.3
Symptom:	When doing RMA of device the port connections for the new device must be identical.		
Condition:	New device's port connections were not identical to the device being RMAed.		
Workaround:	When doing RMA of device the port connections for the new device must be identical.		

Parent Defect ID:	EFA-9906	Issue ID:	EFA-9906
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.0

Parent Defect ID:	EFA-9906	Issue ID:	EFA-9906
Symptom:	When concurrent EFA tenant EPG create or update operation is requested where the commands involve large number of vlans and/or ports, one of them could fail with the error "EPG: <epg-name> Save for Vlan Records save Failed".		
Condition:	The failure is reported when concurrent DB write operation are done by EFA Tenant service as part of the command execution.		
Workaround:	This is a transient error and there is no workaround. The failing command can be executed once again and it will succeed.		
Recovery:	The failing command can be rerun separately and it will succeed.		

Parent Defect ID:	EFA-9952	Issue ID:	EFA-9952
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.0
Symptom:	When concurrent EFA tenant EPG delete operations are requested where the commands involve large number of vlans and/or ports, one of them could fail with the error "EPG network-property delete failed"		
Condition:	The failure is reported when concurrent DB write operation are done by EFA Tenant service as part of the command execution.		
Workaround:	This is a transient error and there is no workaround. The failing command can be executed once again and it will succeed.		
Recovery:	The failing command can be rerun separately and it will succeed		

Parent Defect ID:	EFA-9990	Issue ID:	EFA-9990
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.0
Symptom:	EPG update ctag-range-add operation with the existing ctag-range (i.e. ctag1, ctag2) and modified native vlan (ctag2) succeeds without any effect		

Parent Defect ID:	EFA-9990	Issue ID:	EFA-9990
Condition:	Below are the steps to reproduce the issue: 1. Create Endpoint group with ctag1, ctag2 and native vlan as ctag1 2. Update the Endpoint group (created in step 1) using ctag-range-add operation with the same set of ctags (i.e. ctag1, ctag2) and different native VLAN ctag2		
Workaround:	If user intends to modify the native vlan from ctag1 to ctag2 in an EPG, then the user will need to remove ctag1 (using ctag-range-delete) from the EPG and add ctag2 (using ctag-range-add) as native vlan to the EPG		

Parent Defect ID:	EFA-10371	Issue ID:	EFA-10371
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.1
Symptom:	Additional Route Target may be configured under VRF "address-family ipv6 unicast" device configuration when EPG update is performed with vrf-add operation on concurrent EPGs that use same VRF.		
Workaround:	No workaround		
Recovery:	Below are the steps to recover from the issue: 1. Delete VRF from all EndpointGroups by performing EPG Update <vrf-delete> operation 2. Add VRF to EndpointGroups by performing EPG Update <vrf-add> operation		

Parent Defect ID:	EFA-10377	Issue ID:	EFA-10377
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.1
Symptom:	Manual or Auto DRC can timeout on a scaled setup (when attempted soon after the fabric configure is success) with more number of Backup Routing enabled VRFs because EFA would start a mini DRC in the background (as soon as fabric configure is success) to provision the updated MD5 password on the Backup Routing neighbours.		

Parent Defect ID:	EFA-10377	Issue ID:	EFA-10377
Condition:	1. Configure non-clos fabric with backup-routing enabled. 2. Configure tenant, po, lot of vrf (e.g. 50), epgs, bgp peer-group, bgp static peers. 3. Configure maintenance-mode enable-on-reboot on the SLX. 4. Update fabric setting to configure MD5 password. 5. Configure fabric created in step 1 in order to provision MD5 password on Backup Routing neighbors for all the tenant VRFs. 6. Reload SLX to trigger MM triggered DRC or trigger manual DRC, as soon as the fabric configure is complete in step 5. 7. DRC will timeout since the provisioning of MD5 password on the Backup Routing neighbours was not allowed to be completed after step 5.		
Workaround:	1. Update MD5 password setting in fabric and configure fabric. 2. Allow MD5 password to get provisioned on all BR neighbors of all the tenant VRFs on the SLX. 3. Perform manual/auto DRC once MD5 password is provisioned.		
Recovery:	Manual or Auto DRC can be reattempted again once the fabric MD5 password is provisioned on all Backup Routing neighbors for all tenant VRFs.		

Parent Defect ID:	EFA-10397	Issue ID:	EFA-10397
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.0
Symptom:	Native Vlan gets added as trunk VLAN to ports/ port channels after DRC is executed		
Condition:	1. Create EPG1 with PO1 and switchport mode trunk with native VLAN V1. 2. Create EPG2 with the same PO as used in step1 i.e. PO1 and new port channel PO2 . Switchport mode is configured as trunk without native VLAN. 3. Execute Manual/auto DRC . 4. Native VLAN V1 gets added as trunk VLAN to PO2, on the SLX.		
Recovery:	1.Introduce manual drift on SLX by executing "no switchport" on port channels which are not intended to have Native VLAN as trunk VLAN. 2.Perform manual/auto DRC. 3. After DRC execution only the required VLAN members will be added to the port-channel. Native VLAN will be removed from the not intended port channels		

Parent Defect ID:	EFA-10560	Issue ID:	EFA-10560
	S3 - Moderate		

Parent Defect ID:	EFA-10560	Issue ID:	EFA-10560
Severity:			
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.1
Symptom:	VRF goes to "vrf-device-srbfd-delete-pending" after the execution of vrf update static-route-bfd-add operation with invalid source IP or invalid destination IP.		
Condition:	1. Create VRF VRF1 and update VRF1 with static-route-bfd-add operation. 2. Provide the below payload with invalid IP address containing leading zeroes during static-route-bfd-add operation. --ipv4-static-route-bfd 10.20.61.92,214.5.94.13,214.5.94.02,300,300,3 3. static-route-bfd-add operation fails due to invalid IP and the rollback (delete) operation also fails due to the invalid IP further resulting in "vrf-device-srbfd-delete-pending" state of the VRF.		
Workaround:	Any IP Address with leading zeroes (eg: 214.5.94.02) are not recommended to be provided as user input . The correct IP to be used is 214.5.94.2 instead of 214.5.94.02.		

Parent Defect ID:	EFA-10718	Issue ID:	EFA-10718
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.1
Symptom:	Non-existing connections between super-spines in EFA		
Condition:	If an endpoint of a connection (between 2 devices) is moved to a different device with the same port, the old connection remains as a stale entry in the EFA database. This condition occurs since the last device update by EFA but prior to handling any RASlog events which exhibits the non-existing connection.		
Workaround:	No Workaround		

Parent Defect ID:	EFA-10982	Issue ID:	EFA-10982
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.3
Symptom:	Efa inventory drift-reconcile history failed after reloading L01/L02		

Parent Defect ID:	EFA-11036	Issue ID:	EFA-11036
	S3 - Moderate		

Parent Defect ID:	EFA-11036	Issue ID:	EFA-11036
Severity:			
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.0
Symptom:	Error in ts-server.log "Error: Failed to fetch device information for device"		

Parent Defect ID:	EFA-11058	Issue ID:	EFA-11058
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.3
Symptom:	EFA API Documentation lists incorrect strings in REST responses which might not be updated with the actual response fields.		
Condition:	The API documentation is not updated.		
Recovery:	Fetch the correct values from the actual EFA REST response.		

Parent Defect ID:	EFA-11248	Issue ID:	EFA-11248
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.4

Parent Defect ID:	EFA-11248	Issue ID:	EFA-11248
Symptom:	Observation 1 : Delay for long : few nodes moved to cfg-refresh/cfg-refresh-error: 30 min after, auto device update helps to move Border-leaf states as “cfg-in-sync Again after 30 min, auto device update helps to move leaf states as “cfg-in-sync Again after 30 min, auto device update helps to move spine states as “cfg-in-sync Observation 2 : No change in spine config, shown as cfg-refresh Spine node lldp peer node leaf/border leaf validates, if the MCT link failure, spine node doesn’t get chance to move to 4th stage (as part of firmware download case /lldp) Observation 3 : B2 : Broder leaf non-selection group node went to cfg-refresh If lldp update is missed on peer nodes Border Leaf1, and the fabric got lldp on B2 which leads to failure on fabric operation. B2 node never gets an update event from inventory and there is no chance to compute fabric app/state update.		
Workaround:	Step1 : efa fabric error show --name stage3 Step2: execute Drift-only on error node (border MCT leaf) Step3: execute Drift-only on Leaf node Step4: execute Drift-only on Spine node [or] If the state is not moved from cfg-referesh, force to do DRC on the node.		

Parent Defect ID:	EFA-11520	Issue ID:	EFA-11520
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.2
Symptom:	The Dynamic BGP Listen-Limit is not configured on the Border_leaf nodes		

Parent Defect ID:	EFA-11739	Issue ID:	EFA-11739
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.5
Symptom:	EFA return success when configure 1GbpsAN speed on 100G switch port		

Parent Defect ID:	EFA-11770	Issue ID:	EFA-11770
	S3 - Moderate		

Parent Defect ID:	EFA-11770	Issue ID:	EFA-11770
Severity:			
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.5
Symptom:	EFA return 'invalid value' output for "Auto" set speed command		

Parent Defect ID:	EFA-11867	Issue ID:	EFA-11867
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.4
Symptom:	DRC timeout during SLX upgrade.		
Condition:	The logic that qualifies the start of a DRC during the firmware download workflow was incorrectly getting updated on an inventory service restart. This caused the "Drift Reconcile Start Timeout Failure" failure for device 21.144.144.201 (b144_BL1).		

Defects Closed without Code Changes

The following defects were closed in Extreme Fabric Automation 2.6.0.

Parent Defect ID:	EFA-10305	Issue ID:	EFA-10305
Reason Code:	Not Reproducible	Severity:	S2 - Major
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.4.2
Symptom:	EndpointGroup creation fail with error - "Device: <ip-address> has a VRF <vrf-name> configuration with different number of Static Routes"		
Workaround:	No workaround		
Recovery:	Below are the steps to recover from the issue: 1. Delete VRF from all EndpointGroups by performing EPG Update <vrf-delete> operation 2. Add VRF to EndpointGroups by performing EPG Update <vrf-add> operation		

Parent Defect ID:	EFA-10387	Issue ID:	EFA-10387
Reason Code:	Already Reported	Severity:	S2 - Major
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.1
Symptom:	-EFA OVA services not starting if no IP address is obtained on bootup.		

Parent Defect ID:	EFA-10387	Issue ID:	EFA-10387
Condition:	When EFA OVA is deployed, and does not obtain a DHCP IP address, not all EFA services will start		
Workaround:	Configure static IP, or obtain IP address from DHCP. cd /opt/godcapp/efa type: source deployment.sh When the EFA installer appears, select Upgrade/Re-deploy Select OK Select single node, Select OK Select the default of No for Additional management networks. Select yes when prompted to redeploy EFA. Once EFA has redeployed, all services should start		

Parent Defect ID:	EFA-10389	Issue ID:	EFA-10389
Reason Code:	Not Reproducible	Severity:	S3 - Moderate
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.1
Symptom:	When upgrade process is quit at any possible stage, older EFA stack doesn't get identified from the same node on which process has been initiated.		
Condition:	If user selects "No" when EFA asks for final confirmation before upgrade process gets started, the process gets terminated, but older stack can't be identified any longer on SLX. Checking "show efa status" reflects "EFA application is not installed. Exiting..." However there is no functional impact on EFA setup and EFA setup continues to work properly on TPVMs with existing version.		
Workaround:	Upgrade process can be initiated again from peer node		

Parent Defect ID:	EFA-10398	Issue ID:	EFA-10398
Reason Code:	Working as Designed	Severity:	S2 - Major
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.1
Symptom:	EFA Tenant REST Request fails with an error "service is not available or internal server error has occurred, please try again later"		
Condition:	Execution of the EFA Tenant REST requests which take more time (more than 15 minutes) to get completed		

Parent Defect ID:	EFA-10398	Issue ID:	EFA-10398
Workaround:	Execute "show" commands to verify if the failed REST request was indeed completed successfully. Re-execute the failed REST request as applicable.		
Recovery:	No recovery		

Parent Defect ID:	EFA-10778	Issue ID:	EFA-10778
Reason Code:	Insufficient Information	Severity:	S3 - Moderate
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.3
Symptom:	efa inventory device firmware-download prepare': 'Failed to prepare devices'		
Condition:			
Workaround:	Wait for FWDL to complete. We will lock out any modifications to the prepared list while a FWDL execution is in progress for the given fabric, even if it's a device that is not undergoing a FWD		
Recovery:			

Parent Defect ID:	EFA-10879	Issue ID:	EFA-10879
Reason Code:	Insufficient Information	Severity:	S3 - Moderate
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.3
Symptom:	switch hangs in MM mode		
Condition:	ssh rule is missing in iptables after maintenance mode reboot.		

Parent Defect ID:	EFA-10967	Issue ID:	EFA-10967
Reason Code:	Already Reported	Severity:	S2 - Major
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.3
Symptom:	Fabric-wide Firmware download will fail on timeout if the number of devices in the prepare group is greater than 5.		
Workaround:	The number of devices in the Fabric-wide Firmware download prepare group should be less than or equal to 5.		

Parent Defect ID:	EFA-11238	Issue ID:	EFA-11238
Reason Code:	Already Implemented	Severity:	S3 - Moderate
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.4

Parent Defect ID:	EFA-11238	Issue ID:	EFA-11238
Symptom:	Services restarted due to Kubernetes restarting. Kubernetes restarted because Mariadb was not ready for a while.		
Workaround:	Rebooting the node would fix this issue and cause Mariadb and Galera cluster to come up in the right states		
Recovery:	Rebooting the node should fix this issue, however there no better workaround at the moment		

Parent Defect ID:	EFA-11401	Issue ID:	EFA-11401
Reason Code:	Configuration/User Error	Severity:	S3 - Moderate
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.4
Symptom:	Execution error: 500 Internal Server Error after upgrade to 2.5.4		
Condition:	If invalid IP address are provided in virtual routes CLI.		

Parent Defect ID:	EFA-11421	Issue ID:	EFA-11421
Reason Code:	Configuration/User Error	Severity:	S3 - Moderate
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.4.6
Symptom:	EFA upgrade failed from 2.4.6 to 2.5.4 -Installation failed.		
Condition:	If old EFA installation was not complete		

Parent Defect ID:	EFA-11606	Issue ID:	EFA-11606
Reason Code:	Design Limitation	Severity:	S3 - Moderate
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.2
Symptom:	EFA in non operational state after SLX reboot during EFA upgrade		
Condition:	IF SLX is rebooted during EFA installation.		

Parent Defect ID:	EFA-11674	Issue ID:	EFA-11674
Reason Code:	Not a Software Defect	Severity:	S3 - Moderate
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.4
Symptom:	Upgrade from 20.3.2b to 20.3.2d on 18-switch node failed.		
Condition:	uncommitted firmware version on the switches which leads to this error.		

Parent Defect ID:	EFA-11685	Issue ID:	EFA-11685
	Not a Software Defect	Severity:	S2 - Major

Parent Defect ID:	EFA-11685	Issue ID:	EFA-11685
Reason Code:			
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.4
Symptom:	TPVM upgrade from 4.2.4 to 4.3.0 failed during EFA re-deployment step		
Condition:	If standby tpvm node is shutdown before tpvm upgrade on the active node was completed		

Parent Defect ID:	EFA-11719	Issue ID:	EFA-11719
Reason Code:	Feature/Function Not Supported	Severity:	S3 - Moderate
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.5
Symptom:	EFA response: Error : undefined response type when issue command "efa fabric setting update --name fab-158 --rack-ld-l3-backup-port 0/30 --rack-ld-mct-ports 0/30,0/31"		

Parent Defect ID:	EFA-11783	Issue ID:	EFA-11783
Reason Code:	Configuration/User Error	Severity:	S3 - Moderate
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.4
Symptom:	efa inventory drift-reconcile execute is failing.		
Condition:	conflicting out of band entries between SLX' config and tenant's configuration		

Parent Defect ID:	EFA-11798	Issue ID:	EFA-11798
Reason Code:	Insufficient Information	Severity:	S3 - Moderate
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.4
Symptom:	TPVM Migration Fails while upgrading SLX		
Condition:	Unknown		
Workaround:	Closed due to insufficient information		

Parent Defect ID:	EFA-11876	Issue ID:	EFA-11876
Reason Code:	Configuration/User Error	Severity:	S3 - Moderate
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.4

Parent Defect ID:	EFA-11876	Issue ID:	EFA-11876
Symptom:	Installation of efa-2.5.4 on ubuntu 18.04 VM fails at 99%		
Condition:	During uninstallation of EFA, there is an error in deletion of efa user		

Parent Defect ID:	EFA-11880	Issue ID:	EFA-11880
Reason Code:	Already Reported	Severity:	S2 - Major
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.3
Symptom:	EFA 2.5.2 Re-deploy post a TPVM Rollback failed on first attempt. Failed to start efa services		

Open Defects

The following defects are open in Extreme Fabric Automation 2.6.0.

Parent Defect ID:	EFA-8904	Issue ID:	EFA-8904
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.4.2
Symptom:	Single node deployment fails with 'DNS resolution failed.'		
Condition:	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.'		
Workaround:	After un-deployment of the multi-node installation, perform a reboot of the server/TPVM.		

Parent Defect ID:	EFA-9065	Issue ID:	EFA-9065
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.4.3
Symptom:	EFA Port Channel remains in cfg-refreshed state when the port-channel is created immediately followed by the EPG create using that port-channel		

Parent Defect ID:	EFA-9065	Issue ID:	EFA-9065
Condition:	Below are the steps to reproduce the issue: 1. Create port-channel po1 under the ownership of tenant1 2. Create endpoint group with po1 under the ownership of tenant1 3. After step 2 begins and before step 2 completes, the raslog event w.r.t. step 1 i.e. port-channel creation is received. This Ralsog event is processed after step 2 is completed		
Recovery:	1. Introduce switchport or switchport-mode drift on the SLX for the port-channel which is in cfg-refreshed state 2. Perform manual DRC to bring back the cfg-refreshed port-channel back to cfg-in-sync		

Parent Defect ID:	EFA-9439	Issue ID:	EFA-9439
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.0
Symptom:	Dev-State and App-State of EPG Networks are not-provisioned and cfg-ready		
Condition:	Below are the steps to reproduce the issue: 1) Create VRF with local-asn 2) Create EPG using the VRF created in step 1 3) Take one of the SLX devices to administratively down state 4) Perform VRF Update "local-asn-add" to different local-asn than the one configured during step 1 5) Perform VRF Update "local-asn-add" to the same local-asn that is configured during step 1 6) Admin up the SLX device which was made administratively down in step 3 and wait for DRC to complete		
Workaround:	No workaround as such.		
Recovery:	Following are the steps to recover: 1) Log in to SLX device which was made admin down and then up 2) Introduce local-asn configuration drift under "router bgp address-family ipv4 unicast" for the VRF 3) Execute DRC for the device		

Parent Defect ID:	EFA-9456	Issue ID:	EFA-9456
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.4.3
Symptom:	EFA fabric configuration fails on a large fabric topology of 30 switches.		

Parent Defect ID:	EFA-9456	Issue ID:	EFA-9456
Condition:	The issue will be observed if devices being added to fabric have IP addresses assigned on interfaces and these IP addresses are already reserved by EFA for other devices.		
Workaround:	Delete the IP addresses on interfaces of devices having conflicting configuration so that new IP addresses can be reserved for these devices. One way to clear the device configuration is using below commands: 1. Register the device with inventory efa inventory device register --ip <ip1, ip2> --username admin --password password 2. Issue debug clear "efa fabric debug clear-config --device <ip1, ip2>"		
Recovery:	Delete the IP addresses on interfaces of devices having conflicting configuration so that new IP addresses can be reserved for these devices. One way to clear the device configuration is using below commands: 1. Register the device with inventory efa inventory device register --ip <ip1, ip2> --username admin --password password 2. Issue debug clear "efa fabric debug clear-config --device <ip1, ip2>" 3. Add the devices to fabric		

Parent Defect ID:	EFA-9570	Issue ID:	EFA-9570
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.0
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-9576	Issue ID:	EFA-9576
	S2 - Major		

Parent Defect ID:	EFA-9576	Issue ID:	EFA-9576
Severity:			
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.0
Symptom:	Deletion of the tenant by force followed by the recreation of the tenant and POs can result in the error "Po number <id> not available on the devices".		
Condition:	Below are the steps to reproduce the issue: 1. Create tenant and PO. 2. Delete the tenant using the "force" option. 3. Recreate the tenant and recreate the PO in the short time window.		
Workaround:	Avoid performing tenant/PO create followed by tenant delete followed by the tenant and PO recreate in the short time window.		
Recovery:	Execute inventory device prior to the PO creation.		

Parent Defect ID:	EFA-9591	Issue ID:	EFA-9591
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.0
Symptom:	"efa fabric configure" fails with error after previously changing the fabric password in the configured fabric		
Condition:	This condition was seen when "efa fabric configure --name <fabric name>" was issued after modifying the MD5 password. Issue is observed when certain BGP sessions are not in an ESTABLISHED state after clearing the BGP sessions as part of fabric configure.		
Workaround:	Wait for BGP sessions to be ready by checking the status of BGP sessions using "efa fabric topology show underlay --name <fabric name>"		
Recovery:	Wait for BGP sessions to be ready. Check the status of BGP sessions using "efa fabric topology show underlay --name <fabric name>"		

Parent Defect ID:	EFA-9758	Issue ID:	EFA-9758
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.0
Symptom:	EFA is not reconciling the remote-asn of BGP peer configuration after the user modified the remote-asn of BGP peer out of band,		

Parent Defect ID:	EFA-9758	Issue ID:	EFA-9758
Workaround:	None		
Recovery:	Revert the remote ASN of BGP peer on the device through SLX CLI to what EFA has configured previously.		

Parent Defect ID:	EFA-9799	Issue ID:	EFA-9799
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.0
Symptom:	'efa status' response shows standby node status as 'UP' when node is still booting up		
Condition:	If SLX device is reloaded where EFA standby node resides, then 'efa status' command will still show the status of standby as UP.		
Workaround:	Retry the same command after some time.		

Parent Defect ID:	EFA-9874	Issue ID:	EFA-9874
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.0
Symptom:	When EPG is in the "anycast-ip-delete-pending" state and the user performs "epg configure", it will succeed without actually removing anycast-ip from SLX.		
Condition:	Below are the steps to reproduce the issue: 1) Configure EPG with VRF, VLAN and anycast-ip (ipv4/ipv6) on a single rack Non-CLOS fabric. 2) Bring one of the devices to admin-down. 3) EPG Update anycast-ip-delete for anycast-ip ipv4 or ipv6. This will put EPG in "anycast-ip-delete-pending" state. 4) Bring the admin-down device to admin-up. 5) In this state, the only allowed operations on EPG are "epg configure" and EPG update "anycast-ip-delete". 6) Perform "epg configure --name <epg-name> --tenant <tenant-name>".		
Workaround:	No workaround.		
Recovery:	Perform the same anycast-ip-delete operation when both devices are admin-up.		

Parent Defect ID:	EFA-9907	Issue ID:	EFA-9907
	S2 - Major		

Parent Defect ID:	EFA-9907	Issue ID:	EFA-9907
Severity:			
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.0
Symptom:	When concurrent EFA tenant EPG update port-add or port-delete operation is requested where the commands involve large number of vlans and/or ports, one of them could fail with the error "vni in use error".		
Condition:	The failure is reported when Tenant service gets stale information about a network that existed a while back but not now. This happens only when the port-add and port-delete are done in quick succession		
Workaround:	Avoid executing port-add and port-delete of same ports in quick succession and in concurrence.		
Recovery:	None		

Parent Defect ID:	EFA-10048	Issue ID:	EFA-10048
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.0
Symptom:	EPG: epgev10 Save for devices failed When concurrent EFA tenant EPG create or update operation is requested where the commands involve large number of vlans and/or ports, one of them could fail with the error "EPG: <epg-name> Save for devices Failed".		
Condition:	The failure is reported when concurrent DB write operation are done by EFA Tenant service as part of the command execution.		
Workaround:	This is a transient error and there is no workaround.		
Recovery:	The failing command can be rerun separately and it will succeed.		

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		

Parent Defect ID:	EFA-10062	Issue ID:	EFA-10062
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		
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-10093	Issue ID:	EFA-10093
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.0
Symptom:	Deletion of the VLAN/BD based L3 EPGs in epg-delete-pending state will result in creation and then deletion of the VLAN/BD on the admin up device where the VLAN/BD was already removed		
Condition:	Issue occurs with the below steps: 1. Create L3 EPG with VLAN/BD X on an MCT pair 2. Admin down one of the devices of the MCT pair 3. Delete the L3 EPG. This results in the L3 configuration removal (corresponding to the L3 EPG getting deleted) from the admin up device and no config changes happen on the admin down device and the EPG transits to epg-delete-pending state 4. Admin up the device which was made admin down in step 2 5. Delete the L3 EPG which transited to epg-delete-pending state in step 3		
Recovery:	Not needed		

Parent Defect ID:	EFA-10252	Issue ID:	EFA-10252
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.1

Parent Defect ID:	EFA-10252	Issue ID:	EFA-10252
Symptom:	When concurrent EFA tenant EPG update port-group-add operations are requested where the tenant is bridge-domain enabled, one of them may fail with the error "EPG network-property delete failed"		
Condition:	The failure is reported when concurrent resource allocations by EFA Tenant service as part of the command execution.		
Workaround:	This is a transient error and there is no workaround.		
Recovery:	The failing command can be rerun separately and it will succeed		

Parent Defect ID:	EFA-10268	Issue ID:	EFA-10268
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.1
Symptom:	When concurrent EPG deletes on bd-enabled tenant are requested where the EPGs involve large number of vlans, local-ip and anycast-ip addresses, one of them may fail with the error "EPG: <epg-name> Save for Vlan Records save Failed".		
Condition:	The failure is reported when concurrent DB write operation are done by EFA Tenant service as part of the command execution.		
Workaround:	This is a transient error and there is no workaround. The failing command can be executed once again and it will succeed.		
Recovery:	The failing command can be rerun separately and it will succeed.		

Parent Defect ID:	EFA-10288	Issue ID:	EFA-10288
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.1
Symptom:	When a bgp peer is created and update operations are performed when one of the devices are in admin down state, the configuration for the admin up device is deleted from the slx switch but remains in efa when "efa tenant service bgp peer configure --name <name> --tenant <tenant>" is performed.		

Parent Defect ID:	EFA-10288	Issue ID:	EFA-10288
Condition:	The bgp peer gets deleted from the SLX but not from EFA. This issue is seen when the following sequence is performed. 1. Create static bgp peer 2. Admin down one of the devices 3. Update the existing bgp static peer by adding a new peer 4. Update the existing bgp static peer by deleting the peers which were first created in step1. Delete from both devices 5. Admin up the device 6. efa tenant service bgp peer configure --name "bgp-name" --tenant "tenant-name" Once the bgp peer is configured, the config is deleted from the switch for the device which is in admin up state whereas EFA still has this information and displays it during bgp peer show		
Workaround:	Delete the peer for admin up device first and then delete the peer from admin down device as a separate cli command.		
Recovery:	Perform a drift reconcile operation for the admin up device so that the configuration gets reconciled on the switch.		

Parent Defect ID:	EFA-10445	Issue ID:	EFA-10445
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.0
Symptom:	Tenant service may occasionally reject subsequent local-ip-add command incorrectly.		
Condition:	When continuous EPG updates with repeated local-ip-add and local-ip-delete operations are done on the same EPG repeatedly without much gap in-between, Tenant service may occasionally retain stale information about the previously created IP configuration and may reject subsequent local-ip-add command incorrectly.		

Parent Defect ID:	EFA-10445	Issue ID:	EFA-10445
Workaround:	There is no work-around to avoid this. Once the issue is hit, user may use a new local-ip-address from another subnet.		
Recovery:	Follow the steps below to remove the stale IP address from Tenant's knowledge base: 1. Find the management IP for the impacted devices. this is displayed in the EFA error message 2. Find the interface VE number. This is same as the CTAG number that the user was trying to associate the local-ip with 3. Telnet/SSH to the device management IP and login with admin privilege 4. Set the local IP address in the device configure t interface ve <number> ip address <local-ip> 5. Do EFA device update by executing 'efa inventory device update --ip <IP> and wait for a minute for the information to be synchronized with Tenant service database 6. Reset the local IP address in the device configure t interface ve <number> no ip address 7. Do EFA device update and wait for a minute for the information to be synchronized with Tenant service database These steps will remove the stale entries and allow future local-ip-add operation to be successful.		

Parent Defect ID:	EFA-10455	Issue ID:	EFA-10455
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.1
Symptom:	"efa status" takes several minutes longer than expected to report a healthy EFA status.		
Condition:	This problem happens when kubernetes is slow to update the standby node's Ready status. This is a potential issue in the shipped version of kubernetes.		
Recovery:	EFA will recover after a period of several minutes.		

Parent Defect ID:	EFA-10548	Issue ID:	EFA-10548
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.2

Parent Defect ID:	EFA-10548	Issue ID:	EFA-10548
Symptom:	When EPG delete operations are done concurrently for EPGs that are on bridge-domain based tenant where the EPG was created with more number of bridge-domains, one of the command may fail with the error "EPG: <epg name> Update for pw-rofile Record save Failed".		
Condition:	The failure is reported when concurrent DB write operation are done by EFA Tenant service as part of the command execution causing the underlying database to report error for one of operation.		
Workaround:	This is a transient error that can rarely happen and there is no workaround.		
Recovery:	The failing command can be rerun separately and it will succeed.		

Parent Defect ID:	EFA-10754	Issue ID:	EFA-10754
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.2
Symptom:	EFA - Backup create fails (timeout)		
Condition:	The device is stuck with the service lock taken as noted in the example inventory log message. This will happen when performing an EFA backup if the backup is performed near the expiration time of the authentication token. {"@time":"2021-10-13T16:19:53.132404 CEST","App":"inventory","level":"info","msg":"executeCBCR: device '21.150.150.201' is already Locked with reason : configbackup ","rqId":"4f144a0c-7be6-4056-8371-f1dc39eb28b3"}		
Recovery:	efa inventory debug devices-unlock --ip 21.150.150.201" will resolve the issue and backup can be done after efa login.		

Parent Defect ID:	EFA-11063	Issue ID:	EFA-11063
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.4
Symptom:	The standby status of the EFA node shows as down when actually the node is ready for failover		
Condition:	The issue happened because one of the pods - rabbitmq was in Crashloopbackoff instead of init mode. This is not a functional issue since its just a status issue.		

Parent Defect ID:	EFA-11063	Issue ID:	EFA-11063
Workaround:	Reboot the standby - which doesn't cause any down time. Another workaround is to restart k3s using systemctl restart k3s command.		
Recovery:	Rebooting the node will fix the pods or restarting k3s will fix the issue		

Parent Defect ID:	EFA-11105	Issue ID:	EFA-11105
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.4
Symptom:	EFA tenant VRF and EPG show "App State: cfg-refresh-err" after a VRF change is made directly on SLX.		
Condition:	Following are the steps to reproduce- Step1) Introduce VRF drift on SLX device by removing "vrf-forwarding" from VE Interfaces associated with the given VRF Step2) Perform "efa inventory device update" for the SLX device where VRF is instantiated Step3) Perform any VRF Update operation Step4) Perform DRC for the same SLX device where VRF is instantiated		
Workaround:	No workaround		
Recovery:	Step1) Remove VRF from the EndpointGroups to which it belongs by using EPG Update "vrf-delete" Step2) Add VRF to all the EndpointGroups again by using EPG Update "vrf-add"		

Parent Defect ID:	EFA-11177	Issue ID:	EFA-11177
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.4
Symptom:	When a tenant with EPGs having 4000+ VLANs across 10+ devices, is deleted with the 'force' option, the delete operation may fail.		
Condition:	This failure happens because Tenant service executes a large database query line which may fail to execute by EFA's database backend.		

Parent Defect ID:	EFA-11177	Issue ID:	EFA-11177
Workaround:	Delete the EPGs belonging to the tenant first and then delete the tenant. This will ensure that the database query lines are split across these multiple request.		
Recovery:	There is no recovery required. This failure does not lead to inconsistency of EFA's database or the SLX device's configurations.		

Parent Defect ID:	EFA-11768	Issue ID:	EFA-11768
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.6.0
Symptom:	This issue was seen when the user tried to delete the devices from the fabric. The bgp peer groups associated to the devices were not removed from the switch.		
Condition:	Initiating a device clean up using the following command does not clean up the associated bgp peer groups from the device. efa fabric device remove --ip 10.20.48.161-162,10.20.48.128-129,10.20.54.83,10.20.61.92-93,10.20.48.135-136 --name fabric2 --no-device-cleanup		
Workaround:	Delete the bgp peer group before issuing a device clean up for the fabric.		
Recovery:	Manually delete the peer groups from the switch.		

Parent Defect ID:	EFA-11779	Issue ID:	EFA-11779
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.4
Symptom:	EFA installation or upgrade procedure abruptly exits without any error.		
Condition:	Security Hardening script, '/opt/security/extr-granite.py' has been run on the system prior to upgrade.		
Workaround:	Before running EFA upgrade, 1. Edit /etc/ssh/sshd_config, remove the following entries ClientAliveInterval 300 ClientAliveCountMax 0 2. Restart ssh service.		

Parent Defect ID:	EFA-11813	Issue ID:	EFA-11813
	S3 - Moderate		

Parent Defect ID:	EFA-11813	Issue ID:	EFA-11813
Severity:			
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.6.0
Symptom:	This issue can be seen for a bgp peer or peer group when update-peer-delete or delete operations are performed with one device for the mct pair in admin down state. The bgp peer gets deleted from the SLX but not from EFA.		
Condition:	Steps to reproduce: 1. Create static bgp peer 2. Admin down one of the devices 3. Update the existing bgp static peer by deleting the peers which were first created in step1. Delete from both devices 4. Admin up the device Once the device is brought up, auto drc kicks in and the config which is deleted from the switch due to admin down state has an incorrect provisioning-state and app-state.		
Workaround:	Bring the admin down device up and then delete the required bgp peers.		
Recovery:	No recovery		

Parent Defect ID:	EFA-11980	Issue ID:	EFA-11980
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.4
Symptom:	An EFA TPVM upgrade workflow may fail for a given device along with the automatic recovery to restore the TPVM back to the original version and rejoin the EFA node back into the HA cluster.		
Condition:	During the "EFA Deploy Peer and Rejoin" step, the EFA image import into the k3s container runtime fails. During the "TPVM Revert" step, the k3s on the active EFA node would not allow the standby EFA node to join the cluster due to a stale node-password in k3s.		
Workaround:	None		
Recovery:	Manually recover the TPVM and EFA deployment by following the procedure described in the link below: EFA 2.5.2 Re-deploy post a TPVM Rollback failed on first attempt. https://extremeportal.force.com/ExtrArticleDetail?an=000099582		

Parent Defect ID:	EFA-11992	Issue ID:	EFA-11992
	S2 - Major		

Parent Defect ID:	EFA-11992	Issue ID:	EFA-11992
Severity:			
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.6.0
Symptom:	When a device is deleted from inventory, the corresponding route-maps are not removed from the specified device for any route-maps that have active BGP peer bindings.		
Condition:	Issue will be seen when user removes the device from inventory and the device has route-map configurations with active bindings		
Workaround:	The user must remove the route-maps from the device manually prior to device deletion.		
Recovery:	After the device is removed from inventory user can remove the route-map configuration on that device manually.		

Parent Defect ID:	EFA-12033	Issue ID:	EFA-12033
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.6.0
Symptom:	Using EFA CLI, the user is able to delete non-EFA managed/OOB (out of band) route-map entries and add rules to non-EFA managed/OOB (out of band) prefix-list.		
Condition:	The user configures some OOB route-map or prefix-list entry on the device directly using SLX CLI/other management means and then tries to delete this route-map entry or add rules under this prefix list entry using EFA. This shouldn't be allowed from EFA as they are not EFA managed entities		
Workaround:	No workaround		
Recovery:	If user deletes the OOB entry or adds rules under OOB prefix-list by mistake it can be added back or removed manually on the device through SLX CLI/other management means.		

Parent Defect ID:	EFA-12058	Issue ID:	EFA-12058
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.6.0
Symptom:	The error 'Error updating traefik with efasecret' is seen during node replacement.		

Parent Defect ID:	EFA-12058	Issue ID:	EFA-12058
Condition:	EFA node replacement is successful.		
Workaround:	Re-add subinterfaces using 'efa mgmt subinterfaces' CLI.		

Parent Defect ID:	EFA-12105	Issue ID:	EFA-12105
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.6.0
Symptom:	A "Drift Reconcile Completion Status Failure" may occur during an EFA firmware download of an SLX device in a fabric.		
Condition:	A DRC status failure can occur if the SLX device also fails during the firmware download. The DRC failure is observed during the drift-reconcile completion step on either the spine node that is hosting the active EFA node TPVM or any device in the same firmware download group which is concurrently running the firmware download workflow at the time of HA failover. This is likely due to the SLX device rebooting and activating the new firmware. During the EFA HA failover, the REST endpoint for the go-inventory service is not established properly and causes the drift-reconcile process to fail.		
Workaround:	None		
Recovery:	Run "efa inventory drift-reconcile execute --ip <SLX device IP address> --reconcile" to retry the drift-reconcile process on the failed device.		

Parent Defect ID:	EFA-12114	Issue ID:	EFA-12114
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.4

Parent Defect ID:	EFA-12114	Issue ID:	EFA-12114
Symptom:	In rare circumstances, kubernetes' EndpointSliceController can fall out of sync leading to incorrect iptables rules being instantiated. This can lead to EFA APIs failing because they are redirected to non-existent services.		

Recovery:	EFA's monitor process will detect and attempt to remediate this situation automatically. If it fails to do so, the following can help:
	On both TPVMs, as the super-user,
	$ systemctl restart k3s
	If the problem recurs, these further steps, run as super-user, may help:
	$ sed -i -E 's/EndpointSlice=true/EndpointSlice=false/' /lib/systemd/system/k3s.service
	$ systemctl daemon-reload
	$ systemctl restart k3s		

Parent Defect ID:	EFA-12141	Issue ID:	EFA-12141
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.6.0
Symptom:	After EFA backup and restore, drifted route maps could be shown as cfg-in-sync state.		
Condition:	Issue could be seen after EFA backup and restore, if prefix lists and route maps are removed by EFA after backup.		
Workaround:	There is no workaround. It is a display issue.		
Recovery:	If a drift is present on device, running the 'efa inventory drift-reconcile' command will reconcile the entities on the device.		

Parent Defect ID:	EFA-12154	Issue ID:	EFA-12154
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.6.0
Symptom:	A firmware download can fail with "Firmware Download Failed" status.		

Parent Defect ID:	EFA-12154	Issue ID:	EFA-12154
Condition:	1) The current SLX firmware version on the devices which are being upgraded must be 20.2.3c, 20.2.3d, 20.2.3e, and 20.3.4. 2) The --noAutoCommit flag is specified for firmware download execution. 3) Any device that is in the same firmware download group with the device hosting the active EFA node, can encounter the firmware download failure. The firmware download failure occurs when the active EFA node is reloaded to activate the new firmware while the other device is in the middle of an SLX firmware download. The HA failover will cause the firmware download workflows to be restarted at the last completed step. Since the SLX firmware download did not complete, the SLX firmware download command will be issued to the device again. The SLX firmware 20.2.3c through 20.3.4 returns an error stating that it "Cannot start download before the new image is committed."		
Workaround:	Prepare a group list that contains only active EFA nodes and execute at the end of the SLX upgrade cycle		

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.