Extreme Fabric Automation Release Notes

2.6.1

9037330-01 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/

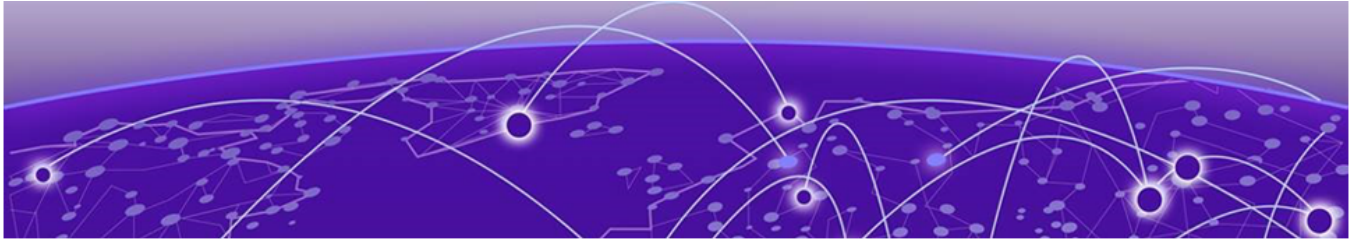
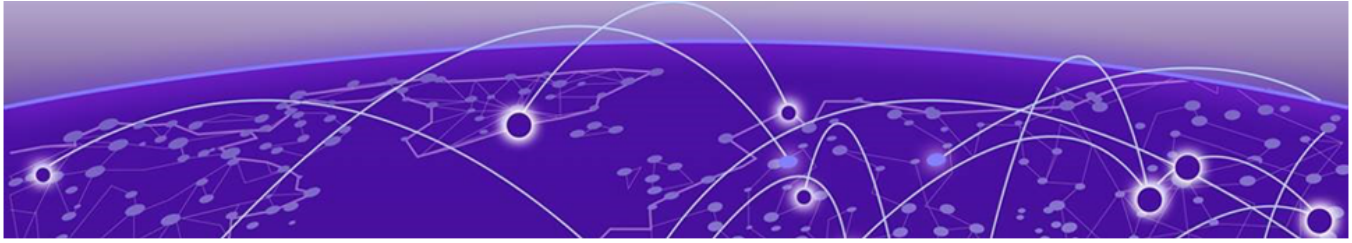


Table of Contents



Release Notes

New In This Release

Extreme Fabric Automation 2.6.1 resolves several issues.

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 1: 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 2: 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 3: 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 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	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, 2.6.1

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	✔				✔
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 5: 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 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 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 2.6.1.

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.		
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
	S3 - Moderate		

Parent Defect ID:	EFA-8448	Issue ID:	EFA-8448
Severity:			
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.		
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.		

Parent Defect ID:	EFA-9813	Issue ID:	EFA-9813
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
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

Parent Defect ID:	EFA-9990	Issue ID:	EFA-9990
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		
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-11587	Issue ID:	EFA-11587
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.4
Symptom:	EFA not closing unsuccessful SSH attempts when password expires on SLX		
Recovery:	No Recovery		

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.		

Parent Defect ID:	EFA-11779	Issue ID:	EFA-11779
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-12081	Issue ID:	EFA-12081
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.2
Symptom:	Installing k3s container orchestration Failed.		
Condition:	Feature is already implemented in EFA 2.5.3,		

Parent Defect ID:	EFA-12160	Issue ID:	EFA-12160
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.6.0
Symptom:	device support save is not getting collected with 502 Bad Gateway error where efa ss is scp'ed to remote server		

Parent Defect ID:	EFA-12196	Issue ID:	EFA-12196
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.4
Symptom:	.EFA upgrade from 2.5.4 to 2.5.5 failed because of DNS resolution		

Parent Defect ID:	EFA-12204	Issue ID:	EFA-12204
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.5
Symptom:	EFA RBAC does not work as expected		

Parent Defect ID:	EFA-12247	Issue ID:	EFA-12247
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.2

Parent Defect ID:	EFA-12247	Issue ID:	EFA-12247
Symptom:	EFA External DCO Interface went missing post EFA Upgrade		
Condition:	When EFA is upgraded to a newer version, EFA backup is taken before the upgrade procedure is triggered. The backup file is named "EFA-Upgrade-<Version>-<Build>.tar". If restore is performed using this backup file, then management subinterfaces and routes will not be available.		
Workaround:	For restore procedure, use any 'User' generated backup file. The migration support was added in EFA 2.5.4		
Recovery:	In case the restore is already performed, then recreate the subinterfaces and routes using CLI.		

Parent Defect ID:	EFA-12282	Issue ID:	EFA-12282
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.4
Symptom:	Missing git on TPVM after switch replacement		

Parent Defect ID:	EFA-12322	Issue ID:	EFA-12322
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.6.0
Symptom:	.Cannot create backup - logged out from EFA before action is ready		

Parent Defect ID:	EFA-12372	Issue ID:	EFA-12372
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.6.0
Symptom:	.EFA - Error - The command cannot be completed at this time		

Parent Defect ID:	EFA-12400	Issue ID:	EFA-12400
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.6.0
Symptom:	.EFA login fails after active spine reboot		

Parent Defect ID:	EFA-12431	Issue ID:	EFA-12431
	S2 - Major		

Parent Defect ID:	EFA-12431	Issue ID:	EFA-12431
Severity:			
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.6.0
Symptom:	TPVM 4.3.0 to 4.4.0, upgrade get failed via EFA 2.6.0 but upgrades well on SLX.		

Parent Defect ID:	EFA-12490	Issue ID:	EFA-12490
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.6.0
Symptom:	EFA commands failing after active spine reboot		

Parent Defect ID:	EFA-12492	Issue ID:	EFA-12492
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.6.0
Symptom:	EFA command fails with "Execution error: undefined response type"		

Parent Defect ID:	EFA-12516	Issue ID:	EFA-12516
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.6.0
Symptom:	EFA command fails with "Execution error: undefined response type"		

Defects Closed without Code Changes

The following defects were closed in Extreme Fabric Automation 2.6.1.

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"		

Parent Defect ID:	EFA-10305	Issue ID:	EFA-10305
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.		
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.		

Parent Defect ID:	EFA-10389	Issue ID:	EFA-10389
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		
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

Parent Defect ID:	EFA-10879	Issue ID:	EFA-10879
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
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

Parent Defect ID:	EFA-11421	Issue ID:	EFA-11421
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
Reason Code:	Not a Software Defect	Severity:	S2 - Major
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.4

Parent Defect ID:	EFA-11685	Issue ID:	EFA-11685
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		

Parent Defect ID:	EFA-12283	Issue ID:	EFA-12283
Reason Code:	Not a Software Defect	Severity:	S3 - Moderate
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.5
Symptom:	MGMT Interface - netstat port is not displayed		
Condition:	Not a valid defect		

Parent Defect ID:	EFA-12428	Issue ID:	EFA-12428
Reason Code:	Not a Software Defect	Severity:	S2 - Major
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.5
Symptom:	EFA deploy failed: Default gateway is not reachable		
Condition:	Issue was with customer setup, not a valid defect		

Open Defects

The following defects are open in Extreme Fabric Automation 2.6.1.

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-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		

Parent Defect ID:	EFA-9570	Issue ID:	EFA-9570
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
Severity:	S2 - Major		
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.		

Parent Defect ID:	EFA-9591	Issue ID:	EFA-9591
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,		
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-9907	Issue ID:	EFA-9907
Severity:	S2 - Major		
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		

Parent Defect ID:	EFA-9907	Issue ID:	EFA-9907
Workaround:	Avoid executing port-add and port-delete of same ports in quick succession and in concurrence.		
Recovery:	None		

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		
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-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-10525	Issue ID:	EFA-10525
Severity:	S3 – Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.4

Parent Defect ID:	EFA-10525	Issue ID:	EFA-10525
Symptom:	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-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-11813	Issue ID:	EFA-11813
Severity:	S3 - Moderate		
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.		

Parent Defect ID:	EFA-11813	Issue ID:	EFA-11813
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-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.		
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.		

Parent Defect ID:	EFA-12105	Issue ID:	EFA-12105
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
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-12117	Issue ID:	EFA-12117
Severity:	S3 – Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.4

Parent Defect ID:	EFA-12117	Issue ID:	EFA-12117
Symptom:	EFA not closing unsuccessful SSH attempts when password expires on SLX		
Recovery:	No Recovery		

Parent Defect ID:	EFA-12182	Issue ID:	EFA-12182
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.4
Symptom:	The issue can be replicated by adding extra link to the existing ICL link. This could find the error in “efa fabric show” The issue is not seen on every attempt.		
Condition:	Dynamic adding of links to existing ICL, The speed of interface is not updated to the LLDP database causing the the devices to go into error state.		
Workaround:	Remove, readd the device and configure fabric after adding new links.		
Recovery:	Remove, readd the device and configure fabric OR manually update the lldp db with the correct speed and update devices.		

Parent Defect ID:	EFA-12228	Issue ID:	EFA-12228
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.4
Symptom:	Efa system backup failure		
Recovery:	No Recovery		

Parent Defect ID:	EFA-12237	Issue ID:	EFA-12237
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.4
Symptom:	EPG update port-group-delete operation results in the runtime error "Execution error: service is not available or internal server error has occurred, please try again later"		

Parent Defect ID:	EFA-12237	Issue ID:	EFA-12237
Condition:	Below are the steps to reproduce the issue: 1. Create a BD based tenant under a CLOS or Non-CLOS fabric. 2. Create a BD based EPG (under the ownership of the tenant created in step 1) with some ctags and some member port-channels. 3. For the reasons unknown, the BD (Bridge Domain) configuration pertaining to one of the member port-channel got deleted from the EFA DB, causing the DB to be in an inconsistent state. 4. Execute EPG update "port-group-delete" operation to remove the member port-channel whose BD configuration is inconsistent.		
Recovery:	No recovery through EFA CLI. The inconsistent DB needs to be corrected by creating dummy BD (Bridge Domain) entries in the database followed by EPG update "port-group-delete".		

Parent Defect ID:	EFA-12305	Issue ID:	EFA-12305
Severity:	S3 – Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.6.1
Symptom:	EFA not closing unsuccessful SSH attempts when password expires on SLX		
Recovery:	No Recovery		

Parent Defect ID:	EFA-12331	Issue ID:	EFA-12331
Severity:	S3 – Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.4
Symptom:	DRC takes too long to complete when a switch reload causes a transient kubernetes error.		
Recovery:	The system will recover on its own		

Parent Defect ID:	EFA-12237	Issue ID:	EFA-12237
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.4
Symptom:	EPG update port-group-delete operation results in the runtime error "Execution error: service is not available or internal server error has occurred, please try again later"		

Parent Defect ID:	EFA-12237	Issue ID:	EFA-12237
Condition:	Below are the steps to reproduce the issue: 1. Create a BD based tenant under a CLOS or Non-CLOS fabric. 2. Create a BD based EPG (under the ownership of the tenant created in step 1) with some ctags and some member port-channels. 3. For the reasons unknown, the BD (Bridge Domain) configuration pertaining to one of the member port-channel got deleted from the EFA DB, causing the DB to be in an inconsistent state. 4. Execute EPG update "port-group-delete" operation to remove the member port-channel whose BD configuration is inconsistent.		
Recovery:	It's applicable with large SLX configuration		

Parent Defect ID:	EFA-12344	Issue ID:	EFA-12344
Severity:	S3 – Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.4
Symptom:	After firmware download (with maint mode enabled on reboot) the device takes a long time to finish DRC thus taking device out of maint mode		
Recovery:	It's applicable with large SLX configuration		

Parent Defect ID:	EFA-12429	Issue ID:	EFA-12429
Severity:	S2 – Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.6.0
Symptom:	After failover active EFA down, Standby is up		

Parent Defect ID:	EFA-12441	Issue ID:	EFA-12441
Severity:	S2 – Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.5
Symptom:	The RabbitMQ port was getting exposed on the EFA management interface and all sub-interfaces.		

Parent Defect ID:	EFA-12441	Issue ID:	EFA-12441
Workaround:	For manually created sub-interfaces after EFA installation, the EFA iptables policy will need to be restarted in order to apply filtering rules to these new interfaces. The command for this (as root) is: 'systemctl restart efa-iptables.service'.		
Recovery:	Same as workaround		

Parent Defect ID:	EFA-12480	Issue ID:	EFA-12480
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.6.1
Symptom:	Scale Config : VRF doesn't allow to have more than 4095 SR in single creation		
Workaround	No Workaround		
Recovery:	No Recovery		

Parent Defect ID:	EFA-12454	Issue ID:	EFA-12454
Severity:	S2 – Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.6.0
Symptom:	If the password on an SLX device is changed manually through the SLX command and the password is modified in EFA as well using the command "efa inventory device update --ip <IP> --username <user> --password <password", then the subsequent "efa tenant ...." commands that correspond to the device (for which the password is changed) will fail with the error "Error : Could not connect to Devices: <device-ip>"		
Condition:	Below are the steps to reproduce the issue: 1. The SLX device password is changed manually through the SLX command 2. The SLX device password is modified in EFA as well using the command "efa inventory device update --ip <IP> --username <user> --password <password" 3. "efa tenant ...." commands that correspond to the device (for which the password is changed) are executed		

Parent Defect ID:	EFA-12454	Issue ID:	EFA-12454
Workaround:	1. Change the device password through EFA using the command "efa inventory device update --ip <IP> --username <user> --password <password" 2. Change EFA inventory key-value store information for the corresponding device by using "efa inventory kvstore create --key switch.<IP addr>.password --value <new-password> --encrypt" 3. Wait for up to 15 minutes for this information to be consumed by the tenant service		
Recovery:	Two recovery steps are available		

Parent Defect ID:	EFA-12516	Issue ID:	EFA-12516
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.6.0
Symptom:	After changing IP and running "efa-change-ip" script EFA pods are in boot loop		
Recovery:	Rollback is automatically performed so no stale config is left on the switch. No recovery is required		

Parent Defect ID:	EFA-12539	Issue ID:	EFA-12539
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.6.1
Symptom:	EPG update request with port-group-add operation and EPG create request where multiple ctags are mapped to one bridge-domain, may fail with error "Error 1452: Cannot add or update a child row"		
Condition:	Error will be observed when one of the following use cases are executed on bridge-domain enabled tenant. Use case-1: 1. Create an EPG with multiple ctags mapped to one bridge-domain and with ports across SLX devices that are not part of an MCT pair Use case-2: 1. Create an EPG with multiple ctags mapped to one bridge-domain and with ports or port-channels on one SLX device 2. Update the EPG with port(s) on new SLX device that is not an MCT pair of first device		

Parent Defect ID:	EFA-12539	Issue ID:	EFA-12539
Workaround:	Create the EPG with all the required ports and with one ctag-bridge-domain mapping first. Then do epg update with ctag-add-range operation to add additional ctags to the same bridge-domain		
Recovery:	Rollback is automatically performed so no stale config is left on the switch. No recovery is required		

Parent Defect ID:	EFA-12555	Issue ID:	EFA-12555
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.6.1
Symptom:	EPG update request with port-group-add operation and EPG create request where multiple ctags are mapped to one bridge-domain, may fail with error "Error 1452: Cannot add or update a child row"		
Condition:	Error will be observed when one of the following use cases are executed on bridge-domain enabled tenant. Use case-1: 1. Create an EPG with multiple ctags mapped to one bridge-domain and with ports across SLX devices that are not part of an MCT pair Use case-2: 1. Create an EPG with multiple ctags mapped to one bridge-domain and with ports or port-channels on one SLX device 2. Update the EPG with port(s) on new SLX device that is not an MCT pair of first device		
Recovery:	Recreate L3 EPG the port-groups, further anycast-ip updates will work as expected.		

Parent Defect ID:	EFA-12556	Issue ID:	EFA-12556
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.6.1
Symptom:	If all port-groups are deleted from the L3 EPG, then anycast-address details are removed from the EFA database, thus next port-group operations fails with validations error.		

Parent Defect ID:	EFA-12556	Issue ID:	EFA-12556
Condition:	1. Create L3 epg with device ports [0/10,11] 2. EPG update port-group-delete operation with both ports from the device. 3. EPG update with port-group-add with device port [0/10]		
Recovery:	Delete and recreate the EPG with anycast-details and then perform port-group add operations		

Parent Defect ID:	EFA-12557	Issue ID:	EFA-12557
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.6.1
Symptom:	L3 EPG update with operation anycast-ip-delete with all anycast-ips(configured as part of EPG), is allowed leading to Ve without any v4/v6 anycast-ips.		
Condition:	1. Create L3 EPGs with both ipv4 and ipv6 anycast-ips 2. EPG update with anycast-ip-delete, pass all anycast-ips configured as part of step 1 3. After EPG update, all anycast-ips are removed from the DB and device both Workaround: Pass anycast-ip one by one to the EPG update CLI. Last anycast-ip removal will not be allowed and validation error will be thrown.		
Workaround:	Pass anycast-ip one by one to the EPG update CLI. Last anycast-ip removal will not be allowed and validation error will be thrown.		

Parent Defect ID:	EFA-12558	Issue ID:	EFA-12558
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.6.1
Symptom:	L3 NPEPG(without ports) update with operation anycast-ip delete, does not remove Anycast-ip from the EFA DB.		
Condition:	1. Create L3 EPG without ports 2. Update epg with operation: anycast-ip-delete 3. Anycast-ip not removed from the DB.		
Workaround:	Delete and re-create the EPG to remove the anycast-address		

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.