Extreme Fabric Automation Release Notes

2.7.0

9037429-00 Rev AB
January 2024

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see: www.extremenetworks.com/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: https://www.extremenetworks.com/support/policies/open-source-declaration/

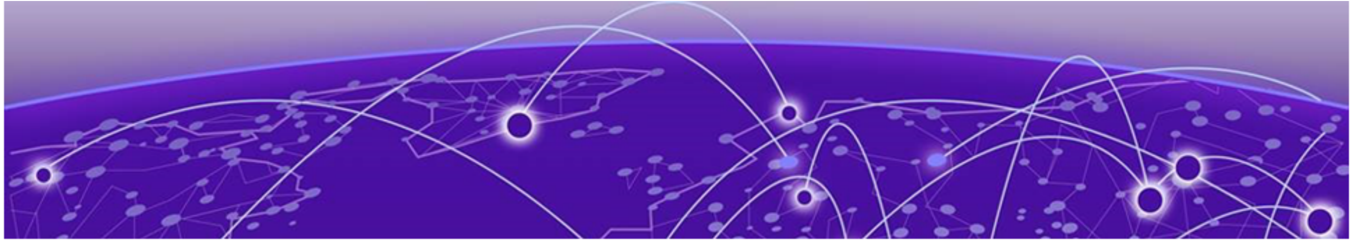
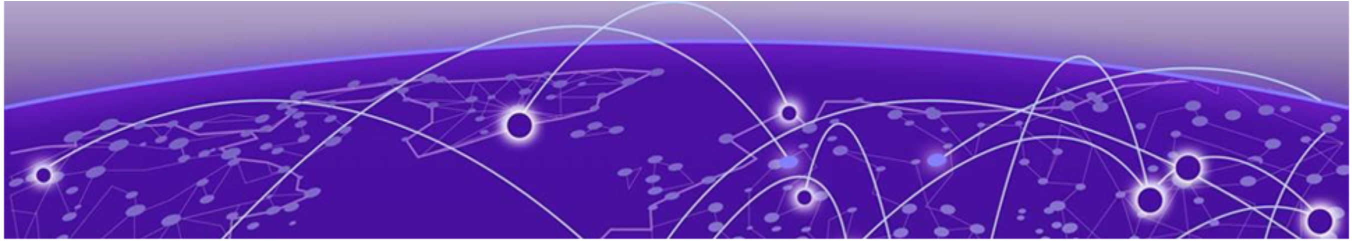


Table of Contents



Release Notes

New In This Release

Extreme Fabric Automation 2.7.0 provides the following features and improvements.

Table 1: Features and Improvements

Feature	Description
Traffic Mirroring support	Describes Traffic Mirroring and its configuration procedure. For more information, see the *Extreme Fabric Automation Administration Guide, 2.7.0*
Backup Routing support on BGP peer	Describes Backup Routing neighbors configuration on BGP peer. For more information, see the *Extreme Fabric Automation Administration Guide, 2.7.0*
IP prefix-list and route-map features	Describes how to create, delete, and update IP prefix list and route map on devices. For more information, see the *Extreme Fabric Automation Administration Guide, 2.7.0*
DRC Optimization	Describes Drift and Reconcile (DRC) Optimization, it's architecture, and details about parallel DRC operations. For more information, see the *Extreme Fabric Automation Administration Guide, 2.7.0*

Table 1: Features and Improvements (continued)

Feature	Description
Infrastructure improvements and upgrades	Describes • Northbound IPv6 changes • Active/standby approach to HA • TPVM snapshot, EFA backup versioning • Manage gateway changes in EFA For more information, see the *Extreme Fabric Automation Administration Guide, 2.7.0*
	Describes flexible EFA deployment in EFA (single CLI). For more information, see the *Extreme Fabric Automation Deployment Guide, 2.7.0*
	Updated the EFA system backup location to include the EFA version and build number in the backup tar file name. For more information, see the *Extreme Fabric Automation Administration Guide, 2.7.0*
Firmware download code optimizations and enhancements	Optimizes firmware download steps, firmware download to include DRC, and replaced maintenance mode with new exec mode. For more information, see the *Extreme Fabric Automation Administration Guide, 2.7.0*
Multiple Anycast IP support	Describes multiple anycast IP configuration. For more information, see the *Extreme Fabric Automation Administration Guide, 2.7.0*
EFA login to the switch with different user names triggering as a security violation on the switch	Describes the solution to resolve the security violation issue on the switches. For more information, see the *Extreme Fabric Automation Administration Guide, 2.7.0*
RBAC: Observing "export EFA_TOKEN" command suggestion while a tenant user logging in	Describes the solution when an RBAC user gets the export EFA_TOKEN suggestion while logging in to EFA. For more information, see the *Extreme Fabric Automation Administration Guide, 2.7.0*
EFA CLI or REST request with scale config taking longer than 15 minutes fails with error "service is not available or internal server error has occurred"	Describes the solution when you get an error while trying to delete tenants. For more information, see the *Extreme Fabric Automation Administration Guide, 2.7.0*

Table 1: Features and Improvements (continued)

Feature	Description
Edit Active Fabric Settings	Describes which fabric settings can be updated in small data center and Clos fabric. For more information, see the *Extreme Fabric Automation Administration Guide, 2.7.0*
Fabric Event Handling	Provides the list of events generated by RASlog event or device update handled in Fabric services. For more information, see the *Extreme Fabric Automation Administration Guide, 2.7.0*
Security enhancements	• Security GPR - Password Protection - Describes encryption key details for SLX password cache. • Certificate handling generated by an external CA - Describes EFA's handling of certificates signed or created by external CA for all services protected by TLS. • EFA third-party certificate acquired through trusted CAs cannot be properly applied to EFA - Provides workaround for DNS server certificate. • Notification support for certificate expiration for EFA - Provides notification to users to update the north bound certificates when they are about to expire. • Support for renewal of default EFA certificate For more information, see the *Extreme Fabric Automation Security Guide, 2.7.0*
Improvements	• Configure BGP PIC from EFA • Modify RIB ECMP under Hardware Route Profile • Fabric and IP range options for updating inventory device settings • Configure time zone per Fabric level • Supports 4 secure syslog servers • EFA deploy-with-rollback for single node deployment support • Option to delete or clear FWDL which is stuck in progress • Should not unwind to no-install after a failed upgrade For more information, see the *Extreme Fabric Automation Administration Guide, 2.7.0*

For more information, see Defects Closed with Code Changes on page 10.

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, 2.7.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), 2.7.x	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

Table 4: TPVM Deployment Models (continued)

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

Table 5: TPVM Software Support

TPVM Version	SLX-OS 20.2.3 d/e/f	SLX-OS 20.3.2	SLX-OS 20.3.2a	SLX-OS 20.3.2 b	SLX-OS 20.3.2c	SLX-OS 20.3.2 d	SLX-OS 20.3.4/ 4a	SLX-OS 20.4.1	Ubuntu Version	EFA Version
4.2.4	Yes	No	No	No	No	No	No	No	18.04	2.4.x
4.2.5	No	Yes	Yes	No	No	No	No	No	18.04	2.4.x, 2.5.0
4.2.5	No	No	No	Yes	No	No	No	No	18.04	2.5.1, 2.5.2
4.2.5	No	No	No	No	Yes	No	No	No	18.04	2.5.3
4.3.0	No	No	No	No	No	Yes	No	No	18.04	2.5.4, 2.5.5

Table 5: TPVM Software Support (continued)

TPVM Version	SLX-OS 20.2.3d/e/f	SLX-OS 20.3.2	SLX-OS 20.3.2a	SLX-OS 20.3.2b	SLX-OS 20.3.2c	SLX-OS 20.3.2d	SLX-OS 20.3.4/4a	SLX-OS 20.4.1	Ubuntu Version	EFA Version
4.4.0	No	No	No	No	No	No	Yes	No	18.04	2.6.0, 2.6.1
4.5.0	No	No	No	No	No	No	No	Yes	18.04	2.7.0

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		✔	✔	✔	✔
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

EFA Upgrade Prerequisites

Prerequisites for EFA upgrade process with the default gateway changed:

1. Ensure that no DNS configuration exists under TPVM config and resolve.conf.

2. Presence of management connectivity from SLX and TPVM to external build server image, wherein image is available during SLX and TPVM upgrade process.

If file/etc/sshd/sshd_config is modified to non-default values, then manually readjust the following parameters:

- MaxStartups 30:30:100
- MaxAuthTries 6
- LoginGraceTime 120

Note
The hardening script bundled with EFA 2.6.1 will not automatically modify the above mentioned parameters.

Known Limitations

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

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

Defects Closed with Code Changes

The following defects, which were previously disclosed as open, were resolved in Extreme Fabric Automation 2.7.0.

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-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		
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-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.		

Parent Defect ID:	EFA-9576	Issue ID:	EFA-9576
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-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-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-10252	Issue ID:	EFA-10252
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.1
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.		

Parent Defect ID:	EFA-10252	Issue ID:	EFA-10252
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.		
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		

Parent Defect ID:	EFA-10288	Issue ID:	EFA-10288
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-10606	Issue ID:	EFA-10606
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.2
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-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)		

Parent Defect ID:	EFA-10754	Issue ID:	EFA-10754
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-10759	Issue ID:	EFA-10759
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.2
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 must be less than or equal to 5.		

Parent Defect ID:	EFA-11002	Issue ID:	EFA-11002
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.2
Symptom:	SNMP Host with ?#%&*+(characters is not supported		
Condition:	.		
Workaround:	Please create SNMP hostnames without these characters.		
Recovery:	Please create SNMP hostnames without these characters		

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-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.		
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-11813	Issue ID:	EFA-11813
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.6.0

Parent Defect ID:	EFA-11813	Issue ID:	EFA-11813
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-11983	Issue ID:	EFA-11983
	S3 - Moderate		

Parent Defect ID:	EFA-11983	Issue ID:	EFA-11983
Severity:			
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.0
Symptom:	Error : Ports Failed to allocate ClientIDs: [13] as its already consumed by other clients		

Parent Defect ID:	EFA-11992	Issue ID:	EFA-11992
Severity:	S2 - Major		
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-12114	Issue ID:	EFA-12114
	S3 - Moderate		

Parent Defect ID:	EFA-12114	Issue ID:	EFA-12114
Severity:			
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:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.0
Symptom:	Not able to add new spine link due to duplicate entries in device links		
Condition:	A duplicate device link is created for the same interface. If the user has changed link connection to new device, we see this issue		
Recovery:	Remove duplicate entries either manually or through the script.		

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.		

Parent Defect ID:	EFA-12141	Issue ID:	EFA-12141
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-12147	Issue ID:	EFA-12147
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.2
Symptom:	EFA upgrade failed CNIS 1.2 to 1.3		

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 devices to go into error state.		
Workaround:	Remove, read the device and configure fabric after adding new links.		
Recovery:	Remove, read the device and configure fabric OR manually update the lldp db with the correct speed and update devices.		

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-12344	Issue ID:	EFA-12344
Severity:	S3 – Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.4

Parent Defect ID:	EFA-12344	Issue ID:	EFA-12344
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-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.		
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-12454	Issue ID:	EFA-12454
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.4
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 1. 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". Then wait for 15 minutes for this information to be available to Tenant service 2. If the password information needs to be quickly made available to Tenant service or if the first step does not help, restart the tenant service with sudo or root privilege using 'efactl restart-service gotenant-service'		

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-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		

Parent Defect ID:	EFA-12554	Issue ID:	EFA-12554
	S3 - Moderate		

Parent Defect ID:	EFA-12554	Issue ID:	EFA-12554
Severity:			
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.6.0
Symptom:	Response from REST get for LLDP neighbors when there are none is null instead of empty which was expected		

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.		

Parent Defect ID:	EFA-12558	Issue ID:	EFA-12558
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		

Parent Defect ID:	EFA-12692	Issue ID:	EFA-12692
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.7.0
Symptom:	After last EPG delete, IP and MAC access lists are not removed from the device.		
Condition:	1. Create EPG1 with port-property ACL on the device1 2. Create EPG2 with network-property ACL on the device1. 3. Verify on the device, ACL configurations are pushed 4. Delete both EPG1 and EPG2 5. Do show mac access-list/ show ip access-list. MAC and IP Access-lists not removed from the device.		
Recovery:	Manually delete the MAC and IP access-lists from the device.		

Parent Defect ID:	EFA-12722	Issue ID:	EFA-12722
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.5
Symptom:	FlexiLab: MCT PO64 goes down on device seliinsw00288 when doing DRC on cluster device seliinsw00279		

Parent Defect ID:	EFA-12796	Issue ID:	EFA-12796
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.7.0
Symptom:	During reconcile, Drifted ACL rules not identified and reconciled on the device.		

Parent Defect ID:	EFA-12796	Issue ID:	EFA-12796
Condition:	1. Create EPG with PP ACL on the device port/PO. 2. Manually remove the rules under the ACL from the SLX device. 3. Trigger DRC flow. Drift in the ACL rules is not identified, hence during reconciliation, the rules are not pushed to the device.		
Recovery:	Manually configure drifted rules under the ACL		

Parent Defect ID:	EFA-12858	Issue ID:	EFA-12858
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.7.0
Symptom:	OOB created Monitor Session is deleted from SLX		
Condition:	Below are the steps to reproduce the issue: 1) Manually create a monitor session on the SLX i.e. Create an OOB (Out Of Band) monitor session on SLX 2) Create Tenant and Mirror Session from EFA		
Workaround:	No workaround		
Recovery:	Manually recreate the deleted OOB monitor session on SLX again		

Parent Defect ID:	EFA-12933	Issue ID:	EFA-12933
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.7.0
Symptom:	Monitor Session(s) and Portchannels are not deleted from SLX		
Condition:	Below are the steps to reproduce the issue: 1) Create Fabric 2) Create Tenant and Portchannels 3) Create Mirror Session using Portchannel as a mirror source 4) Delete fabric with force option or remove devices from inventory		
Workaround:	No workaround		
Recovery:	1) Manually delete the EFA created Mirror Session from SLX device 2) Manually delete the EFA created Portchannels from SLX device		

Parent Defect ID:	EFA-12955	Issue ID:	EFA-12955
	S3 - Moderate		

Parent Defect ID:	EFA-12955	Issue ID:	EFA-12955
Severity:			
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.5
Symptom:	Error message seen while trying to add ports to an EPG		

Parent Defect ID:	EFA-12967	Issue ID:	EFA-12967
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.7.0
Symptom:	LLDP remains disabled on the mirror destination port of the SLX		
Condition:	Below are the steps to reproduce the issue: 1) Create a Tenant and create a Mirror Session. The mirror session create disables the LLDP on the mirror destination port 2) Delete the Mirror Session created in step 1		
Workaround:	No workaround		
Recovery:	"no lldp disable" needs to be performed manually on the SLX port		

Parent Defect ID:	EFA-12968	Issue ID:	EFA-12968
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.7.0
Symptom:	Tenant service restarts on rare cases when REST based configuration commands are sent in a tight loop causing REST clients to get HTTP error 502.		
Condition:	This can happen on rare occasions when REST based configuration commands are sent in a tight loop over a period of time.		
Workaround:	There is no workaround available		
Recovery:	Rerun the failed command once Tenant service is back up, which would happen in a couple of minutes		

Parent Defect ID:	EFA-12987	Issue ID:	EFA-12987
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.4
Symptom:	Efa Drift-and-reconcile keeps failing on one of the switch in fabric		

Parent Defect ID:	EFA-13028	Issue ID:	EFA-13028
	S2 - Major		

Parent Defect ID:	EFA-13028	Issue ID:	EFA-13028
Severity:			
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.7.0
Symptom:	DRC fails while reconciling ACL configurations if ACL has different rule with same sequence number.		
Condition:	1. Create the EPG with PP/NP ACL on the device Ports/Networks. 2. Manually delete the rule under the ACL and create another rule with the same sequence number, on the SLX device. 3. Trigger DRC.		
Recovery:	Manually configure the expected rule under ACL		

Parent Defect ID:	EFA-13069	Issue ID:	EFA-13069
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.7.0
Symptom:	Mirror Session create fail with error - "More than one mirror destination ports available on the device <device-ip> for the tenant <tenant-name>"		
Condition:	Below are the steps to reproduce the issue: 1) Create Tenant with more than one mirror-destination-port per device 2) Create Mirror Session with Global Vlan as mirror source and an explicit mirror destination (and not auto derived mirror destination)		
Workaround:	1) Update Tenant to delete mirror-destination ports from devices using "efa tenant update --operation mirror-destination-port-delete --mirror-destination-port <ports>" so that only one mirror-destination port per device remains in tenant 2) Create Mirror Session again with Global Vlan as mirror source and the explicit mirror destination (and not auto derived mirror destination)		
Recovery:	No recovery		

Parent Defect ID:	EFA-13189	Issue ID:	EFA-13189
	S3 - Moderate		

Parent Defect ID:	EFA-13189	Issue ID:	EFA-13189
Severity:			
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.2
Symptom:	HTTP Server configuration is shutdown on some switches in the fabric after upgrade of EFA/TPVM		

Parent Defect ID:	EFA-13254	Issue ID:	EFA-13254
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.6.1
Symptom:	3 of EFA Pods fails Liveliness / Rediness checks causing Init containers to stop and causing crashloopback		

Defects Closed without Code Changes

The following defects were closed in Extreme Fabric Automation 2.7.0.

Parent Defect ID:	EFA-9456	Issue ID:	EFA-9456
Reason Code:	Insufficient Information	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.		
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.		

Parent Defect ID:	EFA-9456	Issue ID:	EFA-9456
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-9799	Issue ID:	EFA-9799
Reason Code:	Already Implemented	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-10093	Issue ID:	EFA-10093
Reason Code:	Working as Designed	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		

Parent Defect ID:	EFA-10093	Issue ID:	EFA-10093
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-10525	Issue ID:	EFA-10525
Reason Code:	Already Reported	Severity:	S3 - Moderate
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.0
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-10684	Issue ID:	EFA-10684
Reason Code:	Insufficient Information	Severity:	S2 - Major
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.1
Symptom:	EFA cannot start - Init:ErrImageNeverPull		

Parent Defect ID:	EFA-12058	Issue ID:	EFA-12058
Reason Code:	Not Reproducible	Severity:	S3 - Moderate
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.6.0

Parent Defect ID:	EFA-12058	Issue ID:	EFA-12058
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-12081	Issue ID:	EFA-12081
Reason Code:	Insufficient Information	Severity:	S3 - Moderate
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.2
Symptom:	Installing k3s container orchestration Failed.		
Workaround:	Feature is already implemented in EFA 2.5.3		

Parent Defect ID:	EFA-12105	Issue ID:	EFA-12105
Reason Code:	Already Implemented	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-12154	Issue ID:	EFA-12154
Reason Code:	Already Implemented	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		

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-12247	Issue ID:	EFA-12247
Reason Code:	Not a Software Defect	Severity:	S3 - Moderate
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.2
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 actually 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-12331	Issue ID:	EFA-12331
	S3 – Moderate		

Parent Defect ID:	EFA-12331	Issue ID:	EFA-12331
Severity:			
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-12429	Issue ID:	EFA-12429
Reason Code:	Not Reproducible	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-12539	Issue ID:	EFA-12539
Reason Code:	Not a Software Defect	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		
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		

Open Defects

The following defects are open in Extreme Fabric Automation 2.7.0.

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		
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		

Parent Defect ID:	EFA-9570	Issue ID:	EFA-9570
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-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-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
	S3 - Moderate		

Parent Defect ID:	EFA-10063	Issue ID:	EFA-10063
Severity:			
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-12133	Issue ID:	EFA-12133
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.5.5
Symptom:	On the last port-group delete, VRF VRF1 is not cleaned up from the device, when the VRF is shared across the EPGs.		
Condition:	Below are the steps to reproduce the issue: 1. Create L3 EPG EPG1 with Device1Port1 and VRF1. 2. Create L3 EPG EPG2 with Device1Port2, Device2Port1, and VRF1 3. Update EPG EPG2 with "port-group-delete" of Device1Port2 4. Update EPG EPG1 with "port-group-delete" of Device1Port1. This is the last port getting deleted from the device which should have resulted in the deletion of the VRF VRF1 from the Device1.		
Recovery:	Recovery way 1: 1. Delete EPG1. 2. EPG2 update with port-group add D1P2 and then remove D1P2 from EPG. After the port removal D1P2 (last-port) vrf will be removed from the device. Recovery way 2: Manually remove the vrf from the device.. Inventory update.		

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-12600	Issue ID:	EFA-12600
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.3.2
Symptom:	EFA certificates have expired or about to expire.		
Recovery:	Perform the following steps to renew EFA certificates on 2.3.x and 2.4.x. 1. cd /apps/efa/efacerts 2. Generate a new certificate using the tls.key from <IP>-certs folder # openssl req -new -sha256 -key <IP>-certs/tls.key -subj "/CN=efa.extremenetworks.com" | openssl x509 -req -sha256 \ -CA /apps/efa/efacerts/extreme-ca.cert.pem \ -CAkey /apps/efa/efacerts/extreme-ca.key.pem \ -CAcreateserial \ -out newtls.crt -days 365 \ -extensions v3_req -extfile /apps/efa/efacerts/extreme-openssl.cnf-san 3. Install the new certificate into traefik using the following shell script # if ./install_efa_certs_st.sh --cert /apps/efa/efacerts/newtls.crt --key /apps/efa/efacerts/<IP>-certs/tls.key ; then cp newtls.crt <IP>-certs/tls.crt cp newtls.crt /apps/efadata/certs/own/tls.crt echo SUCCESS fi 4. Wait for the traefik pod to restart (1-2min) 5. Restart the running goraslog pod		

Parent Defect ID:	EFA-12710	Issue ID:	EFA-12710
	S2 - Major		

Parent Defect ID:	EFA-12710	Issue ID:	EFA-12710
Severity:			
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.7.0
Symptom:	With rollback , Multi-node upgrade with node replacement is not supported. This happens when user gives command efa deploy with-rollback for multi-node replacement, user is given option 1) Multi Node Build Upgrade and 2) Multi Node Build Upgrade With Node Replacement . If user chooses the option 2 Multi Node Build Upgrade With Node Replacement . Installer prompts "With rollback , replacement upgrade not supported Do you wish to restart the install? (yes/no)"		
Condition:	This happens when user gives command efa deploy with-rollback for Multi Node Build Upgrade With Node Replacement		
Workaround:	When the installer prompts, 1) Multi Node Build Upgrade and 2) Multi Node Build Upgrade With Node Replacement . if User presses option 2 , Installer promtps "With rollback , replacement upgrade not supported Do you wish to restart the install? (yes/no)" User can input no to halt the installation and press yes if he wants to go for option 1) Multi Node Build Upgrade		
Recovery:	When the installer prompts, 1) Multi Node Build Upgrade and 2) Multi Node Build Upgrade With Node Replacement . if User presses option 2 , Installer promtps "With rollback , replacement upgrade not supported Do you wish to restart the install? (yes/no)" User can input no to halt the installation		

Parent Defect ID:	EFA-12777	Issue ID:	EFA-12777
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.7.0
Symptom:	"efa inventory drift-reconcile execute --ip <device-ip>" fails with the status "tenant-dr-timeout" as the time taken to reconcile the scale drifted tenant configuration is beyond the timeout		

Parent Defect ID:	EFA-12777	Issue ID:	EFA-12777
Condition:	Below are the steps to reproduce the issue: 1. Introduce drift w.r.t the scaled tenant configuration e.g. 100 POs, 100 VRFs, 200 EPGs (with around 100 ctags), 300 BGP Peers, 100 BGP Peer-Groups 2. Execute "efa inventory drift-reconcile execute --ip <device-ip>"		
Workaround:	No workaround		
Recovery:	Below steps needs to be re-executed on the device for which the DRC had failed with the status "tenant-dr-timeout" 1. "efa inventory device update --ip <device-ip>" 2. "efa inventory drift-reconcile execute --ip <device-ip>"		

Parent Defect ID:	EFA-12823	Issue ID:	EFA-12823
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.7.0
Symptom:	Prefix Independent Convergence is not detected as drifted and it will not get reconciled.		
Condition:	Occasionally when preforming DRC in maintenance mode on reboot state, the Prefix Independent Convergence fails to detect refreshed state.		
Workaround:	Working around the drift detection is done by validating Prefix Independent Convergence has not drifted before reloading into maintenance mode.		
Recovery:	When Prefix Independent Convergence is not being detected as refreshed, re-configuring the value will allow drift detection to function.		

Parent Defect ID:	EFA-13036	Issue ID:	EFA-13036
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.7.0
Symptom:	EFA created Mirror Session with Global VLANs as the source is not deleted		
Condition:	Below are the steps to reproduce the issue: 1) Create Tenant and EndpointGroup with ctag-range 2) Create Mirror Session with Global VLANs (VLANs to be chosen from the ctag-range mentioned in step 1) as a mirror source 3) Delete EndpointGroup (created in Step1) with the force option		

Parent Defect ID:	EFA-13036	Issue ID:	EFA-13036
Workaround:	No workaround		
Recovery:	Delete Mirror Session using "efa tenant service mirror session delete --tenant <tenant-name> --name <mirror-session-name>"		

Parent Defect ID:	EFA-13080	Issue ID:	EFA-13080
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.7.0
Symptom:	Some configurations when removed from the device will not cause the EFA to move the device to cfg-refresh state.		
Condition:	Case1: EFA doesnt move device to config-refresh on device update. Config does NOT Reconcile on drift-reconcile: Fabric devices app state should be cfg-refreshed, after peer-keepalive configuration removed manually in slx Fabric devices app state should be cfg-refreshed, after "ip address" configuration under a fabric interface removed manually in slx Fabric devices app state should be cfg-refreshed, after loopback interface configuration under a fabric is removed manually in slx Fabric devices app state should be cfg-refreshed, after "address-family l2vpn evpn" is removed Fabric devices app state should be cfg-refreshed, after "no neighbor <ip> next-hop-self" is removed Case2 : EFA doesnt move device to config-refresh on device update. Config does Reconcile on drift-reconcile: Fabric devices app state should be cfg-refreshed, after "maximum-paths" configuration under router bgp removed manually in slx Fabric devices app state should be cfg-refreshed, after "graceful-restart" configuration under router bgp removed manually in slx		
Workaround:	Manually configure the device back in case 1 Run drift-reconcile OR manually configure device back will recover the config in case 2		

Parent Defect ID:	EFA-13083	Issue ID:	EFA-13083
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.7.0
Symptom:	"efa tenant po show", "efa tenant vrf show", "efa tenant epg show", "efa tenant service mirror session show" doesn't show the configuration in cfg-refreshed state even though the configurations (which should have been present but) are not present on the SLX		

Parent Defect ID:	EFA-13083	Issue ID:	EFA-13083
Condition:	Below are the steps to reproduce the issue 1. Configure fabric, tenant, po, vrf, epg, mirror session 2. Execute "efa system backup" 3. Delete the devices from inventory 4. Execute "efa system restore" using the backup taken in step 2 5. Execute "efa tenant po show", "efa tenant vrf show", "efa tenant epg show", "efa tenant service mirror session show"		
Recovery:	Execute "efa inventory device update --ip <device-ip>" and then check the output of "efa tenant po show", "efa tenant vrf show", "efa tenant epg show", "efa tenant service mirror session show" to see the configurations in cfg-refreshed state		

Parent Defect ID:	EFA-13124	Issue ID:	EFA-13124
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.7.0
Symptom:	When endpoint group create or update operation REST requests of multiple endpoint groups each with 50+ ctags are issued concurrently, one or two of the requests may fail with "Error 1452: Cannot add or update a child row: a foreign key constraint fails" or with an error indicating database timeout or an error indicating failure of network property delete.		
Condition:	When multiple endpoint group requests are processed concurrently, some of the database requests initiated by EFA may cause database to abort one of the request with the above mentioned error		
Workaround:	Execute the commands sequentially		
Recovery:	EFA database and SLX device configurations are always not affected by this error and hence no recovery is required. The failed commands shall be rerun sequentially to successful completion of the expected operations		

Parent Defect ID:	EFA-13158	Issue ID:	EFA-13158
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.7.0
Symptom:	"efa inventory drift-reconcile execute --ip <device-ip>" fails with the error "Error: Monitor session already configured"		

Parent Defect ID:	EFA-13158	Issue ID:	EFA-13158
Condition:	Below are the steps to reproduce the issue 1. Create a mirror session on an SLX device using EFA 2. Modify the mirror session configuration on SLX by changing any of the attributes e.g. source, destination, direction, etc. 3. Perform "efa inventory drift-reconcile execute --ip <device-ip> --reconcile"		
Recovery:	Delete existing monitor session from the device and then execute "efa inventory drift-reconcile execute --ip <device-ip>"		

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

Parent Defect ID:	EFA-13187	Issue ID:	EFA-13187
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.7.0
Symptom:	EFA REST CLI to fetch list of tenants may fail with error "Error : Cannot find Tenant <tenant-name>" when there are large number of tenants and epgs configured on them.		
Condition:	When there are large number of tenants with ports spanning across 30+ devices with multiple EPGs configured, database access can be under heavy load causing the above error		

Parent Defect ID:	EFA-13187	Issue ID:	EFA-13187
Workaround:	This is a transient error. Re-execute the same REST command. If this error is observed, information about individual tenant objects can be fetched by 'efa tenant show --name <tenant-name>'		
Recovery:	There is no recovery required as the EFA and SLX configurations are not altered as part of this issue		

Parent Defect ID:	EFA-13254	Issue ID:	EFA-13254
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.6.1
Symptom:	3 of EFA Pods fails Liveliness / Rediness checks causing Init containers to stop and causing crashloopback		

Parent Defect ID:	EFA-13281	Issue ID:	EFA-13281
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.7.0
Symptom:	When 'efa system backup' command is executed with copy to the remote system enabled and the error 'local error: tls: bad record MAC' is seen.		
Workaround:	The backup will be copied to the remote location and the error is harmless.		

Parent Defect ID:	EFA-13291	Issue ID:	EFA-13291
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.7.0
Symptom:	Trusted-Peer IP is configured as its own TPVM IP address during tpvm-upgrade		
Workaround:			

Parent Defect ID:	EFA-13322	Issue ID:	EFA-13322
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.7.0

Parent Defect ID:	EFA-13322	Issue ID:	EFA-13322
Symptom:	At the end of upgrade, the installer displays a message associated with a fresh install and not an upgraded install. The installer will show "Extreme Fabric Automation Stack is now deployed and ready" instead of "Extreme Fabric Automation Stack has been upgraded successfully" This is harmless and the upgrade procedure is unaffected.		
Condition:	When a single-node installation of EFA is upgraded using the SLX CLI with-rollback option		

Parent Defect ID:	EFA-13339	Issue ID:	EFA-13339
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.7.0
Symptom:	The EFA notification service does not send a syslog alert message when an EFA inventory device firmware-download operation fails.		
Condition:	The user attempts to prepare a device for a firmware download using "efa inventory device firmware-download prepare add --ip <device IP>" when the device's management connectivity is unreachable.		
Workaround:	Although the syslog alert message is not available, both the CLI and REST response contain an appropriate error message about the reason for the firmware-download prepare error and the device's connectivity issue.		
Recovery:	None		

Parent Defect ID:	EFA-13362	Issue ID:	EFA-13362
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.7.0
Symptom:	If the use manually removes "member-vlan-all" or " member-bd-all", from the SLX followed by DRC, then the entire cluster configuration will be deleted and recreated.		

Parent Defect ID:	EFA-13362	Issue ID:	EFA-13362
Condition:	1. Create a single rack fabric 2. If the use manually removes "member-vlan-all" or " member-bd-all", from the SLX followed by DRC.		
Workaround:	Manually restore the member-vlan or member-bridge-all configuration in cluster.		

Parent Defect ID:	EFA-13367	Issue ID:	EFA-13367
Severity:	S2 - Major		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.7.0
Symptom:	DRC does not restore config after MCT PO member port shutdown manually in SLX		
Condition:	Execute in device command 'shutdown' of member port of MCT PO. EFA device update brings the device to 'cfg-refresh' Execute Drift-reconcile for device does not bring the member port back up ie 'no shutdown' is not issued on member port interface.		
Workaround:	Execute on device 'no shutdown' on the interface manually on the device.		
Recovery:	Execute 'efa fabric configure' for fabric to bring devices in efa to in-sync state.		

Parent Defect ID:	EFA-13370	Issue ID:	EFA-13370
Severity:	S3 - Moderate		
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.7.0
Symptom:	No alert messages are sent to configured syslog relp subscribers when there is a failure while configuring inventory device interface settings such as admin state, speed, mtu etc.		
Condition:	The lack of logging occurs when there is a failure while configuring inventory device interface settings, such as a failure to establish connection to a device.		
Workaround:	The failure is logged in the inventory log file and can be reviewed there.		
Recovery:	Once the failure condition is corrected there is no need for an alert message to be sent to configured syslog relp subscribers.		

Parent Defect ID:	EFA-13379	Issue ID:	EFA-13379
	S3 - Moderate		

Parent Defect ID:	EFA-13379	Issue ID:	EFA-13379
Severity:			
Product:	Extreme Fabric Automation	Reported in Release:	EFA 2.7.0
Symptom:	Some of the backup routing neighbors get stuck in cfg-refreshed state and the same can be seen in the DRC output		
Condition:	Below are the steps to reproduce the issue 1. Create and configure a fabric with backup routing enabled 2. Create a Tenant, a PO, 5 VRFs and 5 EPGs 3. Update the fabric setting (for the fabric created in step 1) with md5 password 4. Perform fabric configure		
Recovery:	1. Remove backup routing neighbor md5-password from the VRFs which are in cfg-refreshed state (as seen in the DRC output) 2. Execute DRC to reconcile the configs and to move the cfg-refreshed configurations to cfg-in-sync		

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.