Extreme Visibility Manager Release Notes

6.0.0

9037084-00 Rev AA
June 2021

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/

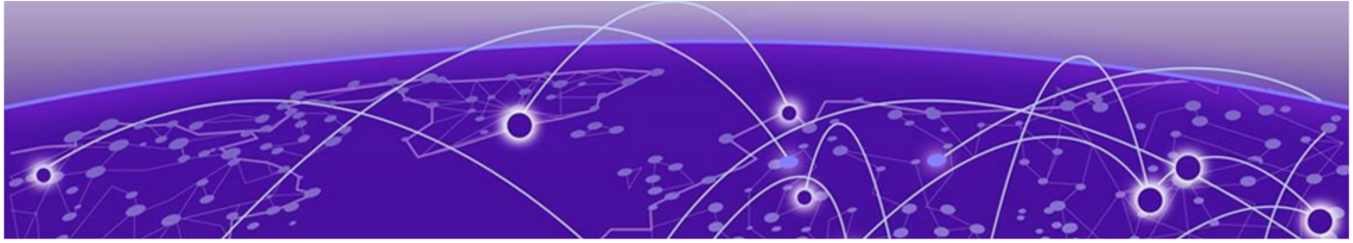
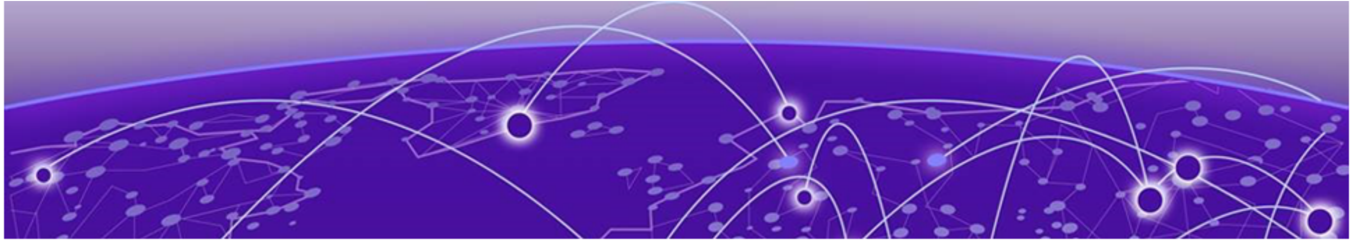


Table of Contents



Preface

Read the following topics to learn about:

- The meanings of text formats used in this document.
- Where you can find additional information and help.
- How to reach us with questions and comments.

Text Conventions

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as ExtremeSwitching switches or SLX routers, the product is referred to as *the switch* or *the router*.

Table 1: Notes and warnings

Icon	Notice type	Alerts you to...
💡	Tip	Helpful tips and notices for using the product
🗒	Note	Useful information or instructions
➡	Important	Important features or instructions
⚠	Caution	Risk of personal injury, system damage, or loss of data
⚠	Warning	Risk of severe personal injury

Table 2: Text

Convention	Description
`screen displays`	This typeface indicates command syntax, or represents information as it is displayed on the screen.
The words *enter* and *type*	When you see the word *enter* in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says *type*.
Key names	Key names are written in boldface, for example **Ctrl** or **Esc**. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press **Ctrl**+**Alt**+**Del**
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
italic text	Italic text indicates variable content.
`[ ]`	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ **x** | **y** | **z** }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, such as passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	In command examples, the backslash indicates a “soft” line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Documentation and Training

Find Extreme Networks product information at the following locations:

Current Product Documentation

Release Notes

Hardware and software compatibility for Extreme Networks products

Extreme Optics Compatibility

Other resources such as white papers, data sheets, and case studies

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit www.extremenetworks.com/education/.

Getting Help

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.

Providing Feedback

The Information Development team at Extreme Networks has made every effort to ensure the accuracy and completeness of this document. We are always striving to improve our documentation and help you work better, so we want to hear from you. We welcome all feedback, but we especially want to know about:

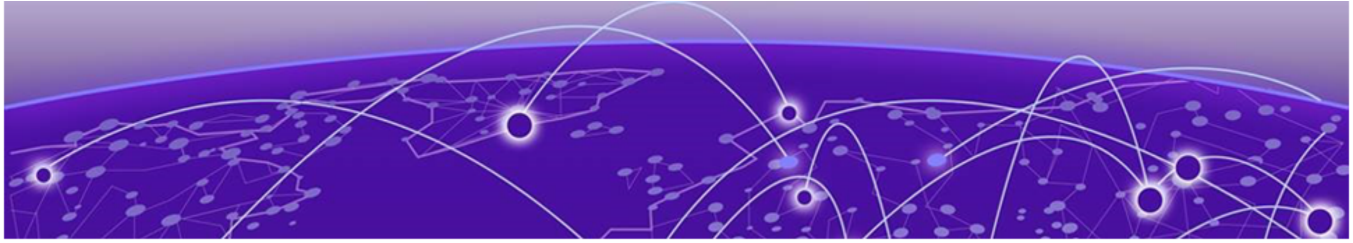
- Content errors, or confusing or conflicting information.

- Improvements that would help you find relevant information in the document.
- Broken links or usability issues.

If you would like to provide feedback, you can do so in three ways:

- In a web browser, select the feedback icon and complete the online feedback form.
- Access the feedback form at https://www.extremenetworks.com/documentation-feedback/.
- Email us at documentation@extremenetworks.com.

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.



Release Notes

Extreme Visibility Manager, a Kubernetes-based microservices application, provides centralized device and policy management as part of the Extreme Visibility solution.

New Features and Enhancements

Extreme Visibility Manager version 6.0.0 offers the following features and enhancements.

Table 4: Features and enhancements

Feature	Description
Region and zone-based architecture	With Visibility Manager, you can manage devices across multiple data centers and geographic locations. You can separate locations into regions and further separate regions into zones. A zone is a set of locations (at least one and no more than five) where devices reside.
Support for the new Extreme 9920 device	The device runs the NPB application, which provides network packet broker functionality. For more information, see Supported Devices on page 9.
Support for SLX and MLX devices	Visibility Manager continues support for the devices that you are monitoring with a previous version of the product. For more information, see Supported Devices on page 9.
Device discovery	Devices are specified by location in a Device Definition file, which you add to Visibility Manager by drag-and-drop or browsing. Discovered devices are grouped on the Configure page by location or device type.
Device types and versions	Device types and device type versions are specified in a Device Type Version Capabilities (DTVC) file, which you add to Visibility Manager by drag-and-drop or browsing.

Table 4: Features and enhancements (continued)

Feature	Description
Locations	Device locations are specified in a locations.csv file. You create the file and upload it during Visibility Manager installation.
Library for rule matches and policies	Matches and policies that you create in the library can be applied to any device that you monitor
Per-device configuration	Device configuration in Visibility Manager mimics the functionality of command-line interface commands running on device operating systems. You can configure the following: • Policies • Policy rule matches • Ingress groups and egress groups • Tunnels • Port channels and ports
Built-in and custom dashboards	Dashboards display real-time streaming data for at-a-glance monitoring of selected devices and metrics.
Service chains	Service chains are graphical representations of the relationship between groups and policies for a selected device. You can easily see where a policy is used and how often.
User, system, and device logs	User logs identify user transactions related to devices, device configuration, and device type. System logs describe the status of Extreme 9920 devices. Device-specific logs identify events in real time.
Role-based access control (RBAC)	RBAC determines which functions a user can perform, based on the user's role. Visibility Manager has two roles, System Admin and Network Operator, each with different permissions for various functions.

Supported Devices

Extreme Visibility Manager supports several devices and their software.

Table 5: Supported devices and software

Device	Supported Software
Extreme 9920	Extreme 9920 software, version 21.1.0.0, with the NPB application
ExtremeRouting MLX series	NetIron 06.3.00d
ExtremeSwitching SLX 9140	SLX-OS 18s.1.03a, SLX-OS 18s.1.03b
ExtremeSwitching SLX 9240	SLX-OS 18s.1.03a, SLX-OS 18s.1.03b

System Requirements

Extreme Visibility Manager is installed on multiple virtual machines (VMs).

VM requirements

VM Type	Minimum Number of VMs	System Requirements	Maximum Devices
Control plane	1	• 2 vCPU • 4 GB RAM • 32 GB storage	N/A
Region	3	• 4 vCPU • 16 GB RAM • 200 GB storage	100 devices per region
Zone	1	• 2 vCPU • 4 GB RAM • 32 GB storage	25 devices per zone

System prerequisites

- Install `libguestfs-tools` (for quick installation) on the Hypervisor where VMs are hosted.

  ```
  sudo yum install libguestfs-tools
  ```

- Do not use the `192.168.0.0/16` series of IP addresses as management IP addresses for VMs.
- Do not use capital letters in host names.
- Ensure that all VMs have the same time zone as the devices that you want to monitor.

  ```
  timedatectl set-timezone <time-zone>
  ```

Supported connection protocols

Connections between Visibility Manager and the Extreme 9920 device are over secure TLS.

Connections between Visibility Manager and SLX or MLX devices are over UDP without TLS.

Browser requirements

You can access the Visibility Manager user interface with the following browsers:

- Google Chrome
- Mozilla Firefox

Certificate requirements

Visibility Manager uses HTTPS and requires self-signed certificates.

Installation

For complete information about installing Extreme Visibility Manager, see the *Extreme Visibility Manager Deployment Guide, 6.0.0*.

Limitations and Restrictions

Note the following caveats for this release of Extreme Visibility Manager.

Listener policy byte count is incorrect when truncation is enabled

On the Extreme 9920 device, the byte count for truncated packets is the actual byte count seen by the egress ACL before truncation.

LACP LAG is not supported for Extreme 9920 devices

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

Only one region is supported

This release of Visibility Manager supports the creation and management of only one region.

Open Defects

The following defects are open in this release of Extreme Visibility Manager.

Parent Defect ID:	XVM-562	Issue ID:	XVM-562
Severity:	S2 - High		
Product:	XVM	Reported in Release:	XVM 0.1.0
Symptom:	During the device discovery using the CSV file upload, if any of the given parameters are wrong in the input for some entries (except the ip address), No error message is shown in the GUI.		
Condition:	If the major parameters like IP Address, Device Version, User Name or Password are wrong, device discovery failure is shown on the GUI		
Workaround:	Making sure that all the parameters are correct before uploading the CSV file for the discovery		
Recovery:	Unless the major parameters like IP Address, Device Version, User Name or Password are wrong device discovery will work fine. If these major parameters are wrong, discovery will fail and user needs to do the retry of the discovery after correcting them		

Parent Defect ID:	XVM-828	Issue ID:	XVM-828
Severity:	S3 - Medium		
Product:	XVM	Reported in Release:	XVM 0.1.0
Symptom:	When user wants to delete Device Type for a specific location there is no option to do the same in Manage Device Types		
Condition:	When user wants to delete Device Type for specific location		

Parent Defect ID:	XVM-828	Issue ID:	XVM-828
Workaround:	User needs to delete Device Type which will be deleted for all the locations.		
Recovery:	User needs to delete Device Type for all locations and then add Device Type for needed location again.		

Parent Defect ID:	XVM-1409	Issue ID:	XVM-1409
Severity:	S2 - High		
Product:	XVM	Reported in Release:	XVM 0.1.0
Symptom:	Sometime user notification shows a hour glass		
Condition:	Observed once when portchannel is added		
Workaround:	No functional loss.		
Recovery:	No functional loss.		

Parent Defect ID:	XVM-1738	Issue ID:	XVM-1738
Severity:	S3 - Medium		
Product:	XVM	Reported in Release:	XVM 0.1.0
Symptom:	When user choses to breakout ports, the broken parts are shown at the top of the Ports config object instead at its original order		
Condition:	When port breakout option is done for a port		
Workaround:	The page needs to be refreshed to see the ports in the correct order		
Recovery:	usabiliy issue with no functional impact. Hence no recovery steps required.		

Parent Defect ID:	XVM-1844	Issue ID:	XVM-1844
Severity:	S3 - Medium		
Product:	XVM	Reported in Release:	XVM 6.0.0
Symptom:	Device specific error message with an error code is seen while performing configuration operation due to permission issues.		
Condition:	Discover a 9920 device with a user having role 'user' and perform config operation.		
Workaround:	To discover a 9920 device, always use a user who has 'admin' privileges.		

Parent Defect ID:	XVM-1993	Issue ID:	XVM-1993
Severity:	S2 - High		
Product:	XVM	Reported in Release:	XVM 6.0.0
Symptom:	Device add failure with an error "Already present"		
Condition:	Happens when the device is upgraded when it is already discovered from xvm.		

Parent Defect ID:	XVM-1993	Issue ID:	XVM-1993
Workaround:	Delete all dtcv for the device		
Recovery:	Delete all dtcv for the device		

Parent Defect ID:	XVM-2121	Issue ID:	XVM-2121
Severity:	S3 - Medium		
Product:	XVM	Reported in Release:	XVM 6.0.0
Symptom:	Ingress policy and Egress policy charts are not getting populated		
Condition:	When the device dashboard is accessed immediately after discovery, policy charts are not displayed.		
Workaround:	Refresh the page or toggle the tabs.		

Parent Defect ID:	XVM-2123	Issue ID:	XVM-2123
Severity:	S1 - Critical		
Product:	XVM	Reported in Release:	XVM 6.0.0
Symptom:	While Installing qcow, the IP address doesnot recognize the format IPADDRESS/PREFIX		
Workaround:	The IP Address should be given in format "aaa.bbb.ccc.ddd" or The details containing w.r.t to vm in file xvmconf can be pushed to qcow as explained in installation document.		

Parent Defect ID:	XVM-2125	Issue ID:	XVM-2125
Severity:	S2 - High		
Product:	XVM	Reported in Release:	XVM 6.0.0
Symptom:	Some of the services will fail to start.		
Condition:	Issue was seen after multiple regional VM reboots scenario.		

Parent Defect ID:	XVM-2125	Issue ID:	XVM-2125
Workaround:	1. Power on Leader node 2. backup old data folder on problematic regional nodes. "mv /var/lib/pgsql/12/data /var/lib/pgsql/12/data_org 3. execute below command "pg_basebackup -h <Leader regional IP> -U cmon_replication -Xs -P -R -D /var/lib/postgresql/12/data" 4 Execute below command and wait for State to change from "creating Replica" to running. [root@ ~]# patronictl -c /opt/app/patroni/etc/postgresql.yml list postgres + Cluster: postgres (6969515509939729866) -------------------- MemberHostRoleStateTLLag in MB --+ pg_10.37.136.16210.37.136.162 running20 pg_10.37.136.16310.37.136.163Leaderrunning pg_10.37.136.16410.37.136.164 running80		
Recovery:	1. Power on Leader node 2. backup old data folder on problematic regional nodes. "mv /var/lib/pgsql/12/data /var/lib/pgsql/12/data_org 3. execute below command "pg_basebackup -h <Leader regional IP> -U cmon_replication -Xs -P -R -D /var/lib/postgresql/12/data" 4 Execute below command and wait for State to change from "creating Replica" to running. [root@ ~]# patronictl -c /opt/app/patroni/etc/postgresql.yml list postgres + Cluster: postgres (6969515509939729866) -------------------- Member Host Role State TL Lag in MB --+ pg_10.37.136.162 10.37.136.162 running 2 0 pg_10.37.136.163 10.37.136.163 Leader running pg_10.37.136.164 10.37.136.164 running 8 0 We can prevent this issue by monitoring patroni instances and checking for last column of "Lag in MB", if count is not coming back to 0 for long time we can follow above steps to recover.		

Parent Defect ID:	XVM-2128	Issue ID:	XVM-2128
Severity:	S2 - High		
Product:	XVM	Reported in Release:	XVM 6.0.0
Symptom:	"Region Service Message Processing Timedout" message shown on UI when user tries to delete the same ACL multiple times before receiving the notification/ confirmation for the first delete operation. No impact on XVM functionality.		
Condition:	When user continuously clicks on delete button of Policy Match Rule to delete the same ACL without waiting for delete notification from XVM.		
Workaround:	Wait for the successful or failure notification from XVM.		

Parent Defect ID:	XVM-2130	Issue ID:	XVM-2130
	S2 - High		

Parent Defect ID:	XVM-2130	Issue ID:	XVM-2130
Severity:			
Product:	XVM	Reported in Release:	XVM 6.0.0
Symptom:	NGNPB configuration details are not displayed on XVM UI after migrating policy, rules from MLX/SLX devices.		
Condition:	When ACL rules, policy configuration of source device has syntax/semantic conflicts with NGNPB accepted configuration.		
Workaround:	Refresh configuration of the NGNPB device again to display the details.		

Parent Defect ID:	XVM-2135	Issue ID:	XVM-2135
Severity:	S3 - Medium		
Product:	XVM	Reported in Release:	XVM 6.0.0
Symptom:	Delay observed in processing of multiple devices discovery using CSV file, resulting in UI "Processing your request message will be appearing"		
Condition:	Discover > 5 devices using CSV file.		
Workaround:	Add less number of devices (< 5) from CSV file and repeat the same when we have multiple devices		
Recovery:	There is no functionality issue, the add window will be present for more time and will disappear once discovery completed.		

Parent Defect ID:	XVM-2141	Issue ID:	XVM-2141
Severity:	S3 - Medium		
Product:	XVM	Reported in Release:	XVM 6.0.0
Symptom:	Policy and Matches cannot have the same name in XVM across the different types even if it is allowed on the device.		
Condition:	The issue is seen when the same name is provided for different type of match or different policies and configuration is not allowed to apply.		
Workaround:	Provide different names for different type of policy or the matches.		
Recovery:	There will be error seen if same name is provided and configuration is not allowed to apply. So no recovery is needed.		

Parent Defect ID:	XVM-2142	Issue ID:	XVM-2142
Severity:	S3 - Medium		
Product:	XVM	Reported in Release:	XVM 6.0.0
Symptom:	Duplicate port entries are seen in the interface statistics dashboard.		

Parent Defect ID:	XVM-2142	Issue ID:	XVM-2142
Condition:	When the SCS service gets re-initialized, the duplicate entries are seen in the statistics dashboard.		
Workaround:	Refresh the page, new stats entries will be updated correctly.		

Parent Defect ID:	XVM-2148	Issue ID:	XVM-2148
Severity:	S3 - Medium		
Product:	XVM	Reported in Release:	XVM 6.0.0
Symptom:	Deleting egress object with Network Operator role displays incorrect message saying "Delete Request Failed".		
Condition:	When user with Network Operator role deletes egress or any config object		
Workaround:	There is no functionality loss, hence no workaround required.		
Recovery:	No Recovery is required as there is no functional issue.		

Parent Defect ID:	XVM-2149	Issue ID:	XVM-2149
Severity:	S3 - Medium		
Product:	XVM	Reported in Release:	XVM 6.0.0
Symptom:	Tunnel origination configuration is not reverted to previous state incase of failure notifications.		
Condition:	Tunnel origination configuration rejected from device due to incorrect address.		
Workaround:	Configuration can be deleted and added again with correct values.		

Parent Defect ID:	XVM-2151	Issue ID:	XVM-2151
Severity:	S3 - Medium		
Product:	XVM	Reported in Release:	XVM 6.0.0
Symptom:	Adding back the same ACL match rule which was deleted using the same window fails.		
Condition:	Delete and re add the same ACL match rule.		
Workaround:	Close the current ACL edit window and retry.		

Parent Defect ID:	XVM-2160	Issue ID:	XVM-2160
Severity:	S2 - High		
Product:	XVM	Reported in Release:	XVM 6.0.0
Symptom:	Some times, SFMS Service gets re-initiated while trying to fetch service chains in a scaled environment.		

Parent Defect ID:	XVM-2160	Issue ID:	XVM-2160
Condition:	In scaled environment with bulk configuration.		
Workaround:	No functional impact. Re-initiated Service continues to work normally.		

Parent Defect ID:	XVM-2162	Issue ID:	XVM-2162
Severity:	S2 - High		
Product:	XVM	Reported in Release:	XVM 6.0.0
Symptom:	Configuration is reconciled from device and old config is retained after Refresh Configuration (on-demand reconciliation).		
Condition:	1. When refresh configuration is performed after rebooting the device. 2. Applying default config on device, this reboots the device.		
Workaround:	Wait for few minutes (~4-5) before executing refresh configuration. This will allow XVM to reconnect to the device services.		

Parent Defect ID:	XVM-2164	Issue ID:	XVM-2164
Severity:	S3 - Medium		
Product:	XVM	Reported in Release:	XVM 6.0.0
Symptom:	Device discovery fails with an error notification		
Condition:	Rediscover a device that is in the error state due to incorrect DTCV and location.		
Workaround:	Delete the device in the error state and rediscover it with the correct DTCV and location information.		

Parent Defect ID:	XVM-2165	Issue ID:	XVM-2165
Severity:	S3 - Medium		
Product:	XVM	Reported in Release:	XVM 6.0.0
Symptom:	Session expiry alert is shown multiple times		
Condition:	When configuration page is opened with consolidated view.		
Workaround:	Need to click alert multiple times to view the login page.		
Recovery:	Recovery is not needed as there is no functionality loss.		

Parent Defect ID:	XVM-2180	Issue ID:	XVM-2180
Severity:	S2 - High		
Product:	XVM	Reported in Release:	XVM 6.0.0
Symptom:	The ingress group dashboard chart is not populated with data.		

Parent Defect ID:	XVM-2180	Issue ID:	XVM-2180
Condition:	Reconciliation of an ingress group added through CLI after device discovery.		
Workaround:	Delete and rediscover the device.		

Parent Defect ID:	XVM-2182	Issue ID:	XVM-2182
Severity:	S1 - Critical		
Product:	XVM	Reported in Release:	XVM 6.0.0
Symptom:	Techsupport cannot be done from control plane VM		
Workaround:	Techsupport can be executed in machine where install files are downloaded		

Parent Defect ID:	XVM-2185	Issue ID:	XVM-2185
Severity:	S3 - Medium		
Product:	XVM	Reported in Release:	XVM 6.0.0
Symptom:	Notification is updated with a successful device discovery message even though the discovery failed.		
Condition:	Rediscover a device that is in the error state with incorrect DTCV and location change.		
Workaround:	Delete the device in the error state and rediscover it with the correct DTCV and location information.		

Parent Defect ID:	XVM-2192	Issue ID:	XVM-2192
Severity:	S3 - Medium		
Product:	XVM	Reported in Release:	XVM 6.0.0
Symptom:	In installation tar file, controlplane.conf, region.conf and zone.conf , if NTP_CONF="0" , still configuring for NTP		
Condition:	In installation tar file , controlplane.conf, region.conf and zone.conf , if NTP_CONF="0" , still configuring for NTP		
Workaround:	in controlplane.conf, region.conf and zone.conf , making NTP_CONF=0 (without double quotes)		