



Avaya Virtual Services Platform 4000 Fault Management

Release 5.1.2
NN46251-702
Issue 09.01
January 2017

© 2013-2017, Avaya, Inc.
All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

"Documentation" means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: <https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010> under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

"Hosted Service" means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, [HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO](https://support.avaya.com/LICENSEINFO) UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR

IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO](https://support.avaya.com/LICENSEINFO), UNDER THE LINK "AVAYA SOFTWARE LICENSE TERMS (Avaya Products)" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

Licence types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at <https://support.avaya.com/LicenseInfo> under the link "Heritage Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the

documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: <https://support.avaya.com/Copyright> or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE

[WWW.SIPRO.COM/CONTACT.HTML](http://www.sipro.com/contact.html). THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: <https://support.avaya.com> or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of <https://support.avaya.com/security>.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (<https://support.avaya.com/css/P8/documents/100161515>).

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: <https://support.avaya.com>, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: <https://support.avaya.com> for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: <https://support.avaya.com> (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction	6
Purpose.....	6
Related resources.....	6
Support.....	9
Chapter 2: New in this document	11
Chapter 3: Fault management fundamentals	12
Local alarms.....	12
Link state change control.....	12
Connectivity Fault Management.....	13
Chapter 4: Key Health Indicators using ACLI	14
Displaying KHI performance information.....	14
Displaying KHI control processor information.....	21
Clearing KHI information.....	22
Displaying KHI Fabric Extend ONA status.....	22
Displaying KHI Fabric Extend ONA global information.....	24
Chapter 5: Key Health Indicators using EDM	26
Clearing KHI statistics.....	26
Displaying KHI port information.....	27
Chapter 6: Link state change control using ACLI	28
Controlling link state changes.....	28
Displaying link state changes.....	29
Chapter 7: Link state change control using EDM	30
Controlling link state changes.....	30
Chapter 8: Log and trap fundamentals	31
Overview of traps and logs.....	31
Secure syslog.....	33
Simple Network Management Protocol.....	34
Log message format.....	35
Log files.....	38
Log file transfer.....	39
Chapter 9: Log configuration using ACLI	41
Configuring a UNIX system log and syslog host.....	41
Variable definitions.....	43
Job aid.....	44
Configuring secure forwarding.....	45
Variable definitions.....	46
Installing root certificate for syslog client.....	47
Variable definition.....	48

Configuring logging.....	48
Configuring the remote host address for log transfer.....	50
Configuring system logging.....	51
Configuring system message control.....	52
Extending system message control.....	53
Viewing logs.....	54
Configuring ACLI logging.....	57
Chapter 10: Log configuration using EDM.....	59
Configuring the system log.....	59
Configuring the system log table.....	60
Chapter 11: SNMP trap configuration using ACLI.....	62
Configuring an SNMP host.....	62
Configuring an SNMP notify filter table.....	63
Configuring SNMP interfaces.....	65
Enabling SNMP trap logging.....	66
Chapter 12: SNMP trap configuration using EDM.....	68
Configuring an SNMP host target address.....	68
Configuring target table parameters.....	70
Configuring an SNMP notify table.....	71
Configuring SNMP notify filter profiles.....	71
Configuring SNMP notify filter profile table parameters.....	72
Enabling SNMP trap logging.....	73

Chapter 1: Introduction

Purpose

This document provides information on features in VSP Operating System Software (VOSS). VOSS runs on the following product families:

- Avaya Virtual Services Platform 4000 Series
- Avaya Virtual Services Platform 7200 Series
- Avaya Virtual Services Platform 8000 Series

Fault Management provides information about how to prevent faults and improve the performance of the Avaya Virtual Services Platform 4000 Series. This includes procedures for link state change, key health indicators, and logs and traps.

The fault management function supports tasks related to managing or preventing faults, troubleshooting, and monitoring and improving the performance of the network or product.

For information on fault management function on Avaya Virtual Services Platform 7200 Series and 8000 Series switches, see *Managing Faults on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-702.

Related resources

Documentation

See the *Documentation Roadmap for Avaya Virtual Services Platform 4000 Series*, NN46251-100 for a list of the documentation for this product.

Training

Ongoing product training is available. For more information or to register, access the website at <http://avaya-learning.com/>.

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support website, go to <http://support.avaya.com> and perform one of the following actions:
 - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
 - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
 - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
 - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

 **Note:**

Videos are not available for all products.

Subscribing to e-notifications

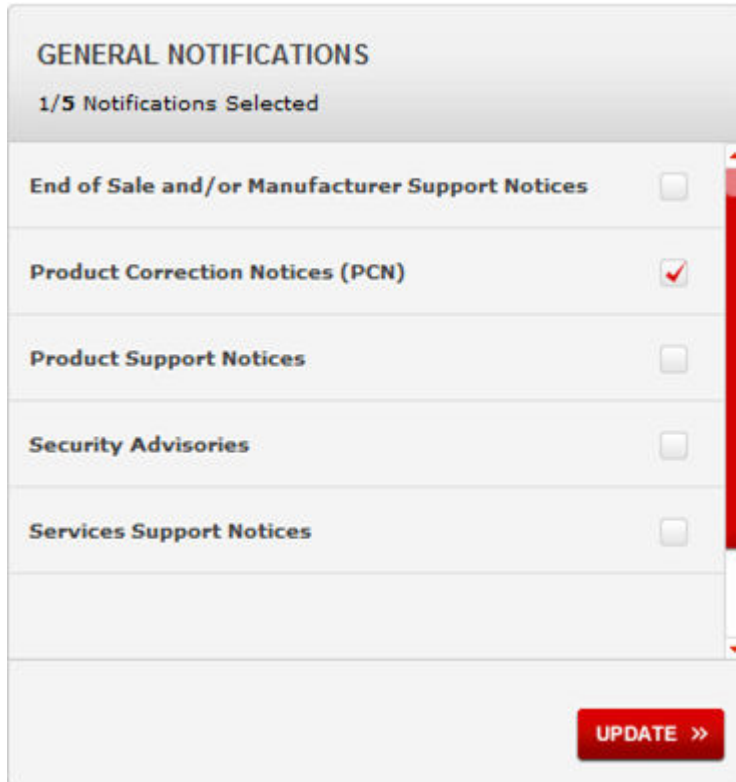
Subscribe to e-notifications to receive an email notification when documents are added to or changed on the Avaya Support website.

About this task

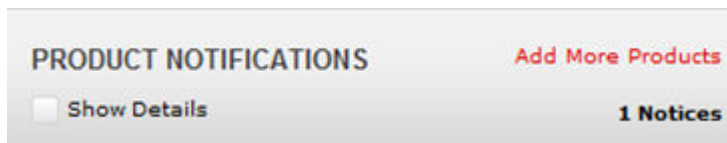
You can subscribe to different types of general notifications, for example, Product Correction Notices (PCN), which apply to any product or a specific product. You can also subscribe to specific types of documentation for a specific product, for example, Application & Technical Notes for Virtual Services Platform 7000.

Procedure

1. In an Internet browser, go to <https://support.avaya.com>.
2. Type your username and password, and then click **Login**.
3. Under **My Information**, select **SSO login Profile**.
4. Click **E-NOTIFICATIONS**.
5. In the GENERAL NOTIFICATIONS area, select the required documentation types, and then click **UPDATE**.



6. Click **OK**.
7. In the PRODUCT NOTIFICATIONS area, click **Add More Products**.



8. Scroll through the list, and then select the product name.
9. Select a release version.
10. Select the check box next to the required documentation types.

The screenshot shows two side-by-side panels. The left panel, titled 'PRODUCTS', has a 'My Notifications' link in the top right. It contains a list of product names: Virtual Services Platform 7000, Virtualization Provisioning Service, Visual Messenger™ for OCTEL® 250/350, Visual Vectors, Visualization Performance and Fault Manager, Voice Portal, Voice over IP Monitoring, W310 Wireless LAN Gateway, WLAN 2200 Series, and WLAN Handset 2200 Series. The right panel, titled 'VIRTUAL SERVICES PLATFORM 7000', has a 'Select a Release Version' dropdown menu set to 'All and Future'. Below this are several checkboxes: 'Administration and System Programming' (unchecked), 'Application Developer Information' (unchecked), 'Application Notes' (unchecked), 'Application and Technical Notes' (checked), 'Declarations of Conformity' (unchecked), and 'Documentation Library' (checked). A red 'SUBMIT >>' button is located at the bottom right of the right panel.

11. Click **Submit**.

Support

Go to the Avaya Support website at <http://support.avaya.com> for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Searching a documentation collection

On the Avaya Support website, you can download the documentation library for a specific product and software release to perform searches across an entire document collection. For example, you can perform a single, simultaneous search across the collection to quickly find all occurrences of a particular feature. Use this procedure to perform an index search of your documentation collection.

Before you begin

- Download the documentation collection zip file to your local computer.
- You must have Adobe Acrobat or Adobe Reader installed on your computer.

Procedure

1. Extract the document collection zip file into a folder.
2. Navigate to the folder that contains the extracted files and open the file named `<product_name_release>.pdx`.

3. In the Search dialog box, select the option **In the index named <product_name_release>.pdx.**
4. Enter a search word or phrase.
5. Select any of the following to narrow your search:
 - Whole Words Only
 - Case-Sensitive
 - Include Bookmarks
 - Include Comments
6. Click **Search**.

The search results show the number of documents and instances found. You can sort the search results by Relevance Ranking, Date Modified, Filename, or Location. The default is Relevance Ranking.

Chapter 2: New in this document

The following section details what is new in *Fault Management of Avaya Virtual Services Platform 4000 Series*, NN46251-702.

Release 5.1.2

Secure syslog

This release introduces the Secure syslog feature that provides security for the communication path between a syslog server and a syslog client.

For more information, see:

- [Secure syslog](#) on page 33
- [Configuring secure forwarding using ACLI](#) on page 45
- [Configuring cert-store with TLS using ACLI](#) on page 47
- [Configuring the system log table using EDM](#) on page 60

Release 5.1.1

Remote Monitoring (RMON)

All of the RMON configuration procedures were consolidated into one document. For RMON1 and RMON2 information, see *Performance Management of Avaya Virtual Services Platform 4000 Series*, NN46251-701.

Chapter 3: Fault management fundamentals

Fault management includes the tools and features available to monitor and manage faults. This section provides overview for local alarms, link state changes (port flapping), and Connectivity Fault Management.

Local alarms

Avaya Virtual Services Platform 4000 Series contains a local alarms mechanism. Local alarms are raised and cleared by applications running on the switch. Active alarms are viewed using the `show alarm database` command in ACLI. Local alarms are an automatic mechanism run by the system that do not require any additional user configuration. Check local alarms occasionally to ensure no alarms require additional operator attention. The raising and clearing of local alarms also creates a log entry for each event.

Link state change control

Rapid fluctuation in a port link state is called link flapping.

Link flapping is detrimental to network stability because it can trigger recalculation in spanning tree and the routing table.

If the number of port down events exceeds a configured limit during a specified interval, the system forces the port out of service.

You can configure link flap detection to control link state changes on a physical port. You can set thresholds for the number and frequency of changes allowed.

You can configure the system to take one of the following actions if changes exceed the thresholds:

- send a trap
- bring down the port

If changes exceed the link state change thresholds, the system generates a log entry.

Connectivity Fault Management

The Shortest Path Bridging MAC (SPBM) network needs a mechanism to debug connectivity issues and isolate faults. This function is performed at Layer 2, not Layer 3. Connectivity Fault Management (CFM) operates at Layer 2 and provides an equivalent of the `ping` and `traceroute` commands. To support troubleshooting of the SPBM cloud, Virtual Services Platform 4000 supports a subset of CFM functionality. For more information about CFM, see *Configuring Avaya Fabric Connect on VSP Operating System Software*, NN47227-510.

Chapter 4: Key Health Indicators using ACLI

The Key Health Indicators (KHI) feature of Avaya Virtual Services Platform 4000 Series provides a subset of health information that allows for quick assessment of the overall operational state of the device.

*** Note:**

The KHI feature is not intended to provide a comprehensive debugging solution. Instead, KHI identifies key information that could lead Avaya support personnel towards discovery of a specific failure. After the technician assesses the KHI information, further debugging is required to determine the specific reason for the fault.

Avaya recommends that you capture KHI information during normal operations to provide a baseline for Avaya support personnel when detecting fault situations.

Displaying KHI performance information

About this task

Use the following commands to display information about the performance of the Key Health Indicator feature.

Procedure

1. Display buffer performance and utilization statistics for KHI:

```
show khi performance buffer-pool [{slot[-slot][, ...]]}
```

2. Show current utilization, 5-minute average utilization, and 5-minute high water mark with date and time of event:

```
show khi performance cpu [{slot[-slot][, ...]]}
```

3. Display memory performance and utilization statistics for KHI on the specified slot or all slots:

```
show khi performance memory [{slot[-slot][, ...]]}
```

4. Display process performance and utilization statistics for KHI on the specified slot or all slots:

```
show khi performance process [{slot[-slot][, ...]]}
```

5. Display thread performance and utilization statistics for KHI on the specified slot or all slots:

```
show khi performance pthread [{slot[-slot][, ...]]
```

6. Display internal memory management resource performance and utilization statistics for KHI on the specified slot or all slots:

```
show khi performance slabinfo [{slot[-slot][, ...]]
```

Example

```
VSP-4850GTS#show khi performance buffer-pool 1
```

```
Slot:1
CPP:
  UsedFBuffs: 1
  FreeFBuffs: 1599
  NoFbuff: 0

Network stack system:
  UsedMbuf: 52
  FreeMbuf: 47798
  SocketMbuf: 15

Network stack data:
  UsedMbuf: 1
  FreeMbuf: 10751

Letter API message queue:
  QHigh: 0
  QNormal: 0
  FreeQEntries: 51200
```

```
VSP-4850GTS#show khi performance cpu 1
```

```
Slot:1
  Current utilization: 11
  5-minute average utilization: 10
  5-minute high water mark: 13 (02/13/13 14:00:47)
```

```
Switch:1>show khi performance memory 1
```

```
Slot:1
  Used: 514560 (KB)
  Free: 521260 (KB)
  Current utilization: 49 %
  5-minute average utilization: 49 %
  5-minute high water mark: 49 (02/13/13 09:41:24)
```

```
VSP-4850GTS#show khi performance process 1
```

```
Slot:1
```

PID	PPID	PName	VmSize	VmLck	VmRss	VmData	VmStk	VmExe	VmLib
1	0	init	1892	0	652	164	88	32	1512
2	0	kthreadd	0	0	0	0	0	0	0
3	2	ksoftirqd/0	0	0	0	0	0	0	0
4	2	events/0	0	0	0	0	0	0	0
5	2	khelper	0	0	0	0	0	0	0
8	2	async/mgr	0	0	0	0	0	0	0
73	2	sync_supers	0	0	0	0	0	0	0
75	2	bdi-default	0	0	0	0	0	0	0
77	2	kblockd/0	0	0	0	0	0	0	0
89	2	khubd	0	0	0	0	0	0	0
104	2	rpciod/0	0	0	0	0	0	0	0
128	2	kswapd0	0	0	0	0	0	0	0
180	2	aio/0	0	0	0	0	0	0	0

Key Health Indicators using ACLI

```

184 2      nfsiod      0      0      0      0      0      0      0
191 2      crypto/0    0      0      0      0      0      0      0
265 2      mtddbckd   0      0      0      0      0      0      0
426 1      udevd      2216   0      604    172    88     96     1628
515 2      scsi_eh_0  0      0      0      0      0      0      0
521 2      usb-storage 0      0      0      0      0      0      0
1912 1     portmap    1876   0      408    164    88     16
1512                                     1925 1
rc          3108   0      1368   132    88     736    1764
1936 1      sshd       4896   0      908    372    88     392    3328
1941 1      syslogd    2432   0      624    172    88     564    1512
943 1      klogd      2432   0      612    172    88     564    1512
1944 1925  S25vssp    3272   0      1560   296    88     736    1764
015 1944  rc.appfs.vsp4k 3128   0      1416   152    88     736    1764
4266 2      wdd        0      0      0      0      0      0      0
4306 2      i2c_wq     0      0      0      0      0      0      0
4320 2      sfp_q      0      0      0      0      0      0      0
4322 2      psu_q      0      0      0      0      0      0      0
4342 2      workqueue_0 0      0      0      0      0      0      0
4349 2      workqueue_1 0      0      0      0      0      0      0
387 4015  start      3116   0      1380   140    88     736    1764
4420 4387  lifecycle  13520  0      4572   3924   88     376    6456
4425 4420  logger     2436   0      680    176    88     564    1512
4434 4420  sockserv   4148   0      996    68     88     8      3452
4435 4420  oom95      61744  0      55008  53648  88     68     6104
4436 4434  logger     2436   0      584    176    88     564    1512
4437 4420  oom90      61744  0      55008  53648  88     68     6104
4438 4435  logger     2436   0      584    176    88     564    1512
4439 4437  logger     2436   0      580    176    88     564    1512
4440 4420  imgsync.x  12724  0      4052   3916   88     112    6324
4441 4440  logger     2436   0      680    176    88     564    1512
4486 4420  logServer  14336  0      4796   3436   88     1396   7136
4487 4420  trcServer  9308   0      3100   1512   88     88     5928
4488 4420  cbcp-main.x 424180 0      305904 364408 88     39416  10856
4489 4487  logger     2436   0      580    176    88     564    1512
4490 4420  rssServer  9412   0      3128   1512   88     108    5948
4491 4420  dbgServer  9336   0      3116   1512   88     116    5928
4492 4486  logger     2436   0      680    176    88     564    1512
4493 4488  logger     2436   0      684    176    88     564    1512
4494 4490  logger     2436   0      580    176    88     564    1512
4495 4491  logger     2436   0      580    176    88     564    1512
4496 4420  dbgShell   9276   0      3060   1512   88     64     5928
4497 4420  coreManager.x 11892  0      3720   3648   88     92     6168
4498 4496  logger     2436   0      580    176    88     564    1512
4499 4420  cbio-main.x 142868 0      50360  115396 88     14232  6292
4500 4497  logger     2436   0      580    176    88     564    1512
4501 4499  logger     2436   0      684    176    88     564    1512
4502 4420  remCmdAgent.x 10716  0      3612   2624   88     72     6104
4503 4502  logger     2436   0      580    176    88     564    1512
4531 4499  logger     2436   0      680    176    88     564    1512
5039 2      flush-8:0  0      0      0      0      0      0      0

```

```

VSP-4850GTS#show khi performance pthread 1
Slot:1

```

```

-----
TID   PID   PName          CPU(%) 5MinAvg CPU(%) 5MinHiWater CPU(%(time stamp))
-----
1     1     init           0.0    0.0
2     2     kthreadd      0.0    0.0
3     3     ksoftirqd/0   0.0    0.0
4     4     events/0      0.0    0.0
5     5     khelper       0.0    0.0
8     8     async/mgr     0.0    0.0

```

73	73	sync_supers	0.0	0.0
75	75	bdi-default	0.0	0.0
77	77	kblockd/0	0.0	0.0
89	89	khubb	0.0	0.0
104	104	rpciod/0	0.0	0.0
128	128	kswapd0	0.0	0.0
180	180	aio/0	0.0	0.0
184	184	nfsiod	0.0	0.0
191	191	crypto/0	0.0	0.0
265	265	mtdblockd	0.0	0.0
426	426	udev	0.0	0.0
515	515	scsi_ah_0	0.0	0.0
521	521	usb-storage	0.0	0.0
1912	1912	portmap	0.0	0.0
1925	1925	rc	0.0	0.0
1936	1936	sshd	0.0	0.0
1941	1941	syslogd	0.0	0.0
1943	1943	klogd	0.0	0.0
1944	1944	S25vsp	0.0	0.0
4015	4015	rc.appfs.vsp4k	0.0	0.0
4266	4266	wdd	0.0	0.0
4306	4306	i2c_wq	0.0	0.0
4320	4320	sfp_q	0.0	0.0
4322	4322	psu_q	0.0	0.0
4342	4342	workqueue_0	0.0	0.0
4349	4349	workqueue_1	0.0	0.0
4387	4387	start	0.0	0.0
4420	4420	lifecycle	0.0	0.0
4421	4420	_Z15nd_ipc_disp	0.0	0.0
4422	4420	_Z18nd_ipc_send	0.0	0.0
4423	4420	_Z21nd_ipc_rece	0.0	0.0
4424	4420	_ZN10nd_tmr_grp	0.0	0.0
4426	4420	dpmXportRxMonit	0.0	0.0
4427	4420	dpmXportTxMonit	0.0	0.0
4428	4420	ltrBulkTimerThr	0.0	0.0
4429	4420	lc_wd_exception	0.0	0.0
4430	4420	lc_hwwd_feed	0.0	0.0
4431	4420	lc_swwd_feed	0.0	0.0
4432	4420	worker_thread	0.0	0.0
4433	4420	lc_master	0.0	0.0
4425	4425	logger	0.0	0.0
4434	4434	sockserv	0.0	0.0
4435	4435	oom95	0.0	0.0
4442	4435	_Z15nd_ipc_disp	0.0	0.0
4443	4435	_Z18nd_ipc_send	0.0	0.0
4444	4435	_Z21nd_ipc_rece	0.0	0.0
4445	4435	_ZN10nd_tmr_grp	0.0	0.0
4436	4436	logger	0.0	0.0
4437	4437	oom90	0.0	0.0
4446	4437	_Z15nd_ipc_disp	0.0	0.0
4447	4437	_Z18nd_ipc_send	0.0	0.0
4448	4437	_Z21nd_ipc_rece	0.0	0.0
4449	4437	_ZN10nd_tmr_grp	0.0	0.0
4438	4438	logger	0.0	0.0
4439	4439	logger	0.0	0.0
4440	4440	imgsync.x	0.0	0.0
4450	4440	_Z15nd_ipc_disp	0.0	0.0
4451	4440	_Z18nd_ipc_send	0.0	0.0
4452	4440	_Z21nd_ipc_rece	0.0	0.0
4453	4440	_ZN10nd_tmr_grp	0.0	0.0
4454	4440	dpmXportRxMonit	0.0	0.0
4455	4440	dpmXportTxMonit	0.0	0.0
4456	4440	ltrBulkTimerThr	0.1	0.0
4441	4441	logger	0.0	0.0
4486	4486	logServer	0.0	0.0

Key Health Indicators using ACLI

4520	4486	_Z15nd_ipc_disp	0.0	0.0	
4521	4486	_Z18nd_ipc_send	0.0	0.0	
4522	4486	_Z21nd_ipc_rece	0.0	0.0	
4523	4486	_ZN10nd_tmr_grp	0.0	0.0	
4487	4487	trcServer	0.0	0.0	
4504	4487	_Z15nd_ipc_disp	0.0	0.0	
4505	4487	_Z18nd_ipc_send	0.0	0.0	
4506	4487	_Z21nd_ipc_rece	0.0	0.0	
4507	4487	_ZN10nd_tmr_grp	0.0	0.0	
4488	4488	cbcp-main.x	0.0	0.0	
4532	4488	_Z15nd_ipc_disp	0.0	0.0	
4533	4488	_Z18nd_ipc_send	0.0	0.0	
4534	4488	_Z21nd_ipc_rece	0.0	0.0	
4535	4488	_ZN10nd_tmr_grp	0.0	0.0	
4536	4488	tUsrRoot	0.0	0.0	
4537	4488	tExcTask	1.2	1.1	1.1 (02/13/13 14:00:47)
4538	4488	tExcJobTask	0.0	0.0	
4539	4488	tNetTask	0.0	0.0	
4540	4488	traceOutput	0.0	0.0	
4541	4488	profile_cmd	0.0	0.0	
4564	4488	tRlogind	0.1	0.1	0.1 (02/13/13 14:00:47)
4565	4488	tRshd	0.0	0.0	
4566	4488	tFtpdTask	0.1	0.1	0.1 (02/13/13 14:00:47)
4567	4488	tFtpdTask	0.1	0.1	0.1 (02/13/13 14:00:47)
4568	4488	dpmXportRxMonit	0.0	0.0	
4569	4488	dpmXportTxMonit	0.0	0.0	
4570	4488	tndMiscServTask	0.0	0.0	
4571	4488	tLoggerTask	0.0	0.0	
4572	4488	tLicenseTask	0.0	0.0	
4573	4488	_ZN10CLimServer	0.1	0.0	0.1 (02/13/13 21:18:37)
4574	4488	tWdtTask	0.0	0.0	
4575	4488	BootpServer	0.0	0.0	
4576	4488	tSioMsgRx	0.0	0.0	
4655	4488	chEvmTask	0.0	0.0	
4656	4488	chFsmTask	0.0	0.0	
4657	4488	chServiceTask	0.0	0.0	
4659	4488	tSnmpTmr	0.0	0.0	
4660	4488	tSnmpd	0.0	0.0	
4670	4488	tTacacspTask	0.0	0.0	
4671	4488	tTacacsqTask	0.0	0.0	
4672	4488	tMainTask	2.7	2.4	3.3 (02/18/13 05:16:27)
4673	4488	rtMainTask	0.0	0.0	
4674	4488	tCppSend	0.0	0.0	
4675	4488	CppRxFrames_vsp	0.0	0.0	
4677	4488	cfmMain	0.3	0.2	0.2 (02/13/13 14:00:47)
4678	4488	cfmClock	0.1	0.0	0.1 (02/13/13 14:00:47)
4679	4488	tTalkClient	0.0	0.0	
4680	4488	tTrapd	0.0	0.0	
4682	4488	tTrapd	0.0	0.0	
4684	4488	tTdpTimer	0.0	0.0	
4685	4488	chHealthMonitor	0.1	0.0	
4686	4488	tSpfTimer	0.0	0.0	
4687	4488	tIsisTask	0.2	0.1	0.1 (02/13/13 14:00:47)
4689	4488	tWebSrv	0.0	0.0	
4690	4488	Http0	0.0	0.0	
4691	4488	Http1	0.0	0.0	
4692	4488	Http2	0.0	0.0	
4693	4488	Http3	0.0	0.0	
4694	4488	Http4	0.0	0.0	
4695	4488	Http5	0.0	0.0	
4696	4488	Http6	0.0	0.0	
4697	4488	Http7	0.0	0.0	
4698	4488	Http8	0.0	0.0	
4699	4488	Http9	0.0	0.0	
4700	4488	Http10	0.0	0.0	

4701	4488	Http11	0.0	0.0	
4702	4488	Http12	0.0	0.0	
4703	4488	Http13	0.0	0.0	
4704	4488	Http14	0.0	0.0	
4706	4488	Http16	0.0	0.0	
4707	4488	Http17	0.0	0.0	
4708	4488	Http18	0.0	0.0	
4709	4488	Http19	0.0	0.0	
4733	4488	_ZN10nd_tmr_grp	0.2	0.1	0.1 (02/13/13 14:01:07)
4743	4488	tRmonTimer	0.1	0.0	
4744	4488	tMsgCtlTimer	0.0	0.0	
5044	4488	tShell-cli	0.0	0.0	
4489	4489	logger	0.0	0.0	
4490	4490	rssServer	0.0	0.0	
4516	4490	_Z15nd_ipc_disp	0.0	0.0	
4517	4490	_Z18nd_ipc_send	0.0	0.0	
4518	4490	_Z21nd_ipc_rece	0.0	0.0	
4519	4490	_ZN10nd_tmr_grp	0.0	0.0	
4491	4491	dbgServer	0.0	0.0	
4508	4491	_Z15nd_ipc_disp	0.0	0.0	
4509	4491	_Z18nd_ipc_send	0.0	0.0	
4510	4491	_Z21nd_ipc_rece	0.0	0.0	
4511	4491	_ZN10nd_tmr_grp	0.0	0.0	
4492	4492	logger	0.0	0.0	
4493	4493	logger	0.0	0.0	
4494	4494	logger	0.0	0.0	
4495	4495	logger	0.0	0.0	
4496	4496	dbgShell	0.0	0.0	
4512	4496	_Z15nd_ipc_disp	0.0	0.0	
4513	4496	_Z18nd_ipc_send	0.0	0.0	
4514	4496	_Z21nd_ipc_rece	0.0	0.0	
4515	4496	_ZN10nd_tmr_grp	0.0	0.0	
4497	4497	coreManager.x	0.0	0.0	
4557	4497	_Z15nd_ipc_disp	0.0	0.0	
4558	4497	_Z18nd_ipc_send	0.0	0.0	
4559	4497	_Z21nd_ipc_rece	0.0	0.0	
4560	4497	_ZN10nd_tmr_grp	0.0	0.0	
4561	4497	dpmXportRxMonit	0.0	0.0	
4562	4497	dpmXportTxMonit	0.0	0.0	
4563	4497	ltrBulkTimerThr	0.0	0.0	
4498	4498	logger	0.0	0.0	
4499	4499	cbio-main.x	0.0	0.0	
4524	4499	_Z15nd_ipc_disp	0.0	0.0	
4525	4499	_Z18nd_ipc_send	0.0	0.0	
4526	4499	_Z21nd_ipc_rece	0.0	0.0	
4527	4499	_ZN10nd_tmr_grp	0.0	0.0	
4528	4499	tUsrRoot	0.0	0.0	
4529	4499	tExcTask	0.7	0.7	0.7 (02/13/13 14:00:47)
4530	4499	tty	0.0	0.0	
4661	4499	dpmXportRxMonit	0.0	0.0	
4662	4499	dpmXportTxMonit	0.0	0.0	
4663	4499	ltrBulkTimerThr	0.1	0.0	
4664	4499	profile_cmd	0.0	0.0	
4665	4499	tMainTask	0.4	0.3	0.3 (02/13/13 14:00:47)
4667	4499	bcmDPC	0.0	0.0	
4668	4499	_interrupt_thre	0.1	0.0	
4712	4499	bcmTX	0.0	0.0	
4713	4499	bcmXGS3AsyncTX	0.0	0.0	
4714	4499	bcmL2MOD.0	0.0	0.0	
4715	4499	bcmCNTR.0	3.5	3.6	3.6 (02/13/13 14:00:47)
4716	4499	bcmRX	0.2	0.1	0.1 (02/13/13 14:00:47)
4717	4499	tBCMTask	0.0	0.0	
4718	4499	bcmLINK.0	7.9	1.3	2.4 (02/13/13 21:18:17)
4722	4499	tRpdctimer	0.2	0.1	0.1 (02/13/13 14:00:47)
4723	4499	tUsrRoot	0.1	0.0	

Key Health Indicators using ACLI

```

4724 4499 tRspDebugPollTa 0.1 0.1 0.1(02/13/13 14:00:47)
4725 4499 tLcdIntrTask 0.0 0.0
4726 4499 tTimerTask 0.0 0.0
4727 4499 tPortEvt 0.0 0.0
4729 4499 tExcJobTask 0.0 0.0
4500 4500 logger 0.0 0.0
4501 4501 logger 0.0 0.0
4502 4502 remCmdAgent.x 0.0 0.0
4550 4502 _Z15nd_ipc_disp 0.0 0.0
4551 4502 _Z18nd_ipc_send 0.0 0.0
4552 4502 _Z21nd_ipc_rece 0.0 0.0
4553 4502 _ZN10nd_tmr_grp 0.0 0.0
4554 4502 dpmXportRxMonit 0.0 0.0
4555 4502 dpmXportTxMonit 0.0 0.0
4556 4502 ltrBulkTimerThr 0.0 0.0
4503 4503 logger 0.0 0.0
4531 4531 logger 0.0 0.0
5046 5046 flush-8:0 0.0 0.0

```

```

VSP-4850GTS#show khi performance slabinfo
Slot: 1

```

Name	Active	Num	Objsize	Objper	Pageper	Active	Num
Objs	slab	slab	Slabs	Slabs		Objs	Objs
cfq_queue	0	0	112	36	1	0	0
mqueue_inode_cache	8	8	480	8	1	1	1
jffs2_refblock	16	16	248	16	1	1	1
jffs2_i	23	23	344	23	2	1	1
nfs_direct_cache	0	0	72	56	1	0	0
nfs_read_data	38	38	416	19	2	2	2
nfs_inode_cache	0	0	552	14	2	0	0
fat_inode_cache	11	11	360	11	1	1	1
fat_cache	0	0	24	170	1	0	0
ext2_inode_cache	646	187	424	19	2	34	34
posix_timers_cache	0	0	104	39	1	0	0
rpc_inode_cache	19	19	416	19	2	1	1
UNIX	20	19	384	10	1	2	2
UDP-Lite	0	0	480	8	1	0	0
UDP	8	8	480	8	1	1	1
tw_sock_TCP	32	32	128	32	1	1	1
TCP	15	15	1056	15	4	1	1
eventpoll_pwq	102	102	40	102	1	1	1
sgpool-128	12	12	2560	12	8	1	1
sgpool-64	12	12	1280	12	4	1	1
sgpool-32	12	12	640	12	2	1	1
sgpool-16	156	156	320	12	1	13	13
scsi_data_buffer	170	170	24	170	1	1	1
blkdev_queue	39	39	1184	13	4	3	3
blkdev_requests	40	28	200	20	1	2	2
biovec-256	10	10	3072	10	8	1	1
biovec-128	0	0	1536	10	4	0	0
biovec-64	10	10	768	10	2	1	1
sock_inode_cache	187	185	352	11	1	17	17
skbuff_fclone_cache	11	11	352	11	1	1	1
skbuff_head_cache	300	300	160	25	1	12	12
file_lock_cache	39	39	104	39	1	1	1
shmem_inode_cache	860	848	400	10	1	86	86
proc_inode_cache	660	643	328	12	1	55	55
sigqueue	28	28	144	28	1	1	1
radix_tree_node	1144	657	296	13	1	88	88
bdev_cache	38	38	416	19	2	2	2
sysfs_dir_cache	5695	5694	48	85	1	67	67
inode_cache	4368	4270	304	13	1	336	336
dentry	6784	6151	128	32	1	212	212

buffer_head	16856	4733	72	56	1	301	301
vm_area_struct	2576	2516	88	46	1	56	56
mm_struct	90	86	448	9	1	10	10
signal_cache	72	70	480	8	1	9	9
sighand_cache	72	71	1312	12	4	6	6
task_struct	225	222	1072	15	4	15	15
anon_vma	1024	1024	16	256	1	4	4
idr_layer_cache	156	156	152	26	1	6	6
kmalloc-8192	4	4	8192	4	8	1	1
kmalloc-4096	88	83	4096	8	8	11	11
kmalloc-2048	40	33	2048	8	4	5	5
kmalloc-1024	120	113	1024	8	2	15	15
kmalloc-512	296	295	512	8	1	37	37
kmalloc-256	224	222	256	16	1	14	14
kmalloc-128	1536	1523	128	32	1	48	48
kmalloc-64	1664	1443	64	64	1	26	26
kmalloc-32	640	640	32	128	1	5	5
kmalloc-16	1024	1020	16	256	1	4	4
kmalloc-8	2048	2047	8	512	1	4	4
kmalloc-192	273	250	192	21	1	13	13
kmalloc-96	714	700	96	42	1	17	17

Variable definitions

Use the data in the following table to use the `show khi performance` command.

Table 1: Variable definitions

Variable	Value
{slot[-slot][,...]}	Specifies the slot number. Valid slot is 1.

Displaying KHI control processor information

About this task

Use the following commands to display key health information about the packets generated by interface modules, the type of packets and protocols received on a port.

Procedure

Display statistics for control packets that go to the control processor:

```
show khi cpp port-statistics [{slot/port[-slot/port][,...]}]
```

Example

```
VSP-4850GTS#show khi cpp port-statistics 1/1-1/6
```

```
=====
      KHI CPP Details - Port Statistics
=====
Ports   Packet Type                               Rx Packets  Tx Packets
-----
1/1     Ether2_EAP(140)                            0           2
```

1/1	LLC_BPDU (456)	9882	0
1/1	LLC_TDP (464)	0	2312
1/6	Ether2_IPv4_TTL_EXP (50)	13	0
1/6	Ether2_ARP_Other (129)	3	0
1/6	LLC_BPDU (456)	2312	0
1/6	LLC_TDP (464)	0	2314

Variable definitions

Use the data in the following table to use the `show khi cpp` command.

Table 2: Variable definitions

Variable	Value
slot/port[-slot/port][,...]	Identifies the slot and port in one of the following formats: a single slot and port (1/1).

Clearing KHI information

About this task

KHI information can be cleared for a specific slot or across the whole device. Use the command to clear the port statistics.

Procedure

Clear CPP statistics:

```
clear khi cpp <port-statistics>
```

Displaying KHI Fabric Extend ONA status

About this task

Use the following command to display the current status of the Fabric Extend ONA, which includes release information.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Display the ONA status:

```
show khi fe-ona status
```


Example

The following output displays the `show khi fe-ona status` when the ONA is operating normally.

```
Switch:1#show khi fe-ona status
```

```
=====
                        ONA STATUS
=====
ONA Device Status : UP
Running Release Name : v1.0.0.0int006-3-g9749735-dirty
Last Image Upgrade Status : UPGRADE_SUCCESS
Last Image File Used For Upgrde: gdb-secure_ona.tgz
=====
```

The following examples display the output when communication from the VSP 4000 to the ONA is disrupted. Note that the `ONA Down reason` lists the cause of the failure. The reason changes depending on the context of the failure.

The following output displays when the configuration push from VSP 4000 to the ONA fails:

```
Switch:1#show khi fe-ona status
```

```
=====
                        ONA STATUS
=====
ONA Device Status : DOWN
ONA DOWN reason : ONA_CONFIG_DOWNLOAD_FAILED
Running Release Name :
Image Upgrade Status : UNKNOWN
=====
```

The following output displays when the VSP 4000 port connecting to the ONA device port is DOWN:

```
Switch:1#show khi fe-ona status
```

```
=====
                        ONA STATUS
=====
ONA Device Status : DOWN
ONA DOWN reason : ONA_DEVICE_PORT_DOWN
Running Release Name :
Image Upgrade Status : UNKNOWN
Image File Is Being Used For Upgrade :
=====
```

The following output displays when the VSP 4000 is not receiving LLDP packets from the ONA:

```
Switch:1#show khi fe-ona status
```

```
=====
                        ONA STATUS
=====
ONA Device Status : DOWN
ONA DOWN reason : ONA_LLDP_TIMEOUT
Running Release Name :
Image Upgrade Status : UNKNOWN
=====
```

*** Note:**

On the VSP 4000 console, the following log message precedes all three of the above cases:

```
CP1 [03/22/71 09:30:15.336:UTC] 0x00378601 00000000 GlobalRouter ONA
WARNING ONA device status detected down
```

Displaying KHI Fabric Extend ONA global information

About this task

Use the following command to display Fabric Extend ONA global information such as port numbers, IP addresses, and MTU.

Procedure

1. Enter Privileged EXEC mode:
enable
2. Display the ONA global information:
show khi fe-ona detail

Example

```
Switch:1#show khi fe-ona detail
=====
                        ONA RUNTIME INFORMATION
=====
ONA Port Number : 1/15
ONA Management Address : 100.1.1.11
Tunnel Source IP Address : 11.11.12.11
ONA LLDP Port Status : Enabled
ONA Device Port Status : UP
ONA Device Status : UP
MTU : 1000
ONA Network Port Number : 1/35
ONA Mac(ARP) Address : 10:cd:ae:69:b6:50
ONA Source VlanId : 1050
ONA Source VlanIP : 10.0.70.1
ONA Gateway IP : 10.0.70.1
ONA Management IP Mask : 255.255.255.0
ONA Bootmode : 1
ONA Uptime : 0 day(s), 00:00:00
pbit-to-dscp-map p0=16 p1=20 p2=24 p3=30 p4=36 p5=40 p6=48 p7=46
=====
```

* Note:

In the above example, the VSP 4000 receives LLDP packets with the Management IP address of the ONA over the ONA Port (1/15). The VSP 4000 extracts the ONA Management IP from the LLDP packet and resolves the ARP of the ONA over the network port (1/35). After the VSP 4000 resolves the ARP of the ONA IP, the `show khi fe-ona detail` updates the following details:

- ONA Network Port Number
- ONA Mac(ARP) Address

- ONA Source VlanId

Note the following in regard to the `show khi fe-ona detail` output shown above:

- ONA Source VlanIP : 10.0.70.1—This is the IP address of the VSP 4000 VLAN that switches traffic to the ONA network port. In the above output, this is VLAN 1050.
- ONA Gateway IP : 10.0.70.1—This is the ONA gateway IP address that the VSP 4000 gets by querying the ONA. The ONA receives this gateway IP from the DHCP server.

 **Important:**

The ONA Source VlanIP, and ONA Gateway IP addresses must be the same for the tunnels to come up and the traffic to switch.

Chapter 5: Key Health Indicators using EDM

The Key Health Indicators (KHI) feature of Avaya Virtual Services Platform 4000 Series provides a subset of health information that allows for quick assessment of the overall operational state of the device.

 **Note:**

The KHI feature is not intended to provide a comprehensive debugging solution. Instead, KHI identifies key information that could lead Avaya support personnel towards discovery of a specific failure. After the technician assesses the KHI information, further debugging is required to determine the specific reason for the fault.

Avaya recommends that you capture KHI information during normal operations to provide a baseline for Avaya support personnel when detecting fault situations.

Clearing KHI statistics

About this task

Clear KHI statistics.

Procedure

1. In the Device Physical View tab, select the Device.
2. In the navigation tree, expand the following folders: **Configuration > Edit**.
3. Click **Chassis**.
4. Click the **CPP Stats Control** tab.
5. Select the statistics you want to clear.
6. Click **Apply**.

CPP Stats Control field descriptions

Use the data in the following table to use the **CPP Stats Control** tab.

Name	Description
PortStatsClear	Clears port statistics.

Displaying KHI port information

About this task

Use the following commands to display key health information about the types of control packets and protocols received on a port and sent to the control processor.

Procedure

1. In the Device Physical View, select a port.
2. In the navigation tree, expand the following folders: **Configuration > Graph**.
3. Click **Port**.
4. Click the **CPP Stats** tab.

CPP Stats field descriptions

Use the data in the following table to use the **CPP Stats** tab.

Name	Description
Port	Identifies the slot and port.
Packet	Shows the packet type.
PacketName	Shows the name of the packet.
RxPackets	Indicates the number of received packets on the port for the packet type.
TxPackets	Indicates the number of transmitted packets on the port for the packet type.

Chapter 6: Link state change control using ACLI

Detect and control link flapping to bring more stability to your network.

Controlling link state changes

About this task

Configure link flap detection to control state changes on a physical port.

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```
2. Configure the interval for link state changes:

```
link-flap-detect interval <2-600>
```
3. Configure the number of changes allowed during the interval:

```
link-flap-detect frequency <1-9999>
```
4. Enable automatic port disabling:

```
link-flap-detect auto-port-down
```
5. Enable sending a trap:

```
link-flap-detect send-trap
```

Example

1. Enable automatic disabling of the port:

```
VSP-4850GTS(config)# link-flap-detect auto-port-down
```
2. Configure the link-flap-detect interval:

```
VSP-4850GTS(config)# link-flap-detect interval 20
```
3. Enable sending traps:

```
VSP-4850GTS(config)# link-flap-detect send-trap
```

Variable definitions

Use the data in the following table to use the `link-flap-detect` command.

Table 3: Variable definitions

Variable	Value
<auto-port-down>	Automatically disables the port if state changes exceed the link-flap threshold. By default, auto-port-down is enabled. Use the no operator to remove this configuration. To set this option to the default value, use the default operator with the command.
frequency <1-9999>	Configures the number of changes that are permitted during the time specified by the interval command. The default is 20. To set this option to the default value, use the default operator with the command.
interval <2-600>	Configures the link-flap-detect interval in seconds. The default value is 60. To set this option to the default value, use the default operator with the command.
send-trap	Activates traps transmission. The default setting is activated. Use the no operator to remove this configuration. To set this option to the default value, use the default operator with the command.

Displaying link state changes

About this task

Displays link flap detection state changes on a physical port.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Display link state changes:

```
show link-flap-detect
```

Example

```
VSP-4850GTS>enable
VSP-4850GTS#show link-flap-detect

Auto Port Down : enable
Send Trap      : enable
Interval       : 60
Frequency      : 20
```


Chapter 7: Link state change control using EDM

Detect and control link flapping to bring more stability to your network.

Controlling link state changes

About this task

Configure link flap detection to control link state changes on a physical port.

Procedure

1. In the navigation tree, expand the following folders: **Configuration > Edit > Diagnostics**.
2. Click **General**.
3. Click the **Link Flap** tab.
4. Configure the parameters as required.
5. Click **Apply**.

Link Flap field descriptions

Use the data in the following table to use the **Link Flap** tab.

Name	Description
AutoPortDownEnable	Enables or disables Link Flap Detect. If you enable Link Flap Detect, the system monitors the number of times a port goes down during a designated interval. If the number of drops exceeds a specified limit, the system forces the port out-of-service.
SendTrap	Specifies that a trap is sent if the port is forced out-of-service.
Frequency	Specifies the number of times the port can go down. The default is 20.
Interval	Specifies the interval (in seconds) between port failures. The default is 60.

Chapter 8: Log and trap fundamentals

Use the information in this section to help you understand Simple Network Management Protocol (SNMP) traps and log files, available as part of Avaya Virtual Services Platform 4000 Series System Messaging Platform.

Overview of traps and logs

System log messaging

On a UNIX-based management platform, you can use system log (syslog) messaging to manage event messages. The switch syslog software communicates with a server software component named syslogd on the management workstation.

The UNIX daemon syslogd is a software component that receives and locally logs, displays, prints, and forwards messages that originate from sources internal and external to the workstation. For example, syslogd on a UNIX workstation concurrently handles messages received from applications that run on the workstation, as well as messages received from the switch that run in a network accessible to the workstation.

The remote UNIX management workstation performs the following actions:

- Receives system log messages from the switch .
- Examines the severity code in each message.
- Uses the severity code to determine appropriate system handling for each message.

Log consolidation

Virtual Services Platform generates a system log file and can forward that file to a syslog server for remote viewing, storage and analyzing.

The system log captures messages for the following components:

- Extensible Authentication Protocol (EAP)
- Remote Authentication Dial-in User Service (RADIUS)
- Remote Monitoring (RMON)
- Web
- hardware (HW)
- MultiLink Trunking (MLT)
- filter

- Quality of Service (QoS)
- Command line interface (CLI) log
- software (SW)
- Central Processing Unit (CPU)
- Internet Protocol (IP)
- Virtual Local Area Network (VLAN)
- policy
- Simple Network Management Protocol (SNMP) log

The switch can send information in the system log file, including ACLI command log and the SNMP operation log, to a syslog server.

View logs for CLILOG module to track all ACLI commands executed and for fault management purposes. The ACLI commands are logged to the system log file as CLILOG module.

View logs for SNMPLOG module to track SNMP logs. The SNMP operation log is logged to the system log file as SNMPLOG module.

The platform logs CLILOG and SNMPLOG as INFO. Normally, if you configure the logging level to WARNING, the system skips all INFO messages. However, if you enable CLILOG and SNMPLOG the system logs ACLI Log and SNMP Log information regardless of the logging level you set. This is not the case for other INFO messages.

System log client over IPv6 transport

You can log system log messages to external system log hosts with both IPv4 and IPv6 addresses with no difference in functionality or configuration except in the following case. When you configure the system log table in EDM, under the **System Log Table** tab, you must select either IPv4 or IPv6.

Log messages with enhanced secure mode

Enhanced secure mode allows the system to provide role-based access levels, stronger password requirements, and stronger rules on password length, password complexity, password change intervals, password reuse, and password maximum age use. If you enable enhanced secure mode, the system encrypts the entire log file.

With enhanced secure mode enabled, only individuals in the administrator or auditor role can view log files to analyze switch access and configuration activity. However, no access level role can modify the content of the log files, not even the administrator or the auditor access level roles. The administrator has access to the **remove** and **delete** commands.

If you enable enhanced secure mode, you cannot access the following commands for log files at any role-based access level:

- **more**
- **edit**
- **rename**
- **copy**

If someone attempts to access a log file with the preceding commands, an information and warning message displays on the screen.

The following table summarizes log file command access based on role-based access levels.

Table 4: Log commands accessible for various users

Access level role	Commands
Administrator	The remove and delete commands.
No user at any access level.	The following commands: <ul style="list-style-type: none"> • more • edit • rename • copy
Administrator	All configuration commands can only be accessed by the individual in the administrator role, other than the preceding commands.
Administrator and auditor	All show commands for log files.
All users (Administrator, auditor, security, privilege, operator.)	All show commands for log configurations.

With enhanced secure mode enabled, authorized users can use SFTP to transfer files to a remote server with the content encrypted.

SNMP traps

The SNMP trap is an industry-standard method used to manage events. You can set SNMP traps for specific types of log message (for example, warning or fatal), from specific applications, and send them to a trap server for further processing. For example, you can configure the switch to send SNMP traps to a server after a port is unplugged or if a power supply fails.

This document only describes SNMP commands related to traps. For more information about how to configure SNMP community strings and related topics, see *Configuring Security on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-601.

Secure syslog

Syslog is a standard used to send event log messages to devices within a network. The switch sends event messages to a logging server called syslog server. The syslog server stores the log messages and displays them for event reporting. Syslog messages are used for monitoring system activities and troubleshooting.

The secure syslog feature adds security and authenticated access to the plain text event log messages that are communicated between a remote syslog server and a syslog client. Secure syslog feature helps prevent unauthorized access to confidential data transmitted on an unsecured communication channel between a remote syslog server and client.

To implement the security, this feature employs port forwarding using the Secure Shell (SSH) cryptography protocol and Transport Layer Security (TLS) to provide the secure connection between syslog server and client.

After starting the syslog server, to ensure authentication, you must setup a remote port forwarding connection to connect the switch with the remote SSH client or the remote TLS server.

Secure syslog using SSH:

The syslog server is installed on a host that serves as SSH client. The SSH client requests a connection with the SSH server that resides on the switch. A remote port forwarding connection, called secure-forwarding, gets established between the syslog server and the switch. The syslog server now listens for the log messages on the port 601 at the end of the secure channel. The syslog server decrypts the received log messages and either stores or displays the messages.

Secure syslog using TLS:

The syslog server is installed on a host that serves as TLS server. The switch plays the role of a TLS client. A TLS handshake is initiated between the syslog server and the switch. The syslog server transmits a certificate which has subject common name and optional subject alternative name (SAN). Subject common name is always present in the certificate but SAN is optional. The server-cert-name must match with SAN name if present in the certificate else if SAN name is not present, it must match with the Subject Common Name else TLS negotiation fails and the connection to the server is closed. If the server-cert-name part is not configured, then the check is not done.

Once the TLS handshake is successful, the log messages sent from the switch to the syslog server are encrypted. The syslog server decrypts these messages using a private key. The server then stores the messages or forwards them to other servers.

Supported syslog servers:

This feature supports the following syslog servers:

- For SSH tunneling — WinSyslog, which is the Windows OS based syslog server.
- For TLS tunneling — Rsyslog, which is a Linux based open source syslog server.

Simple Network Management Protocol

The Simple Network Management Protocol (SNMP) provides facilities to manage and monitor network resources. SNMP consists of:

- Agents—An agent is software that runs on a device that maintains information about device configuration and current state in a database.
- Managers—An SNMP manager is an application that contacts an SNMP agent to query or modify the agent database.
- The SNMP protocol—SNMP is the application-layer protocol SNMP agents and managers use to send and receive data.
- Management Information Bases (MIB)—The MIB is a text file that specifies the managed objects by an object identifier (OID).

! Important:

The switch does not reply to SNMP requests sent to the Virtual Router Redundancy Protocol (VRRP) virtual interface address; it does, however, reply to SNMP requests sent to the physical IP address.

An SNMP manager and agent communicate through the SNMP protocol. A manager sends queries and an agent responds; however, an agent initiates traps. Several types of packets transmit between SNMP managers and agents:

- Get request—This message requests the values of one or more objects.
- Get next request—This message requests the value of the next object.
- Set request—This message requests to modify the value of one or more objects.
- Get response—An SNMP agent sends this message in response to a get request, get next request, or set request message.
- Trap—SNMP trap is a notification triggered by events at the agent.

Log message format

The log messages for the switch have a standardized format. All system messages are tagged with the following information, except that alarm type and alarm status apply to alarm messages only:

- Avaya proprietary (AP) format—Provides encrypted information for debugging purposes
- CPU slot number—Indicates the CP slot where the command is logged.
- timestamp—Records the date and time at which the event occurred. The format is MM/DD/YY hh:mm:ss.uuu, where uuu is milliseconds. Example: [11/01/10 11:41:21.376].
- event code—Precisely identifies the event reported.
- alarm code—Specifies the alarm code.
- alarm type—identifies the alarm type (Dynamic or Persistent) for alarm messages
- alarm status—identifies the alarm status (set or clear) for alarm messages
- VRF name—Identifies the Virtual Routing and Forwarding (VRF) instance, if applicable.
- module name—Identifies the software module or hardware from which the log is generated.
- severity level—Identifies the severity of the message.
- sequence number—Identifies a specific CLI command.
- context—Specifies the type of the session used to connect to the switch. If the session is a remote session, the remote IP address is identified.
- user name—Specifies the user name used to login to the switch.
- ACLI command—Specifies the commands typed during the ACLI session. The system logs anything type during the ACLI session as soon as the user enters the Enter key.

The following messages are examples of an informational message for CLILOG:

```

CP1 [07/18/14 13:23:11.253] 0x002c0600 00000000 GlobalRouter CLILOG INFO 13 TELNET:
135.55.40.200 rwa show log file name-of-file log.40300001.1806

CP1 [07/18/14 13:24:19.739] 0x002c0600 00000000 GlobalRouter CLILOG INFO 15 TELNET:
135.55.40.200 rwa term more en

CP1 [07/18/14 13:24:22.577] 0x002c0600 00000000 GlobalRouter CLILOG INFO 16 TELNET:
135.55.40.200 rwa show log

CP1 [01/12/70 15:13:59.056] 0x002c0600 00000000 GlobalRouter CLILOG INFO 5 TELNET:
47.17.170.108 rwa syslog host 4

CP1 [01/12/70 15:13:35.520] 0x002c0600 00000000 GlobalRouter CLILOG INFO 4 TELNET:
47.17.170.108 rwa syslog host enable

CP1 [01/12/70 15:13:14.576] 0x002c0600 00000000 GlobalRouter CLILOG INFO 3 TELNET:
47.17.170.108 rwa show syslog

CP1 [01/12/70 15:12:44.640] 0x002c0600 00000000 GlobalRouter CLILOG INFO 2 TELNET:
47.17.170.108 rwa show logging file tail
    
```

The following messages are examples of an informational message for SNMPLOG:

```

CP1 [05/07/14 10:24:05.468] 0x002c4600 00000000 GlobalRouter SNMPLOG INFO 1
ver=v2c public rcVlanPortMembers.2 =

CP1 [05/07/14 10:29:58.133] 0x002c4600 00000000 GlobalRouter SNMPLOG INFO 2
ver=v2c public rcVlanPortMembers.2 =

CP1 [05/07/14 10:30:20.466] 0x002c4600 00000000 GlobalRouter SNMPLOG INFO 3 ver=v2c
public rcVlanPortMembers.1 =
    
```

The following messages are examples of an informational message for system logs:

```

CP1 [07/24/14 18:04:08.304] 0x00000670 00000000 GlobalRouter SW INFO Basic license
supports all features on this device
CP1 [07/24/14 18:04:10.651] 0x00034594 00000000 GlobalRouter SW INFO System boot
CP1 [07/24/14 18:04:10.651] 0x00034595 00000000 GlobalRouter SW INFO VSP-8200 System
Software Release 0.0.0.0 B553
CP1 [07/24/14 18:04:10.779] 0x00010774 00000000 GlobalRouter HW INFO Detected 8 284XSQ
chassis
CP1 [07/24/14 18:04:10.779] 0x0001081c 00400010.2 DYNAMIC SET GlobalRouter HW INFO Slot
2 is initializing.
CP1 [07/24/14 18:04:10.780] 0x0001081c 00400010.1 DYNAMIC SET GlobalRouter HW INFO Slot
1 is initializing.
CP1 [07/24/14 18:04:10.810] 0x00010729 00000000 GlobalRouter HW INFO Detected 8284XSQ
Power Supply in slot PS 1. Adding 800 watts to available power
CP1 [07/24/14 18:04:10.811] 0x00010830 00000000 GlobalRouter HW INFO Detected 8242XSQ
module (Serial#: SDNIV84Q2013) in slot 2
    
```

The system encrypts AP information before writing it to the log file. The encrypted information is for debugging purposes. Only an Avaya Customer Service engineer can decrypt the information. ACLI commands display the logs without the encrypted information. Avaya recommends that you do not edit the log file.

The following table describes the system message severity levels.

Table 5: Severity levels

Severity level	Definition
EMERGENCY	A panic condition that occurs when the system becomes unusable. Usually a severity level of emergency is usually a condition where multiple applications or server are affected. You must correct a severity level of alert immediately.
ALERT	Any condition requiring immediate attention and correction. You must correct a severity level of alert immediately, but usually indicates failure of a secondary system, such as an Internet Service Provider connection.
CRITICAL	Any critical conditions, such as a hard drive error.
ERROR	A nonfatal condition occurred. You can be required to take appropriate action. For example, the system generates an error message if it is unable to lock onto the semaphore required to initialize the IP addresses used to transfer the log file to a remote host.
WARNING	A nonfatal condition occurred. No immediate action is needed. An indication that an error can occur if action is not taken within a given amount of time.
NOTIFICATION	Significant event of a normal and normal nature. An indication that unusual, but not error, conditions have occurred. No immediate action is required.
INFO	Information only. No action is required.
DEBUG	Message containing information useful for debugging.
FATAL	A fatal condition occurred. The system cannot recover without restarting. For example, a fatal message is generated after the configuration database is corrupted.

Based on the severity code in each message, the platform dispatches each message to one or more of the following destinations:

- workstation display
- local log file
- one or more remote hosts

You can log system log messages to external system log hosts with both IPv4 and IPv6 addresses with no difference in functionality or configuration except in the following case. When you configure the system log table in EDM, under the **System Log Table** tab, you must select either IPv4 or IPv6.

Internally, the switch has four severity levels for log messages: INFO, WARNING, ERROR, and FATAL. The system log supports eight different severity levels:

- Debug
- Info
- Notice
- Warning
- Critical
- Error

- Alert
- Emergency

The following table shows the default mapping of internal severity levels to syslog severity levels.

Table 6: Default and system log severity level mapping

UNIX system error codes	System log severity level	Internal severity level
0	Emergency	Fatal
1	Alert	—
2	Critical	—
3	Error	Error
4	Warning	Warning
5	Notice	—
6	Info	Info
7	Debug	—

Log files

The log file captures hardware and software log messages, and alarm messages. Virtual Services Platform 4000 logs to internal flash.

The system saves internal log messages in a circular list in memory, which overwrite older log messages as the log fills. Unlike the log messages in a log file, the internal log messages in memory do not contain encrypted information, which can limit the information available during troubleshooting. Free up the disk space on the flash if the system generates the disk space 75% full alarm. After the disk space utilization returns below 75%, the system clears the alarm, and then starts logging to a file again.

Log file naming conventions

The following list provides the naming conventions for the log file:

- The log file is named as log.xxxxxxxx.sss format. The prefix of the log file name is log. The six characters after the log file prefix contain the last three bytes of the chassis base MAC address. The next two characters are 01. The last three characters (sss) denote the sequence number of the log file.
- The sequence number of the log file is incremented for each new log file created after the existing log file reaches the maximum configured size.
- At initial system start up when no log file exists, a new log file with the sequence number 000 is created. After a restart, the system finds the newest log file from internal flash based on file timestamps. If the newest log file is on the flash that is used for logging, the system continues to use the newest log file. And once the maximum configured size is reached, system continues to create a new log file with incremental sequence number on the internal flash for logging.

Log file transfer

The system logs contain important information for debugging and maintaining the switch. After the current log file reaches the configured maximum size, the system creates a new log file for logging. The system transfers old log files to a remote host. You can configure up to 10 remote hosts, which creates long-term backup storage of your system log files.

Of the 10 configured remote hosts, 1 is the primary host and the other 9 are redundant. Upon initiating a transfer, system messaging attempts to use host 1 first. If host 1 is not reachable, system messaging tries hosts 2 to 10.

If log file transfer is unsuccessful, the system keeps the old log files on internal flash. The system attempts to transfer old log files after the new log file reaches the configured maximum size. The system also attempts to transfer old log files periodically (once in one hundred log writes) if the disk space on the flash is more than 75% full.

You can log system log messages to external system log hosts with both IPv4 and IPv6 addresses with no difference in functionality or configuration.

With enhanced secure mode enabled, authorized users can use SFTP to transfer files to a remote server with the content encrypted.

You can specify the following information to configure the transfer criteria:

- The maximum size of the log file.
- The IP address of the remote host.
- The name prefix of the log file to store on the remote host.

The system appends a suffix of .xxxxxxx.sss to the file name. The first six characters of the suffix contain the last three bytes of the chassis base MAC address. The next two characters are 01. The last three characters (sss) denote the sequence number of the log file. For example, if you configure the name prefix as mylog, a possible file name is mylog.90000001.001.

- The user name and password, if using File Transfer Protocol (FTP) for file transfer. Use the following commands to configure the user name and password:

```
boot config host user WORD<0-16>
```

```
boot config host password WORD<0-16>
```

Be aware of the following restrictions to transfer log files to a remote host:

- The remote host IP address must be reachable.
- If you transfer a log file from a host to the system, (for example, to display it with a show command), rename the log file. Failure to rename the log file can cause the system to use the recently transferred file as the current log, if the sequence number in the extension is higher than the current log file. For example, if bf860005.002 is the current log file and you transfer bf860005.007 to the system, the system logs future messages to the bf860005.007 file. You can avoid this if you rename the log file to something other than the format used by system messaging.
- If your TFTP server is a UNIX-based machine, files written to the server must already exist. For example, you must create dummy files with the same names as your system logs. This action is commonly performed by using the touch command (for example, `touch bf860005.001`).

Three parameters exist to configure the log file:

- the minimum acceptable free space available for logging
- the maximum size of the log file
- the percentage of free disk space the system can use for logging

Although these three parameters exist, you can only configure the maximum size of the log file. The switch does not support the minimum size and percentage of free disk space parameters. The internal flash must be less than 75% full for the system to log a file. If the internal flash is more than 75% full, logging to a file stops to prevent exhausting disk space.

Log file transfer using a wildcard filename

Log files from VOSS Release 4.1 and earlier were created without access permissions. However, file transfers using SFTP require file permissions.

The command `attribute WORD<1-99> [+/-] R` allows you to change the permissions of a file. To change permissions for log files created in VOSS 4.1 and earlier, use the `attribute` command with the wildcard filename `log.*`. Using the command in the form `attribute log.* [+/-]R` changes permissions for log files with names that begin with the characters “log.”.

Important:

You cannot use a wildcard pattern other than `log.*` for this command.

Chapter 9: Log configuration using ACLI

Use log files and messages to perform diagnostic and fault management functions.

Related links

[Configuring a UNIX system log and syslog host](#) on page 41

[Configuring secure forwarding](#) on page 45

[Installing root certificate for syslog client](#) on page 47

[Configuring logging](#) on page 48

[Configuring the remote host address for log transfer](#) on page 50

[Configuring system logging](#) on page 51

[Configuring system message control](#) on page 52

[Extending system message control](#) on page 53

Configuring a UNIX system log and syslog host

About this task

Configure the syslog to control a facility in UNIX machines that logs SNMP messages and assigns each message a severity level based on importance.

You can log system log messages to external system log hosts with both IPv4 and IPv6 addresses with no difference in functionality or configuration using ACLI.

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. Enable the system log:

```
syslog enable
```

3. Specify the IP header in syslog packets:

```
syslog ip-header-type <circuitless-ip|default>
```

4. Configure the maximum number of syslog hosts:

```
syslog max-hosts <1-10>
```

5. Create the syslog host:

```
syslog host <1-10>
```

6. Configure the IP address for the syslog host:

```
syslog host <1-10> address WORD <0-46>
```

7. Enable the syslog host:

```
syslog host <1-10> enable
```

Configure optional syslog host parameters by using the variables in the following variable definition tables.

8. View the configuration to ensure it is correct:

```
show syslog [host <1-10>]
```

Example

```
VSP-4850GTS(config)#syslog enable
```

```
VSP-4850GTS(config)#syslog host 7 address 1.1.1.1
```

```
VSP-4850GTS(config)#syslog host 7 enable
```

```
VSP-4850GTS(config)#show syslog host 7
```

```
      Id : 7
      IpAddr : 1.1.1.1
      UdpPort : 514
      Facility : local7
      Severity : info|warning|error|fatal
      MapInfoSeverity : info
      MapWarningSeverity : warning
      MapErrorSeverity : error
      MapMfgSeverity : notice
      MapFatalSeverity : emergency
      Enable : true
      SecureForwardingMode: none
      Tcp Port : 1025
```

```
VSP-4850GTS(config)#show syslog
```

```
Enable      : true
Max Hosts   : 5
OperState   : active
header      : default
Total number of configured hosts : 3
Total number of enabled hosts : 1
Configured host : 7 8 9
Enabled host : 7
```

```
VSP-4850GTS(config)# syslog host 2 address fe80:0:0:0:22b:4eee:fe5e:73fd
udp-port 515
```

```
VSP-4850GTS(config)# syslog host 2 udp-port 515
```

```
VSP-4850GTS(config)# syslog host 2 enable
```

```
VSP-4850GTS (config) #
```

```
VSP-4850GTS (config) #show syslog host 2
```

```

    Id : 2
    IpAddr : fe80:0:0:0:22b:4eee:fe5e:73fd
    UdpPort : 515
    Facility : local7
    Severity : info|warning|error|fatal
    MapInfoSeverity : info
    MapWarningSeverity : warning
    MapErrorSeverity : error
    MapMfgSeverity : notice
    MapFatalSeverity : emergency
    Enable : true

```

Variable definitions

Use the data in the following table to use the `syslog` command.

Table 7: Variable definitions

Variable	Value
enable	Enables the sending of syslog messages on the device. The default is disabled. Use the no operator before this parameter, no syslog enable to disable the sending of syslog messages on the device. The default is enabled.
ip-header-type <circuitless-ip default>	<p>Specifies the IP header in syslog packets to circuitless-ip or default.</p> <ul style="list-style-type: none"> If the value is default, the IP address of the VLAN is used for syslog packets that are transmitted in-band using input/output (I/O) ports. If the value is circuitless-ip, then for all syslog messages (in-band or out-of-band), the circuitless IP address is used in the IP header. If you configure multiple circuitless IPs, the first circuitless IP configured is used.
max-hosts <1-10>	Specifies the maximum number of syslog hosts supported, from 1–10. The default is 5.

Use the data in the following table to use the `syslog host` command.

Table 8: Variable definitions

Variable	Value
1–10	Creates and configures a host instance. Use the no operator before this parameter, no syslog host to delete a host instance.

Table continues...

Variable	Value
address WORD <0–46>	Configures a host location for the syslog host. WORD <0–46> is the IPv4 or IPv6 address of the UNIX system syslog host in the format A.B.C.D or x:x:x:x:x:x. You can log system log messages to external system log hosts with both IPv4 and IPv6 addresses with no difference in functionality or configuration using ACLI.
enable	Enables the syslog host. Use the no operator before this parameter, no syslog host enable to disable syslog host. The default is disabled.
facility {local0 local1 local2 local3 local4 local5 local6 local7}	Specifies the UNIX facility in messages to the syslog host. {local0 local1 local2 local3 local4 local5 local6 local7} is the UNIX system syslog host facility. The default is local7.
maperror {emergency alert critical error warning notice info debug}	Specifies the syslog severity to use for error messages. The default is error.
mapfatal {emergency alert critical error warning notice info debug}	Specifies the syslog severity to use for fatal messages. The default is emergency.
mapinfo {emergency alert critical error warning notice info debug}	Specifies the syslog severity level to use for information messages. The default is info.
mapwarning {emergency alert critical error warning notice info debug}	Specifies the syslog severity to use for warning messages. The default is warning.
secure-forwarding mode [none] [ssh] [tls server-cert-name WORD<1-64>]	Specifies the mode of secure forwarding of syslog on the host. The default mode is none, that is, both ssh and tls modes are disabled by default.
secure-forwarding tcp-port <1025–49151>	Set tcp-port for secure forwarding of syslog for host. The default tcp-port is 1025. ! Important: The tcp-port 6000 cannot be used, as it is used as an internal port for Internal Spanning Tree (IST).
severity <info warning error fatal> [<info warning error fatal>] [<info warning error fatal>] [<info warning error fatal>]	Specifies the severity levels for which to send syslog messages for the specified modules. The default is info.
udp-port <514-530>	Specifies the User Datagram Protocol port number on which to send syslog messages to the syslog host. This value is the UNIX system syslog host port number from 514–530. The default is 514.

Job aid

The following table describes the fields in the output for the `show syslog host` command.

Parameter	Description
Id	Specifies the ID for the syslog host. The range is 1–10.
IpAddr	Specifies the IP address of the syslog host. You can log system log messages to external system log hosts with both IPv4 and IPv6 addresses.
UdpPort	Specifies the UDP port to use to send messages to the syslog host (514–530). The default is 514.
Facility	Specifies the syslog host facility used to identify messages (local0 to local7). The default is local7.
Severity	Specifies the message severity for which syslog messages are sent. The default is info warning error fatal.
MapInfoSeverity	Specifies the syslog severity to use for INFO messages. The default is info.
MapWarningSeverity	Specifies the syslog severity to use for WARNING messages. The default is warning.
MapErrorSeverity	Specifies the syslog severity to use for ERROR messages. The default is error.
MapMfgSeverity	Specifies the syslog severity to use for Accelar manufacturing messages. The default is notice.
MapFatalSeverity	Specifies the syslog severity to use for FATAL messages. The default is emergency.
Enable	Enables or disables the sending of messages to the syslog host. The default is disabled.
SecureForwardingMode	Specifies the mode in which the syslog messages are securely forwarded. The supported values are ssh, tls, and none. The default is none, which means that secure forwarding is disabled.
TcpPort	Specifies the TCP port to use for secure forwarding for a particular host. The default is 1024.

Configuring secure forwarding

Configuring secure forwarding includes setting the mode for the particular syslog host and setting the TCP port through which the logs are sent to the syslog server.

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. Create the syslog host:

```
syslog host <1-10>
```

Use the `no` operator before this parameter, that is, `no syslog host` to delete a host instance.

3. Configure an IP address for the syslog host:

```
syslog host <1-10> address WORD<0-46>
```

4. Enable the syslog host:

```
syslog host <1-10> enable
```

5. Enable syslog globally:

```
syslog enable
```

6. Set the mode for secure forwarding on the host:

```
syslog host <1-10> secure-forwarding mode [none] | [ssh] | [tls  
server-cert-name WORD<1-64>]
```

7. Set the TCP port:

```
syslog host <1-10> secure-forwarding tcp-port <1025-49151>
```

8. Display the secure forwarding configured values:

```
show syslog host <1-10>
```

9. **(Optional)** Remove the server certificate name:

```
no syslog host <1-10> secure-forwarding mode tls server-cert-name
```

10. **(Optional)** Set secure-forwarding mode to none for a particular host:

```
default syslog host <1-10> secure-forwarding mode
```

Next steps

After configuring secure forwarding on the switch, set the syslog server to be able to see the log messages on the interactive syslog viewer.

- For SSH secure syslog, on the winsyslog server, enter the host IP or the IP of the PC and set the port to 601 which is a default port for TCP and set the protocol type to RFC3195.
- For TLS secure syslog, on the rsyslog server, configure the server to use TLS method and install the root certificate on the server in the switch.

Related links

[Log configuration using ACLI](#) on page 41



[Variable definitions](#) on page 46

Variable definitions

Use the data in the following table to use the `syslog host` command.

Variable	Value
host <1–10>	Specifies the ID for the syslog host. The range is 1–10.
address WORD<0–46>	Configures a host location for the syslog host. WORD <0–46> is the IPv4 or IPv6 address of the UNIX system syslog host in the format A.B.C.D or x:x:x:x:x:x. You can log system log messages to external system log hosts with both IPv4 and IPv6 addresses with no difference in functionality or configuration using ACLI.
enable	Enables the syslog host. Use the no operator before this parameter, no syslog host enable to disable syslog host. The default is disabled.
secure-forwarding	Adds protected syslog using SSH remote port forwarding for host.

Use the data in the following table to use the `syslog host secure-forwarding` command.

Variable	Value
host <1–10>	Creates and configures a host instance. Use the no operator before this parameter, no syslog host to delete a host instance.
mode [none ssh tls server-cert-name WORD<1-64>]	Specifies the mode of secure forwarding of syslog on the host. The default mode is none, that is, both ssh and tls modes are disabled by default.  Note: Certificate validation is done only if the server-cert-name is configured.
tcp-port <1025–49151>	Set tcp-port for secure forwarding of syslog for host. The default tcp-port is 1025. To set the TCP port to default value, use command <code>default syslog host <1–10> secure-forwarding tcp-port</code> .  Important: The tcp-port 6000 cannot be used, as it is used as an internal port for Internal Spanning Tree (IST).

Related links

[Configuring secure forwarding](#) on page 45

Installing root certificate for syslog client

Use the following procedure to install a root certificate for a syslog client.

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. Install a root certificate on the store:

```
syslog root-cert install-filename <file-name>
```

The certificate is installed in folder: /intflash/.cert/.syslogrootinstalledcert/.

*** Note:**

The offline root certificate for TLS syslog must be kept in folder: /intflash/.cert/..syslogofflinerootcert/.

3. Uninstall a root certificate from the store:

```
no syslog root-cert install-filename <file-name>
```

4. To display the installed syslog server root certificate file:

```
show syslog root-cert-file
```

Related links

[Log configuration using ACLI](#) on page 41

[Variable definition](#) on page 48

Variable definition

Use the data in the following table to use the `syslog root-cert` command.

Variable	Value
install-filename <i>WORD</i> <1–128>	Specifies the name of the root certificate to be installed on the store.

Related links

[Installing root certificate for syslog client](#) on page 47

Configuring logging

About this task

Configure logging to determine the types of messages to log and where to store the messages.

*** Note:**

The platform logs CLILOG and SNMPLOG as INFO. Normally, if you configure the logging level to WARNING, the system skips all INFO messages. However, if you enable CLILOG and SNMPLOG the system logs ACLI Log and SNMP Log information regardless of the logging level you set. This is not the case for other INFO messages.

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```
2. Define which messages to log:

```
logging level <0-4>
```
3. Write the log file from memory to a file:

```
logging write WORD<1-1536>
```
4. Show logging on the screen:

```
logging screen
```

Example

```
VSP-4850GTS>enable
VSP-4850GTS#configure terminal
VSP-4850GTS(config)#logging level 0
VSP-4850GTS(config)#logging write log2
VSP-4850GTS(config)#logging screen
```

Variable definitions

Use the data in the following table to use the **logging** command.

Table 9: Variable definitions

Variable	Value
level <0-4>	Shows and configures the logging level. The level is one of the following values: <ul style="list-style-type: none"> • 0: Information — all messages are recorded • 1: Warning — only warning and more serious messages are recorded • 2: Error — only error and more serious messages are recorded • 3: Manufacturing — this parameter is not available for customer use • 4: Fatal — only fatal messages are recorded

Table continues...

Variable	Value
screen	Configures the log display on the screen to on. Use the no form of the command to stop the log display on the screen: <code>no logging screen</code>
transferFile <1-10> address {A.B.C.D} filename-prefix WORD<0-200	Transfers the syslog file to a remote FTP/TFTP server. <1-10> specifies the file ID. The address {A.B.C.D} option specifies the IP address. The filename-prefix WORD<0-200> option sets the filename prefix for the log file at the remote host.
write WORD<1-1536>	Writes the log file with the designated string. WORD<1-1536> is the string or command that you append to the log file. If the string contains spaces, you must enclose the string in quotation marks (").

Configuring the remote host address for log transfer

Before you begin

The IP address you configure for the remote host must be reachable at the time of configuration.

About this task

Configure the remote host address for log transfer. The system transfers the current log file to a remote host after the log file size reaches the maximum size.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Configure the remote host address for log transfer:

```
logging transferFile {1-10} address {A.B.C.D} [filename WORD<0-255>]
```

Example

```
VSP-4850GTS>enable
VSP-4850GTS#configure terminal
VSP-4850GTS(config)#logging transferFile 1 address 172.16.120.10
```

Variable definitions

Use the data in the following table to use the `logging transferFile` command.

Table 10: Variable definitions

Variable	Value
1-10	Specifies the file ID to transfer.
address {A.B.C.D}	Specifies the IP address of the host to which to transfer the log file. The remote host must be reachable or the configuration fails.
filename WORD<0-255>	Specifies the name of the file on the remote host. If you do not configure a name, the current log file name is the default.

Configuring system logging

About this task

System logs are a valuable diagnostic tool. You can send log messages to flash files for later retrieval.

You can change log file parameters at anytime without restarting the system. Changes made to these parameters take effect immediately.

Avaya recommends that you configure logging to a flash file at all times.

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. Enable system logging to a PC card file:

```
boot config flags logging
```

3. Configure the logfile parameters:

```
boot config logfile <64-500> <500-16384> <10-90>
```

Example

```
VSP-4850GTS>enable
```

```
VSP-4850GTS#configure terminal
```

```
VSP-4850GTS(config)#boot config logfile 64 600 10
```

Variable definitions

Use the data in the following table to use the `boot config` command.

Table 11: Variable definitions

Variable	Value
flags logging	Enables or disables logging to a file a flash file. The log file is named using the format log.xxxxxxx.sss. The first six characters after the prefix of the file name log contain the last three bytes of the chassis base MAC address. The next two characters specify the slot number. The last three characters denote the sequence number of the log file.
logfile <64-500> <500-16384> <10-90>	Configures the logfile parameters <ul style="list-style-type: none"> • <64-500> specifies the minimum free memory space on the external storage device from 64–500 KB. Virtual Services Platform 4000 does not support this parameter. • <500-16384> specifies the maximum size of the log file from 500–16384 KB. • <10-90> specifies the maximum percentage, from 10–90%, of space on the external storage device the logfile can use. Virtual Services Platform 4000 does not support this parameter.

Configuring system message control

About this task

Configure system message control to suppress duplicate error messages on the console, and to determine the action to take if they occur.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```
2. Configure system message control action:

```
sys msg-control action <both|send-trap|suppress-msg>
```
3. Configure the maximum number of messages:

```
sys msg-control max-msg-num <2-500>
```
4. Configure the interval:

```
sys msg-control control-interval <1-30>
```
5. Enable message control:

```
sys msg-control
```


Example

```
VSP-4850GTS>enable
VSP-4850GTS#configure terminal
VSP-4850GTS(config)#sys msg-control action suppress-msg
VSP-4850GTS(config)#sys msg-control max-msg-num 10
VSP-4850GTS(config)#sys msg-control control-interval 15
VSP-4850GTS(config)#sys msg-control
```

Variable definitions

Use the data in the following table to use the `sys msg-control` command.

Table 12: Variable definitions

Variable	Value
action <both send-trap suppress-msg>	Configures the message control action. You can either suppress the message or send a trap notification, or both. The default is suppress.
control-interval <1-30>	Configures the message control interval in minutes. The valid options are 1–30. The default is 5.
max-msg-num <2-500>	Configures the number of occurrences of a message after which the control action occurs. To configure the maximum number of occurrences, enter a value from 2–500. The default is 5.

Extending system message control**About this task**

Use the force message control option to extend the message control feature functionality to the software and hardware log messages.

To enable the message control feature, you must specify an action, control interval, and maximum message number. After you enable the feature, the log messages, which get repeated and cross the maximum message number in the control interval, trigger the force message feature. You can either suppress the message or send a trap notification, or both.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Configure the force message control option:

```
sys force-msg WORD<4-4>
```

Example

```
VSP-4850GTS> enable
```

```
VSP-4850GTS# configure terminal
```

Add a force message control pattern. If you use a wildcard pattern (****), all messages undergo message control.

```
VSP-4850GTS(config)# sys force-msg ****
```

Variable definitions

Use the data in the following table to use the `sys force-msg` command.

Table 13: Variable definitions

Variable	Value
<i>WORD<4-4></i>	Adds a forced message control pattern, where <i>WORD<4-4></i> is a string of 4 characters. You can add a four-byte pattern into the force-msg table. The software and the hardware log messages that use the first four bytes that match one of the patterns in the force-msg table undergo the configured message control action. You can specify up to 32 different patterns in the force-msg table, including a wildcard pattern (****) as well. If you specify the wildcard pattern, all messages undergo message control.

Viewing logs

View log files by file name, category, or severity to identify possible problems.

About this task

View ACLI command and SNMP trap logs, which are logged as normal log messages and logged to the system log file.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Show log information:

```
show logging file [alarm] [event-code WORD<0-10>] [module WORD<0-100>] [name-of-file WORD<1-99>] [save-to-file WORD<1-99>] [severity WORD<0-25>] [tail] [vrf WORD<0-32>]
```

Example

Display log file information:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#show logging file
CP1 [02/06/15 22:38:20.678:UTC] 0x00270428 00000000 GlobalRouter SW INFO Lifecy
cle: Start
CP1 [02/06/15 22:38:21.770:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s sockserv started, pid:4794
CP1 [02/06/15 22:38:21.771:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s oom95 started, pid:4795
CP1 [02/06/15 22:38:21.771:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s oom90 started, pid:4796
CP1 [02/06/15 22:38:21.772:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s imgsync.x started, pid:4797
CP1 [02/06/15 22:38:22.231:UTC] 0x0026452f 00000000 GlobalRouter SW INFO No pat
ch set.
CP1 [02/06/15 22:38:22.773:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s logServer started, pid:4840
CP1 [02/06/15 22:38:22.774:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s trcServer started, pid:4841
CP1 [02/06/15 22:38:22.774:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s oobServer started, pid:4842
CP1 [02/06/15 22:38:22.775:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s cbcp-main.x started, pid:4843
CP1 [02/06/15 22:38:22.776:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s rssServer started, pid:4844
CP1 [02/06/15 22:38:22.777:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s dbgServer started, pid:4845
CP1 [02/06/15 22:38:22.777:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s dbgShell started, pid:4846
CP1 [02/06/15 22:38:22.778:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s coreManager.x started, pid:4847
CP1 [02/06/15 22:38:22.779:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s ssio started, pid:4848
CP1 [02/06/15 22:38:22.780:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s hckServer started, pid:4849
CP1 [02/06/15 22:38:22.780:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s remCmdAgent.x started, pid:4850
CP1 [02/06/15 22:38:24.717:UTC] 0x000006cc 00000000 GlobalRouter SW INFO rcStar
t: FIPS Power Up Self Test SUCCESSFUL - 0
CP1 [02/06/15 22:38:24.718:UTC] 0x000006c2 00000000 GlobalRouter SW INFO rcStar
t: Security Stack Init SUCCESSFUL - 0
CP1 [02/06/15 22:38:24.718:UTC] 0x000006c3 00000000 GlobalRouter SW INFO rcStar
t: IPSEC Init SUCCESSFUL
CP1 [02/06/15 22:38:24.718:UTC] 0x000006bf 00000000 GlobalRouter SW INFO rcStar
t: Security Stack Log init SUCCESSFUL - 0
CP1 [02/06/15 22:38:26.111:UTC] 0x000005c0 00000000 GlobalRouter SW INFO Licens
eLoad = ZERO, loading premier license for developer debugging
IO1 [02/06/15 22:38:26.960:UTC] 0x0011054a 00000000 GlobalRouter COP-SW INFO De
tected Master CP in slot 1

--More-- (q = quit)

Switch:1(config)#show logging file module SNMP
CP1 [02/06/15 22:39:58.530:UTC] 0x00004595 00000000 GlobalRouter SNMP INFO Boot
ed with file
CP1 [02/06/15 22:39:59.547:UTC] 0x00004603 00400003.67108870 DYNAMIC CLEAR Glob
```

```
alRouter SNMP INFO 2k card up(CardNum=1 AdminStatus=1 OperStatus=1)
CP1 [02/06/15 22:39:59.547:UTC] 0x00004603 00400003.67108870 DYNAMIC CLEAR Glob
alRouter SNMP INFO 2k card up(CardNum=2 AdminStatus=1 OperStatus=1)
CP1 [02/06/15 22:39:59.547:UTC] 0x00004603 00400003.67108870 DYNAMIC CLEAR Glob
alRouter SNMP INFO 2k card up(CardNum=3 AdminStatus=1 OperStatus=1)
CP1 [02/06/15 22:40:45.839:UTC] 0x000045e5 00400005 DYNAMIC SET GlobalRouter SN
MP INFO Sending Cold-Start Trap
```

Variable definitions

Use the data in the following table to use the **show logging file** command.

Table 14: Variable definitions

Variable	Value
alarm	Displays alarm log entries.
CPU WORD<0-100>	Specifies the CPU event code and filename.
event-code WORD<0-10>	Specifies a number that precisely identifies the event reported.
module WORD<0-100>	Filters and lists the logs according to module. Specifies a string length of 0–100 characters. Categories include SNMP, EAP, RADIUS, RMON, WEB, HW, MLT, FILTER, QOS, CLILOG, SW, CPU, IP, VLAN, IPMC, PIM, POLICY, and SNMPLOG. To specify multiple filters, separate each category by the vertical bar (), for example, FILTER QOS.
name-of-file WORD<1-99>	Displays the valid logs from this file. For example, /intflash/logcopy.txt. You cannot use this command on the current log file—the file into which the messages are currently logged. Specify a string length of 1–99 characters. If you enable enhanced secure mode, the system encrypts the entire log file. After you use the show log file name-of-file WORD<1-99> command, the system takes the encrypted log file name as input, then decrypts it, and prints the output to the screen. You can then redirect the decrypted output to a file that you can store onto the flash. If enhanced secure mode is disabled, the system only encrypts the proprietary portion of the log file.
save-to-file WORD<1-99>	Redirects the output to the specified file and removes all encrypted information. You cannot use the tail option with the save-to-file option. Specify a string length of 1–99 characters.
severity WORD<0-25>	Filters and lists the logs according to severity. Choices include INFO, ERROR, WARNING, and FATAL. To specify multiple filters, separate each severity by the vertical bar (), for example, ERROR WARNING FATAL.
tail	Shows the last results first.
vrf WORD<0-32>	Specifies the name of a VRF instance to show log messages that only pertain to that VRF.

Configuring ACLI logging

Use ACLI logging to track all ACLI commands executed and for fault management purposes. The ACLI commands are logged to the system log file as CLILOG module.

About this task

* Note:

The platform logs CLILOG and SNMPLOG as INFO. Normally, if you configure the logging level to WARNING, the system skips all INFO messages. However, if you enable CLILOG and SNMPLOG the system logs ACLI Log and SNMP Log information regardless of the logging level you set. This is not the case for other INFO messages.

Procedure

1. Enter Global Configuration mode:


```
enable
configure terminal
```
2. Enable ACLI logging:


```
clilog enable
```
3. **(Optional)** Disable ACLI logging:


```
no clilog enable
```
4. Ensure that the configuration is correct:


```
show clilog
```
5. View the ACLI log:


```
show logging file module clilog
```

Example

Enable ACLI logging, and view the ACLI log:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#clilog enable
Switch:1(config)#show logging file module clilog
CP1 [02/13/13 17:27:25.956] 0x002c0600 00000000 GlobalRouter CLILOG INFO 1 CONSOLE
rwa show snmp-server host
CP1 [02/13/13 17:28:10.100] 0x002c0600 00000000 GlobalRouter CLILOG INFO 2 CONSOLE
rwa show snmp-server notif
CP1 [02/13/13 17:28:45.732] 0x002c0600 00000000 GlobalRouter CLILOG INFO 3 CONSOLE
rwa snmp-server force-trap
CP1 [02/13/13 17:29:30.628] 0x002c0600 00000000 GlobalRouter CLILOG INFO 4 CONSOLE
rwa show logging file modug
CP1 [02/14/13 19:39:11.648] 0x002c0600 00000000 GlobalRouter CLILOG INFO 5 CONSOLE
rwa ena
CP1 [02/14/13 19:39:13.420] 0x002c0600 00000000 GlobalRouter CLILOG INFO 6 CONSOLE
rwa conf t
CP1 [02/14/13 19:49:21.044] 0x002c0600 00000000 GlobalRouter CLILOG INFO 7 CONSOLE
rwa filter acl 2 enable
CP1 [02/14/13 19:50:08.540] 0x002c0600 00000000 GlobalRouter CLILOG INFO 8 CONSOLE
```

Log configuration using ACLI

```
rwa filter acl 2 type inpol
CP1 [02/14/13 19:50:38.444] 0x002c0600 00000000 GlobalRouter CLILOG INFO 9 CONSOLE
rwa filter acl 2 type inpoe
CP1 [02/14/13 19:50:52.968] 0x002c0600 00000000 GlobalRouter CLILOG INFO 10 CONSOLE
rwa filter acl enable 2
CP1 [02/14/13 19:51:08.908] 0x002c0600 00000000 GlobalRouter CLILOG INFO 11 CONSOLE
rwa filter acl 2 enable
CP1 [02/15/13 06:50:25.972] 0x002c0600 00000000 GlobalRouter CLILOG INFO 14 CONSOLE
rwa ena
CP1 [02/15/13 06:50:30.288] 0x002c0600 00000000 GlobalRouter CLILOG INFO 15 CONSOLE
rwa conf t
CP1 [02/15/13 06:50:39.412] 0x002c0600 00000000 GlobalRouter CLILOG INFO 16 CONSOLE
rwa show vlan basic
CP1 [02/15/13 06:51:09.488] 0x002c0600 00000000 GlobalRouter CLILOG INFO 17 CONSOLE
rwa show isis spbm
CP1 [02/15/13 06:56:00.992] 0x002c0600 00000000 GlobalRouter CLILOG INFO 19 CONSOLE
rwa spbm 23 b-vid 2 primar1
CP1 [02/15/13 06:56:59.092] 0x002c0600 00000000 GlobalRouter CLILOG INFO 20 CONSOLE
rwa show isis
CP1 [02/15/13 07:10:54.928] 0x002c0600 00000000 GlobalRouter CLILOG INFO 21 CONSOLE
rwa show isis interface
CP1 [02/15/13 07:12:33.404] 0x002c0600 00000000 GlobalRouter CLILOG INFO 22 CONSOLE
rwa show isis spbm
CP1 [02/15/13 07:45:28.596] 0x002c0600 00000000 GlobalRouter CLILOG INFO 23 CONSOLE
rwa ena
CP1 [02/15/13 07:45:30.236] 0x002c0600 00000000 GlobalRouter CLILOG INFO 24 CONSOLE
rwa conf t
CP1 [02/15/13 07:46:29.456] 0x002c0600 00000000 GlobalRouter CLILOG INFO 25 CONSOLE
rwa interface gigabitEther0
CP1 [02/15/13 07:47:28.476] 0x002c0600 00000000 GlobalRouter CLILOG INFO 26 CONSOLE
rwa encapsulation dot1q

--More-- (q = quit)
```

Variable definitions

Use the data in the following table to use the `cliilog` commands.

Table 15: Variable definitions

Variable	Value
enable	Activates ACLI logging. To disable, use the <code>no cliilog enable</code> command.

Chapter 10: Log configuration using EDM

Use log files and messages to perform diagnostic and fault management functions. This section provides procedures to configure and use the logging system in Enterprise Device Manager (EDM).

Configuring the system log

About this task

Configure the system log to track all user activity on the device. The system log can send messages of up to ten syslog hosts.

Procedure

1. In the navigation tree, expand the following folders: **Configuration > Edit > Diagnostics**.
2. Click **System Log**.
3. In the **System Log** tab, select **Enable**.
4. Configure the maximum number of syslog hosts.
5. Configure the IP header type for the syslog packet.
6. Click **Apply**.

System Log field descriptions

Use the data in the following table to use the **System Log** tab.

Name	Description
Enable	Enables or disables the syslog feature. If you select this variable, this feature sends a message to a server on a network that is configured to receive and store diagnostic messages from this device. You can configure the type of messages sent. The default is enabled.
MaxHosts	Specifies the maximum number of remote hosts considered active and can receive messages from the syslog service. The range is 0–10 and the default is 5.

Table continues...

Name	Description
OperState	Specifies the operational state of the syslog service. The default is active.
Header	<p>Specifies the IP header in syslog packets to circuitlessIP or default.</p> <ul style="list-style-type: none"> If the value is default, the IP address of the VLAN is used for syslog packets that are transmitted in-band using input/output (I/O) ports. If the value is circuitlessIP, the circuitless IP address is used in the IP header for all syslog messages (in-band or out-of-band). If you configure multiple circuitless IPs, the first circuitless IP configured is used. <p>The default value is default.</p>

Configuring the system log table

About this task

Use the system log table to customize the mappings between the severity levels and the type of alarms.

You can log system log messages to internal system log hosts with both IPv4 and IPv6 addresses. When you configure the system log table, under the **System Log Table** tab, you must select **ipv4** or **ipv6** in the **AddressType** box. The **Address** box supports both IPv4 and IPv6 addresses.

Procedure

1. In the navigation tree, expand the following folders: **Configuration > Edit > Diagnostics**.
2. Click **System Log**.
3. Click the **System Log Table** tab.
4. Click **Insert**.
5. Configure the parameters as required.
6. Click **Insert**.
7. To modify mappings, double-click a parameter to view a list of options.
8. Click **Apply**.

System Log Table field descriptions

Use the data in the following table to use the **System Log Table** tab.

Name	Description
Id	Specifies the ID for the syslog host. The range is 1–10.
AddressType	Specifies if the address is an IPv4 or IPv6 address.
Address	Specifies the IP address of the syslog host. You can log system log messages to external system log hosts with both IPv4 and IPv6 addresses.
UdpPort	Specifies the UDP port to use to send messages to the syslog host (514–530). The default is 514.
Enable	Enables or disables the sending of messages to the syslog host. The default is disabled.
HostFacility	Specifies the syslog host facility used to identify messages (local0 to local7). The default is local7.
Severity	Specifies the message severity for which syslog messages are sent. The default is info warning error fatal.
MapInfoSeverity	Specifies the syslog severity to use for INFO messages. The default is info.
MapWarningSeverity	Specifies the syslog severity to use for WARNING messages. The default is warning.
MapErrorSeverity	Specifies the syslog severity to use for ERROR messages. The default is error.
MapFatalSeverity	Specifies the syslog severity to use for FATAL messages. The default is emergency.
MapMfgSeverity	Specifies the syslog severity to use for Accelar manufacturing messages. The default is notice.
SecureForwardingTcpPort	Specifies the TCP port to use for secure forwarding for a particular host. The default is 1025.
SecureForwardingMode	Enables or disables secure forwarding of syslog over remote port forwarding. The supported values are ssh, tls, and none. The default is none, which means that secure forwarding is disabled.
SecureForwardingServerCertName	Specifies the server certificate name. Certificate validation is done only if the server certificate name is configured.

Chapter 11: SNMP trap configuration using ACLI

Use Simple Network Management Protocol (SNMP) traps and notifications to gather information about device activities, alarms, and other information on management stations.

For more information about how to configure SNMP community strings and related topics, see *Security for Avaya Virtual Services Platform 4000 Series*, NN46251-601.

Configuring an SNMP host

About this task

Configure an SNMP host so that the system can forward SNMP traps to a host for monitoring. You can use SNMPv1, SNMPv2c, or SNMPv3. You configure the target table parameters (security name and model) as part of the host configuration.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Configure an SNMPv1 host:

```
snmp-server host WORD<1-256> [port <1-65535>] v1 WORD<1-32> [filter WORD<1-32>]
```

3. Configure an SNMPv2c host:

```
snmp-server host WORD<1-256> [port <1-65535>] v2c WORD<1-32> [inform [timeout <0-2147483647>] [retries <0-255>] [mms <1-2147483647>]] [filter WORD<1-32>]
```

4. Configure an SNMPv3 host:

```
snmp-server host WORD<1-256> [port <1-65535>] v3 {noAuthNoPriv|authNoPriv|AuthPriv} WORD<1-32> [inform [timeout <1-2147483647>] [retries <0-255>]] [filter WORD<1-32>]
```

5. Ensure that the configuration is correct:

```
show snmp-server host
```

Example

1. Configure the target table entry:

```
VSP-4850GTS(config)# snmp-server host 198.202.188.207 port 162 v2c
ReadView inform timeout 1500 retries 3 mms 484
```

2. Configure an SNMPv3 host:

```
VSP-4850GTS(config)# snmp-server host 4717:0:0:0:0:0:7933:6 port 163
v3 authPriv Lab3 inform timeout 1500 retries 3
```

Variable definitions

Use the data in the following table to use the `snmp-server host` command.

Table 16: Variable definitions

Variable	Value
inform [timeout <1-2147483647>] [retries <0-255>] [mms <1-2147483647>]	Sends SNMP notifications as inform (rather than trap). To use all three options in one command, you must use them in the following order: <ol style="list-style-type: none"> 1. timeout <1-2147483647> specifies the timeout value in seconds with a range of 1–214748364. 2. retries <0-255> specifies the retry count value with a range of 0–255. 3. mms <1-2147483647> specifies the maximum message size as an integer with a range of 1–2147483647.
filter WORD<1-32>	Specifies the filter profile to use.
noAuthNoPriv authNoPriv AuthPriv	Specifies the security level.
port <1-65535>	Specifies the host server port number.
WORD<1-32>	Specifies the security name, which identifies the principal that generates SNMP messages.
WORD<1-256>	Specifies an IPv4 or IPv6 address.

Configuring an SNMP notify filter table

Before you begin

- For more information about the notify filter table, see RFC3413.

About this task

Configure the notify table to select management targets to receive notifications, as well as the type of notification to send to each management target.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Create a new notify filter table:

```
snmp-server notify-filter WORD<1-32> WORD<1-32>
```

3. Ensure that the configuration is correct:

```
show snmp-server notify-filter
```

Example

```
VSP-4850GTS(config)#snmp-server notify-filter profile3
99.3.6.1.6.3.1.1.4.1
```

```
VSP-4850GTS#show snmp-server notify-filter
```

```
=====
Notify Filter Configuration
=====
Profile Name          Subtree                Mask
-----
profile1              +99.3.6.1.6.3.1.1.4.1  0x7f
profile2              +99.3.6.1.6.3.1.1.4.1  0x7f
profile3              +99.3.6.1.6.3.1.1.4.1  0x7f
```

Variable definitions

Use the data in the following table to use the `snmp-server notify-filter` command.

Table 17: Variable definitions

Variable	Value
<code>WORD<1-32> WORD<1-32></code>	<p>Creates a notify filter table.</p> <p>The first instance of <code>WORD<1-32></code> specifies the name of the filter profile with a string length of 1–32.</p> <p>The second instance of <code>WORD<1-32></code> identifies the filter subtree OID with a string length of 1–32.</p> <p>If the subtree OID parameter uses a plus sign (+) prefix (or no prefix), this indicates include. If the subtree OID uses the minus sign (–) prefix, it indicates exclude.</p> <p>You do not calculate the mask because it is automatically calculated. You can use the wildcard character, the asterisk (*), to</p>

Variable	Value
	specify the mask within the OID. You do not need to specify the OID in the dotted decimal format; you can alternatively specify that the MIB parameter names and the OIDs are automatically calculated.

Configuring SNMP interfaces

About this task

Configure an interface to send SNMP traps. If Avaya Virtual Services Platform 4000 Series has multiple interfaces, configure the IP interface from which the SNMP traps originate.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Configure the destination and source IP addresses for SNMP traps:

```
snmp-server sender-ip {A.B.C.D} {A.B.C.D}
```

3. If required, send the source address (sender IP) as the sender network in the notification message:

```
snmp-server force-trap-sender enable
```

4. If required, force the SNMP and IP sender flag to use the same value:

```
snmp-server force-iphdr-sender enable
```

Example

```
VSP-4850GTS(config)#snmp-server sender-ip 172.16.120.2 172.16.120.5
VSP-4850GTS(config)#no snmp-server force-iphdr-sender enable
```

Variable definitions

Use the data in the following table to use the `snmp-server` command.

Table 18: Variable definitions

Variable	Value
authentication-trap enable	Activates the generation of authentication traps.

Table continues...

Variable	Value
force-iphdr-sender enable	Automatically configures the SNMP and IP sender to the same value. The default is disabled.
force-trap-sender enable	Sends the configured source address (sender IP) as the sender network in the notification message.
sender-ip <A.B.C.D> <A.B.C.D>	Configures the SNMP trap receiver and source IP addresses. Specify the IP address of the destination SNMP server that receives the SNMP trap notification in the first IP address. Specify the source IP address of the SNMP trap notification packet that is transmitted in the second IP address. If this address is 0.0.0.0, the system uses the IP address of the local interface that is closest (from an IP routing table perspective) to the destination SNMP server.

Enabling SNMP trap logging

Use SNMP trap logging to send a copy of all traps to the syslog server.

Before you begin

- You must configure and enable the syslog server.

About this task

Note:

The platform logs CLILOG and SNMPLOG as INFO. Normally, if you configure the logging level to WARNING, the system skips all INFO messages. However, if you enable CLILOG and SNMPLOG the system logs ACLI Log and SNMP Log information regardless of the logging level you set. This is not the case for other INFO messages.

Procedure

1. Enter Global Configuration mode:


```
enable
configure terminal
```
2. Enable SNMP trap logging:


```
snmplog enable
```
3. **(Optional)** Disable SNMP trap logging:


```
no snmplog enable
```
4. View the contents of the SNMP log:


```
show logging file module snmplog
```

Example

Enable SNMP trap logging and view the contents of the SNMP log:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#snmplog enable
Switch:1(config-app)#show logging file module snmp
CP1 [02/06/15 22:39:58.530:UTC] 0x00004595 00000000 GlobalRouter SNMP INFO Boot
ed with file
CP1 [02/06/15 22:39:59.547:UTC] 0x00004603 00400003.67108870 DYNAMIC CLEAR Glob
alRouter SNMP INFO 2k card up(CardNum=1 AdminStatus=1 OperStatus=1)
CP1 [02/06/15 22:39:59.547:UTC] 0x00004603 00400003.67108870 DYNAMIC CLEAR Glob
alRouter SNMP INFO 2k card up(CardNum=2 AdminStatus=1 OperStatus=1)
CP1 [02/06/15 22:39:59.547:UTC] 0x00004603 00400003.67108870 DYNAMIC CLEAR Glob
alRouter SNMP INFO 2k card up(CardNum=3 AdminStatus=1 OperStatus=1)
CP1 [02/06/15 22:40:45.839:UTC] 0x000045e5 00400005 DYNAMIC SET GlobalRouter SN
MP INFO Sending Cold-Start Trap
```

Variable definitions

Use the data in the following table to use the `snmplog` command.

Table 19: Variable definitions

Variable	Value
enable	<p>Enables the logging of traps.</p> <p>Use the command <code>no snmplog enable</code> to disable the logging of traps.</p>
file [grep WORD<1–255> tail]	<p>The parameter only applies to log files generated by releases prior to Release 3.2:</p> <p>Shows the trap log file stored on external flash. You can optionally specify search or display parameters:</p> <ul style="list-style-type: none"> • <code>grep WORD<1–255></code> performs a string search in the log file. <i>WORD<1–255></i> is the string, of up to 255 characters in length, to match. • <code>tail</code> shows the last results first.

Chapter 12: SNMP trap configuration using EDM

Use Simple Network Management Protocol (SNMP) traps and notifications to gather information about device activities, alarms, and other information on management stations. This section provides procedures to configure and use SNMP traps in Enterprise Device Manager (EDM).

For information about how to configure SNMP community strings and related topics, see *Security for Avaya Virtual Services Platform 4000 Series*, NN46251-601.

Configuring an SNMP host target address

About this task

Configure a target table to specify the list of transport addresses to use in the generation of SNMP messages.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Edit** > **SnmpV3**.
2. Click **Target Table**.
3. In the **Target Table** tab, click **Insert**.
4. In the **Name** box, type a unique identifier.
5. In the **TDomain** box, select the transport type of the address. Select **ipv4Tdomain** or **ipv6Tdomain**.
6. In the **TAddress** box, type the transport address and User Datagram Protocol (UDP) port.
7. In the **Timeout** box, type the maximum round trip time.
8. In the **RetryCount** box, type the number of retries to be attempted.
9. In the **TagList** box, type the list of tag values.
10. In the **Params** box, type the SnmpAdminString.
11. In the **TMask** box, type the mask.
12. In the **MMS** box, type the maximum message size.
13. Click **Insert**.

Target Table field descriptions

Use the data in the following table to use the **Target Table** tab.

Name	Description
Name	Specifies a unique identifier for this table. The name is a community string.
TDomain	Specifies the transport type of the address. ipv4Tdomain specifies the transport type of address is an IPv4 address and ipv6Tdomain specifies the transport type of address is IPv6. The default is ipv4Tdomain.
TAddress	Specifies the transport address in xx.xx.xx.xx:port format, for example: 10:10:10:10:162, where 162 is the trap listening port on the system 10.10.10.10.
Timeout	Specifies the maximum round trip time required to communicate with the transport address. The value is in 1/100 seconds from 0–2147483647. The default is 1500. After the system sends a message to this address, if a response (if one is expected) is not received within this time period, you can assume that the response is not delivered.
RetryCount	Specifies the maximum number of retries if a response is not received for a generated message. The count can be in the range of 0–255. The default is 3.
TagList	Contains a list of tag values used to select target addresses for a particular operation. A tag refers to a class of targets to which the messages can be sent.
Params	Contains SNMP parameters used to generate messages to send to this transport address. For example, to receive SNMPv2C traps, use TparamV2.
TMask	Specifies the mask. The value can be empty or in six-byte hex string format. Tmask is an optional parameter that permits an entry in the TargetAddrTable to specify multiple addresses.
MMS	Specifies the maximum message size. The size can be zero, or 484–2147483647. The default is 484. Although the maximum MMS is 2147483647, the device supports the maximum SNMP packet size of 8192.

Configuring target table parameters

About this task

Configure the target table to configure the security parameters for SNMP. Configure the target table to configure parameters such as SNMP version and security levels.

Procedure

1. In the navigation tree, expand the following folders: **Configuration > Edit > SnmpV3**.
2. Click **Target Table**.
3. Click the **Target Params Table** tab.
4. Click **Insert**.
5. In the **Name** box, type a target table name.
6. From the **MPModel** options, select an SNMP version.
7. From the **Security Model** options, select the security model.
8. In the **SecurityName** box, type `readview` or `writeview`.
9. From the **SecurityLevel** options, select the security level for the table.
10. Click **Insert**.

Target Params Table field descriptions

Use the data in the following table to use the **Target Params Table** tab.

Name	Description
Name	Identifies the target table.
MPModel	Specifies the message processing model to use to generate messages: SNMPv1, SNMPv2c, or SNMPv3/USM.
SecurityModel	Specifies the security model to use to generate messages: SNMPv1, SNMPv2c, or USM. You can receive an <code>inconsistentValue</code> error if you try to configure this variable to a value for a security model that the implementation does not support.
SecurityName	Identifies the principal on whose behalf SNMP messages are generated.
SecurityLevel	Specifies the security level used to generate SNMP messages: <code>noAuthNoPriv</code> , <code>authNoPriv</code> , or <code>authPriv</code> .

Configuring an SNMP notify table

About this task

Configure the notify table to select management targets to receive notifications, as well as the type of notification to send to each management target.

Procedure

1. In the navigation tree, expand the following folders: **Configuration > Edit > SnmpV3**.
2. Click **Notify Table**.
3. In the **Notify Table** tab, click **Insert**.
4. In the **Name** box, type a notify table name.
5. In the **Tag** box, type the transport tag for the table.
6. From the **Type** options, select a type.
7. Click **Insert**.

Notify Table field descriptions

Use the data in the following table to use the **Notify Table** tab.

Name	Description
Name	Specifies a unique identifier.
Tag	Specifies the tag.
Type	<p>Determines the type of notification generated. This value is only used to generate notifications, and is ignored for other purposes. If an SNMP entity only supports generation of Unconfirmed-Class protocol data unit (PDU), this parameter can be read-only. The possible values are</p> <ul style="list-style-type: none"> • trap—messages generated contain Unconfirmed-Class Protocol Data Units (PDU) • inform—messages generated contain Confirmed-Class PDUs <p>The default value is trap.</p>

Configuring SNMP notify filter profiles

About this task

Configure the SNMP table of filter profiles to determine whether particular management targets receive particular notifications.

Procedure

1. In the navigation tree, expand the following folders: **Configuration > Edit > SnmpV3**.
2. Click **Notify Table**.
3. Click the **Notify Filter Table** tab.
4. Click **Insert**.
5. In the **NotifyFilterProfileName** box, type a name for the notify filter profile.
6. In the **Subtree** box, type subtree location information in x.x.x.x.x.x.x.x format.
7. In the **Mask** box, type the mask location in hex string format.
8. From the **Type** options, select **included** or **excluded**.
9. Click **Insert**.

Notify Filter Table field descriptions

Use the data in the following table to use the **Notify Filter Table** tab.

Name	Description
NotifyFilterProfileName	Specifies the name of the filter profile used to generate notifications.
Subtree	Specifies the MIB subtree that, if you combine it with the mask, defines a family of subtrees, which are included in or excluded from the filter profile. For more information, see RFC2573.
Mask	Specifies the bit mask (in hexadecimal format) that, in combination with Subtree, defines a family of subtrees, which are included in or excluded from the filter profile.
Type	Indicates whether the family of filter subtrees are included in or excluded from a filter. The default is included.

Configuring SNMP notify filter profile table parameters

Before you begin

- The notify filter profile exists.

About this task

Configure the profile table to associate a notification filter profile with a particular set of target parameters.

Procedure

1. In the navigation tree, expand the following folders: **Configuration > Edit > SnmpV3**.
2. Click **Notify Table**.

3. Click the **Notify Filter Profile Table** tab.
4. Click **Insert**.
5. In the **TargetParamsName** box, type a name for the target parameters.
6. In the **NotifyFilterProfileName** box, type a name for the notify filter profile.
7. Click **Insert**.

Notify Filter Profile Table field descriptions

Use the data in the following table to use the **Notify Filter Profile Table** tab.

Name	Description
TargetParamsName	Specifies the unique identifier associated with this entry.
NotifyFilterProfileName	Specifies the name of the filter profile to use to generate notifications.

Enabling SNMP trap logging

About this task

Enable trap logging to save a copy of all SNMP traps.

Procedure

1. In the navigation tree, expand the following folders: **Configuration > Edit > Diagnostics**.
2. Click **General**.
3. Click the **Error** tab.
4. Select **AuthenticationTraps**.
5. Click **Apply**.

Error field descriptions

Use the data in the following table to use the **Error** tab.

Name	Description
AuthenticationTraps	Enables or disables the sending of traps after an error occurs. The default is disabled.
LastErrorCode	Specifies the last reported error code.
LastErrorSeverity	Specifies the last reported error severity:

Table continues...

Name	Description
	0= Informative Information 1= Warning Condition 2= Error Condition 3= Manufacturing Information 4= Fatal Condition