



Administering Avaya Diagnostic Server with SLA MonTM

Release 2.0
Issue 3
December 2014

© 2014 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 by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. 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 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: <http://support.avaya.com> 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.

Licenses

THE SOFTWARE LICENSE TERMS OR SUPPORT TOOLS LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO](http://support.avaya.com/licenseinfo) 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 and Support Tools, 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.

License 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.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Support tools

"AVAYA SUPPORT TOOLS" MEAN THOSE SUPPORT TOOLS PROVIDED TO PARTNERS OR CUSTOMERS IN CONNECTION WITH MAINTENANCE SUPPORT OF AVAYA EQUIPMENT (E.G., SAL, SLA MON, AVAYA DIAGNOSTIC SERVER, ETC.) AVAYA SUPPORT TOOLS ARE INTENDED TO BE USED FOR LAWFUL DIAGNOSTIC AND NETWORK INTEGRITY PURPOSES ONLY. The customer is responsible for understanding and complying with applicable legal requirements with regard to its network. The Tools may contain diagnostic capabilities that allow Avaya, authorized Avaya partners, and authorized customer administrators to capture packets, run diagnostics, capture key strokes and information from

endpoints including contact lists, and remotely control and monitor end-user devices. The customer is responsible for enabling these diagnostic capabilities, for ensuring users are aware of activities or potential activities and for compliance with any legal requirements with respect to use of the Tools and diagnostic capabilities on its network, including, without limitation, compliance with laws regarding notifications regarding capture of personal data and call recording.

Avaya Support Tools are provided as an entitlement of Avaya Support Coverage (e.g., maintenance) and the entitlements are established by Avaya. The scope of the license for each Tool is described in its License terms and/or the applicable service description document.

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.

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: <http://support.avaya.com/Copyright> or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

Note to Service Provider

The product or Hosted Service may use Third Party Components subject to Third Party Terms that do not allow hosting and require a Service Provider to be independently licensed for such purpose. It is your responsibility to obtain such licensing.

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: <http://support.avaya.com> or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: <http://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: <http://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, 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	8
Purpose of the document	8
Intended audience	8
Document changes since the last issue	8
Related resources	9
Documentation	9
Viewing Avaya Mentor videos	10
Support	10
Chapter 2: SLA Mon overview	11
SLA Mon technology	11
The SLA Mon server and agent deployment	12
SLA Mon security	13
SLA Mon Server security features and recommendations	13
Encryption	13
Firewall and ports	14
Packaging and updates	14
Other security notes	14
Supported products	15
SLA Mon terminology	15
Chapter 3: Managing user configuration of the SLA Mon server	16
Authentication of SLA Mon users using PAM	16
Creating an administrator user on SLA Mon Server	16
Chapter 4: Managing the SLA Mon server license	18
SLA Mon server licensing overview	18
Installing the SLA Mon server license on WebLM	18
Changing the WebLM server address	20
Changing the WebLM server address after the SLA Mon license expires	21
Chapter 5: Managing the SLA Mon server security	22
SSL protocol configuration for the SLA Mon server	22
The SSL protocol for the SLA Mon server	22
Changing the SSL protocol and ciphers for the SLA Mon UI	22
Making changes to the SSL certificates of the SLA Mon server UI	23
Replacing the SSL certificate of the SLA Mon server UI	23
Adding client SSL certificates to the truststore of the SLA Mon server UI	24
Chapter 6: Managing certificates for the communication between the server and the agent	26
Secure communication between the server and the agent	26
Methods to obtain digital certificates	27
Administering the server certificate	27

Certificate enrollment by a signing authority or an in-house CA.....	27
Use of a self-signed certificate.....	33
Use of the Avaya demo certificate.....	40
Administering the CA root certificate on the SLA Mon agents.....	41
The CA root certificate administration on 96x0 and 96x1 series IP deskphones.....	41
The CA root certificate administration on G450 and G430 Media Gateways.....	47
The CA root certificate administration on VSP switches.....	50
Chapter 7: Initial administration.....	54
Initial administration.....	54
Logging on to the SLA Mon web interface.....	54
Administering SLA Mon agents on the SAL Mon server.....	55
Discovering SLA Mon agents.....	55
Agent Discovery field and icon descriptions.....	56
Viewing agent details through a search.....	57
Viewing agent details through the location tree.....	58
Changing the status of an agent.....	59
Agent Search field descriptions.....	59
Administering the SLA Mon server properties.....	61
Administration of the SLA Mon Server properties.....	61
Configuring SNMP traps.....	62
Configuring alarming properties.....	68
Modifying DSCP values.....	72
Test Setup.....	73
Configuring system properties.....	73
System Properties.....	73
Administering zones.....	74
Zone management.....	74
Creating a zone.....	74
Renaming a zone.....	74
Deleting a zone.....	75
Adding a subnet location to a zone.....	75
Removing a subnet location from a zone.....	75
Chapter 8: Administering the SLA Mon server through CLI.....	76
Administration of SLA Mon through CLI.....	76
Starting a CLI session on the SLA Mon server.....	76
CLI commands for the SLA Mon server.....	77
Viewing the CLI commands for the SLA Mon server.....	82
Discovering SLA Mon agents through CLI of the SLA Mon server.....	82
Chapter 9: Administering test patterns.....	83
Test patterns.....	83
Adding a test pattern.....	83
Copying a test pattern.....	84
Deleting a test pattern.....	84

Customizing an automatic test pattern.....	85
Customizing a manual test pattern.....	85
Exporting a test pattern.....	86
Importing data to a test pattern.....	87
Test Patterns field descriptions.....	88
Test Execution.....	91
Running a user-defined test pattern.....	91
Viewing the list of subnet pairs in a test pattern.....	92
Chapter 10: Remotely controlling Avaya endpoints.....	93
Remote control of Avaya endpoints.....	93
Remotely controlling Avaya endpoints through the SLA Mon web interface.....	94
Starting a remote control session from the SLA Mon web interface.....	94
Agent Remote page.....	95
Using the SLA Mon web interface to remotely control touch screen interactions.....	97
Using the SLA Mon web interface to make a call from a remotely controlled Avaya endpoint.....	98
Remotely controlling Avaya endpoints through CLI.....	98
Starting a phone remote control session from CLI of SLA Mon Server.....	98
CLI commands for the phone remote control mode.....	99
Initiating a call remotely using CLI of SLA Mon Server.....	100
Answering a call coming to a remotely controlled endpoint through CLI of SLA Mon Server.....	101
Pressing buttons on an endpoint remotely controlled by CLI.....	101
Getting a screenshot of the current display on an endpoint.....	102
Monitoring events on an endpoint through CLI.....	102
Stopping event monitoring through CLI of SLA Mon Server.....	103
Making bulk calls from CLI.....	103
Chapter 11: Packet capture.....	105
Packet capture overview.....	105
Packet capture through the SLA Mon web interface.....	105
Starting a packet capture session through the SLA Mon web interface.....	105
Packet Capture field descriptions.....	107
Downloading captured packets through the SLA Mon web interface.....	108
Packet capture through the SLA Mon CLI.....	109
Starting a packet capture session through CLI.....	109
Downloading captured packets through CLI.....	110
Removing packet capture instances through CLI.....	111
Chapter 12: Network Monitoring.....	113
Overview.....	113
Network Summary page.....	113
Viewing the network summary for a traffic type and a performance parameter.....	117
Viewing network summary based on selected zones and locations.....	118
Viewing the intrazone network summary grid.....	118
Viewing the network performance graphs between two locations.....	119

Chart Detail page.....	119
Chapter 13: Troubleshooting	124
Agents stop responding to commands, and “BAD_KEY” errors are seen in any of the /var/log/ slamon/* log files.....	124
Tests failing, or remote control and packet capture not working after successful discovery.....	124
Unable to remote control the 9641 SIP phones after a reboot.....	125
FAQs.....	125
Appendix A: Alarms that the SLA Mon server generates	128
Appendix B: Additional certificate-related information	130
Viewing certificate properties.....	130
Identify certificate chain.....	131
PEM/X509 format certificate.....	131
Copying the CA root certificate installed on the SLA Mon server.....	132
Product SHA256 and Intermediate CA support.....	133

Chapter 1: Introduction

Purpose of the document

The guide provides information about the following:

- Overview of the diagnostic features of Avaya Diagnostic Server with the SLA Mon™ technology.
- Administration of the SLA Mon server and agents.
- Use of the diagnostic features to monitor Avaya endpoints and customer network for troubleshooting and servicing.

Intended audience

The audience for this document is anyone who:

- Installs and configures Avaya Diagnostic Server.
- Administers the SLA Mon™ server.
- Uses the diagnostic features of Avaya Diagnostic Server with SLA Mon™ to monitor and troubleshoot Avaya endpoints, Ethernet Routing Switches (ERS), Virtual Services Platform (VSP) switches, and Avaya Branch Gateways on the customer network.
- Uses the diagnostic features of Avaya Diagnostic Server with SLA Mon™ to monitor customer network.

The audience includes and is not limited to implementation engineers, support personnel, and network engineers from Avaya, business partners, and customers.

Document changes since the last issue

The following changes have been made to this document since the last issue:

- Rewrote the information in Chapter 6, *Managing certificates for the communication between the server and the agent*, with new sections for managing certificates.
- Removed Chapter 3, *Administering the SLA Mon agent*, and merged the content to other relevant chapters.

- Modified the SLA Mon parameter descriptions in the *SLA Mon agent parameters in the endpoints settings file* section.

Related resources

Documentation

The following table lists the documents related to Avaya Diagnostic Server. Download the documents from the Avaya Support website at <http://support.avaya.com>.

Title	Description	Audience
Implementation		
<i>Deploying Avaya Diagnostic Server</i>	Describes the implementation requirements and procedures to deploy the Avaya Diagnostic Server software.	Sales engineers, solution architects, implementation engineers, support personnel, and customers
<i>Deploying Avaya Diagnostic Server using VMware® in the Virtualized Environment</i>	Describes the implementation requirements and procedures to deploy Avaya Diagnostic Server open virtual appliance (OVA) in a virtualized environment.	Sales engineers, solution architects, implementation engineers, support personnel, and customers
Administration		
<i>Administering Avaya Diagnostic Server with SAL Gateway</i>	Provides information about configuring and administering SAL Gateway for remote servicing and alarm transfer facilities of Avaya products at a customer site.	Solution architects, implementation engineers, support personnel, and customers
Other		
<i>Avaya Diagnostic Server Additional Security Configuration Guidance</i>	Provides information on the additional measures that you can take on the Avaya Diagnostic Server host to meet customer security requirements and policies.	Implementation engineers, support personnel, and customers
<i>Avaya Diagnostic Server Port Matrix</i>	Provides information on the ports and sockets that Avaya Diagnostic Server components use. You can use this information to configure your firewall according to your requirements and policies.	Implementation engineers, support personnel, and customers

Title	Description	Audience
<i>Supported products interoperability list for Avaya Diagnostic Server with SLA Mon™</i>	Provides a list of Avaya products that support SLA Mon agent for remote diagnostics and monitoring of the products and the customer network.	Sales engineers, solution architects, implementation engineers, support personnel, and customers

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.

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.

Chapter 2: SLA Mon overview

SLA Mon technology

Avaya Diagnostic Server uses a patented technology, SLA Mon™, to provide you endpoint and network diagnostics features including network monitoring, phone remote control, and packet capture. Through the SLA Mon technology, you can conduct an end-to-end network testing and monitor endpoints to diagnose conditions that might affect the performance of devices and the network.

Note:

An endpoint is an interface that a communicating party uses to connect to a communication channel or a system. Avaya supports various kinds of endpoints that include soft endpoints, video endpoints, and digital, DECT, and IP telephones.

Benefits of SLA Mon

- Extended monitoring capabilities from network to device.
- Improved remote service by reducing the need of onsite technicians and time-consuming deployment of sniffers and other tools.
- Improved testing by providing the ability to automate phone testing and certify readiness in the field during implementation.

Features of SLA Mon

Avaya Diagnostic Server with SLA Mon provides the following features:

Feature	Description
Phone remote control	The phone remote control feature is useful in troubleshooting Avaya endpoints remotely. Through this feature, service professional from Avaya, Partners, and customer can remotely access and control Avaya endpoints that have an SLA Mon agent that is registered with the SLA Mon server. You can also perform remote activities on the endpoints, such as the following: • Press buttons or perform touch events • Trigger calls between Avaya endpoints remotely and observe the events occurring on the remote endpoint.

Feature	Description
Packet capture	The packet capture feature captures the network traffic flowing in and out of Avaya endpoints. You can configure the SLA Mon agent on an endpoint to capture a copy of the network traffic sent and received by the agent. You can analyze the packets to identify issues with the device.
Event monitoring	You can use the event monitoring feature to monitor events occurring on Avaya endpoints, such as button presses or touch events.
Screen capture	You can configure the SLA Mon agent to capture and send a screen shot of the display of Avaya endpoints on request from the server. Service personnel can use the screen capture feature to verify user comments and monitor the screen of the endpoints.
Bulk calls	You can use the bulk calls feature to stress test the communication system and the network. For example, if a branch location has to support 50 simultaneous calls to the central office, you can use the bulk calls feature to simulate the requirement.
Network monitoring	The network monitoring features provide vendor agnostic, end-to-end network insight into conditions that might have an impact on your voice, video, and data applications. The feature provides an easy-to-understand visual representation of your network performance data. Using the network-performance and the call-trace data, you can proactively identify and troubleshoot network issues. The network monitoring feature displays the results of the network performance tests using colored grids and graphs.

The SLA Mon server and agent deployment

You can use the SLA Mon server and agents for network monitoring purposes, providing a network wide analysis of differentiated services (DiffServ) and relationship of DiffServ to the network performance.

The SLA Mon server is configured to run periodic Real-time Transport Protocol (RTP) tests between pairs of SLA Mon agents that are present on Avaya endpoints. The SLA Mon server analyzes the test data and monitors network QoS, such as loss, jitter, delay, and e-MOS. The SLA Mon server provides a history of network QoS metrics and the relationship of the QoS parameters to the network topology and DiffServ.

To check priority remarkings of packets, the server also runs TraceRoute tests periodically.

*** Note:**

Normally, a RTP test take 10 seconds to complete. A TraceRoute test runs once in every 20 minutes. A RTP tests takes more than 10 seconds to complete in case the TraceRoute test runs in parallel.

To reduce the possibility of interruption during network monitoring, Avaya recommends that you use a static configuration on the Avaya endpoints used for monitoring the network and deploy the endpoints at locations where the endpoints are safe from inadvertent disruptions, such as a communication closet.

In a multi-site MPLS network, Avaya recommends that you deploy at least one SLA Mon agent at each site to monitor the performance across the WAN link at each site. You can deploy some additional SLA Mon agents on the site voice subnets to detect DiffServ issues that are attributable to the LAN.

SLA Mon security

SLA Mon agent is discovered by the SLA Mon server. After the discovery packet is detected, the agent registers with the server and sends the discovery packet. The registration process requires the server to authenticate itself using a certificate signed by either the Avaya SIP Root Certificate or preferable by a customer certificate. When registered, the agent accepts the encrypted and authenticated commands from the server on which it is registered.

The variables in the settings file of Avaya endpoints are used to enable the v2 features. By default these features are disabled.

SLA Mon Server security features and recommendations

Encryption

The SLA Mon server uses industry standard technology and practices, and encrypted proprietary communication protocols to keep the server secure. The SLA Mon server uses the Transport Layer Security (TLS) key exchange to provide encryption for all communication between the server and web clients. A login page that requires a valid user name and password or a client certificate protects access to the administrative console.

The proprietary communication protocol between the server and the agent is encrypted using the Advanced Encryption Standard (AES) 128-bits algorithm. AES key exchange is protected using the SSL encryption.

Firewall and ports

For system security, Avaya recommends that you enable the iptables firewall software on the system that hosts the SLA Mon server. Red Hat Enterprise Linux (RHEL) operating system includes the iptables firewall software, enabling the firewall to block all inbound traffic except the traffic that is necessary. After installation, the server opens only those inbound ports in the firewall on the host system that are necessary for the operation of the SLA Mon server.

The server opens the following ports for the operation of the SLA Mon server.

TCP 4511	HTTPS administration console
TCP/UDP 50011	Agent communication
UDP 50010	Packet capture receiver
UDP 50009	Performance monitoring receiver

The SLA Mon server uses some additional ports internally. These ports do not require to be exposed outside the server. Internally, the SLA Mon server services gain access to these ports using the loopback interface. You must block the following ports from external access.

TCP 1099	Java RMI registry
TCP 7654	PostgreSQL database

A firewall can block outside traffic, but the firewall cannot block internal traffic that might not be from a trusted source. Therefore, to prevent any breach in the firewall protection, provide system access to system administrators and trusted users only.

For information about additional security configuration measures, see *Avaya Diagnostic Server Additional Security Configuration Guidance*. For more information about ports that the SLA Mon server uses, see *Avaya Diagnostic Server Port Matrix*.

Packaging and updates

The RPM for the SLA Mon server is digitally signed. The digital signature ensures the authenticity of the package and reduces the possibility for installation of a tampered software.

Other security notes

Security-Enhanced Linux (SELinux) can provide tighter control of system security. Unfortunately, SELinux also introduces complications that can block some software from working properly. Due to complications with PostgreSQL, do not enable the SELinux software on the system hosting the SLA Mon Server.

Supported products

For a list of Avaya products that support the SLA Mon agent, see *Supported products interoperability list for Avaya Diagnostic Server with SLA Mon™* available on the Avaya Support website at <http://support.avaya.com>.

SLA Mon terminology

The following are a few terms that are frequently mentioned in this document:

- **Alarm:** A report of an event that a device gives when it detects a potentially or actually detrimental condition. An alarm notification, sent as an SNMP trap is intended to trigger a human or computer to diagnose the problem causing the alarm and fix it.
- **Subnet (address range) on the Agent Discovery page:** An IP address range with associated location information. The range is specified in the CIDR format. The SLA Mon server uses the information on this page only during agent discovery. The SLA Mon server does not use it again for any other purpose, except during a manual rediscovery.
- **Agent:** On the customer network, each subnet has one or more agents, also called as test agents. You can find the agents by using the agent discovery process. After discovery, the agents register themselves with the SLA Mon server by supplying the agent details. The discovery process associates the location information to the agent during the discovery process.
- **SAL Gateway:** An Avaya product that provides remote access and alarming capabilities for remotely managed devices.
- **Voice over IP (VoIP):** A technology that allows telephone calls to be made over computer networks such as the Internet. VoIP converts analog voice signals into digital data packets and supports real-time, two-way transmission of conversations using Internet Protocol (IP).

Chapter 3: Managing user configuration of the SLA Mon server

Authentication of SLA Mon users using PAM

SLA Mon Server uses an authentication and authorization scheme that is integrated into the operating system using Pluggable Authentication Modules (PAM). SLA Mon Server uses the PAM configuration to authorize users.

The PAM configuration is in `/etc/pam.d/slamon`. By default, the PAM configuration is a symbolic link to point to `/etc/pam.d/login`. The authorization data comes from the operating system groups of the users.

The authorization method for SLA Mon users depends on how the system is configured. If the system uses `pam_unix`, then the authorization is through the operating system user and group management tools, such as `groupadd` and `usermod`.

 Note:

If the system uses LDAP or some other service, you must manage the groups according to the way users and groups are managed in that service. You must not use `netgroups`, but use `groups` instead.

Creating an administrator user on SLA Mon Server

About this task

You can create users with administrator-level rights to the SLA Mon Server Web interface. Use this procedure to create administrator users on SLA Mon Server that uses PAM and the local password and group files to authorize users.

 Note:

If the system uses LDAP or some other authentication or authorization provider, the group name still applies. However, the procedure for adding a group and assigning a user varies.

Procedure

1. Log on to the host server as the root user.

2. Run the following command to create the administrator user group, `eqmAdmin::`

```
groupadd eqmAdmin
```

 Note:

Creating `eqmAdmin` group is optional. The installer creates the `eqmAdmin` group during SLA Mon Server installation. Create the `eqmAdmin` group only if it is not created by the installer.

3. If an administrator user already exists, run the following command to add the user to the group:

```
usermod -a -G eqmAdmin <username>
```

4. If the user does not exist, run the following commands to create the user and set a password for the user:

```
useradd -G eqmAdmin <username>
```

```
passwd <username>
```

5. On system prompt, enter the password which you want to set for the new user ID.
6. To test the new user ID, log on to the SLA Mon Server UI using the new user ID and password.

Chapter 4: Managing the SLA Mon server license

SLA Mon server licensing overview

The SLA Mon server is licensed. You must get a valid license to use the SLA Mon server. After you install the SLA Mon component of Avaya Diagnostic Server, you get a grace period of 30 days for the initial use of the features before the license expires.

To obtain a license for the SLA Mon server, you must contact your Avaya representative.

You can choose to install the WebLM server locally as part of the SLA Mon component installation. The WebLM server comes with the Avaya Diagnostic Server installer package. Otherwise, you can use an existing WebLM server on your network.

*** Note:**

For Avaya Diagnostic Server 2.0 Open Virtualization Appliance (OVA), WebLM does not come bundled with the OVA. If you do not have an existing WebLM server, you can download the WebLM OVA from PLDS and deploy a WebLM virtual appliance. For other Avaya Diagnostic Server 2.0 installation platforms, including software only, ION, and common server, WebLM comes bundled with the software package.

*** Note:**

One WebLM server can support multiple SLA Mon server licenses. For example, if you have five SLA Mon servers, a single WebLM server license supports all five servers. You can raise a request for a license that supports five servers.

Installing the SLA Mon server license on WebLM

Before you begin

Get the license file for the SLA Mon server from your Avaya representative, and save the file at a location accessible from the WebLM server.

Configure the user for the SLA Mon server.

About this task

Use the following procedure to install the licence for the SLA Mon server locally or remotely on a WebLM server.

* Note:

If you installed the WebLM licensing server locally during the installation of the SLA Mon server component, you can install the license file from your local server. If you use a remote WebLM server for the SLA Mon license, you must log on to the remote WebLM server you specified.

Procedure

1. On the web browser, type the URL of the WebLM server as the following:

```
https://<WebLM serve hostname or IP address>:52233/WebLM/
LicenseServer
```

2. On the login page, enter the credentials of an administrator user, and click **Login**.
3. Click the **License Administration** link.

The system displays the WebLM login page.

4. When you access the WebLM server for the first time, perform the following:
 - a. Enter the default user name and password that Avaya provides to log on to the WebLM server.

* Note:

The following are the default user name and password for WebLM:

- User name: admin
- Password: weblmadmin

The system displays the page for changing the password.

- b. Change the password.
5. Log on to the WebLM server as the admin user using the new password.
 6. Navigate to **Server Properties**, and note down the Primary Host ID.
 7. Provide this Primary Host ID to Avaya PLDS to create a license.

* Note:

The Primary Host ID is the MAC address of the first network interface of the physical system.

8. In the left navigation pane on the WebLM home page, click **Install license**.
9. Click **Browse**, and select the license file from the location where you saved the file.
10. Click **Install**.

The WebLM server starts installing the license for the SLA Mon server. The system configures the license in approximately 8 to 9 minutes. After configuring the license file, the system displays the successful installation message.

*** Note:**

The WebLM license installation is common for both the web interface and the CLI of the SLA Mon server. You must install the licence before the expiry of the 30-days trial period for using the SLA Mon features. After the expiry of the trial period, you cannot use the SLA Mon features through the web interface or run any SLA Mon server CLI commands. After you install the license, the web interface does not display the `You are in the 30-days trial period` message.

Next steps

If you logged on to the SLA Mon web interface before or during the license implementation, sign out of the web interface. Sign in again at least 9 minutes after the license was installed.

You must also restart the `slamonsrvr` and `slamonweb` services of the SLA Mon server.

To restart the services, refer to step 4 and 5 of Changing the WebLM server address.

Changing the WebLM server address

About this task

You can change the IP of the WebLM server after the installation of Avaya Diagnostic Server if you entered a wrong IP address when installing the SLA Mon component. Use this procedure to change the IP address of the WebLM server. After changing the WebLM IP address, you must restart the `slamonsrvr` and `slamonweb` services of SLA Mon.

Procedure

1. Log on to the Avaya Diagnostic Server host as a user with administrative privilege.
2. Run the following command to start the SLA Mon CLI:

```
/usr/local/bin/slamoncli
```

3. Run the following command to change the WebLM server IP address:

```
setweblmipadd <IP Address>
```

Where, replace `<IP Address>` with the new IP address of the WebLM server.

4. Run the following command to restart the `slamonsrvr` service:

```
/sbin/service slamonsrvr restart
```

5. Run the following command to restart the `slamonweb` service:

```
/sbin/service slamonweb restart
```

The system updates the WebLM Server IP address.

Changing the WebLM server address after the SLA Mon license expires

About this task

You cannot use the SLA Mon web interface or CLI after the trial period of the SLA Mon license is over or the license expires. Therefore, you cannot run the SLA Mon CLI and use the **setweblmipadd** command to point to a different licensing server where you installed a valid SLA Mon license. If the SLA Mon license expires, use this procedure to change the WebLM IP address that the SLA Mon server uses for licensing.

Procedure

1. Log on to the Avaya Diagnostic Server host as root.
2. Change directory to `/opt/avaya/slamon/bin/`.
3. Run the following command to view the IP address of the WebLM server that the SLA Mon server is presently using:

```
./weblmiputil.sh -show
```

4. Run the following command to change the WebLM server address:

```
./weblmiputil.sh -update <WebLM IP address>
```

Where, replace *<IP Address>* with the IP address of the new WebLM server.

The system updates the address of the WebLM server and displays the `successfully updated` message.

5. Run the following command to view and confirm that the IP address of the WebLM server is updated:

```
./weblmiputil.sh -show
```

Next steps

After changing the WebLM address, restart the `slamonsrvr` and `slamonweb` services of SLA Mon. To restart the services, see step 4 and 5 of the procedure, Changing the WebLM server address.

Chapter 5: Managing the SLA Mon server security

SSL protocol configuration for the SLA Mon server

The SSL protocol for the SLA Mon server

The Secure Sockets Layer (SSL) protocol that the SLA Mon server uses is TLSv1. The following are the ciphers that the SLA Mon server uses:

```
TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_DSS_WITH_AES_256_CBC_SHA,TLS_RSA
_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_WITH_A
ES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,SSL_RSA_WITH_3DES_EDE_CBC_SHA
,SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
```

Changing the SSL protocol and ciphers for the SLA Mon UI

About this task

Use this procedure to change the SSL protocol and ciphers that the SLA Mon server uses for the interaction between the web browser of a user and the SLA Mon UI.

Procedure

1. Log on to the Linux host server with root privileges.
2. Add the following property to the `/var/eqm_data/autoStart.properties` file to change the ciphers for the key server:

```
keyserver.enabled-ciphers=<comma delimited ciphers>
```
3. Add the following property to the `/var/eqm_data/autoStart.properties` file to change the SSL protocol for the key server:

```
keyserver.enabled-ssl-protocols=<comma delimited protocols>
```
4. Edit the `/opt/avaya/slamon/tomcat/conf/server.xml` file as the following to change the ciphers or the protocol for the UI:

```
<Connector port="4511" server="SVCI"
```

```

maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" debug="0" scheme="https" secure="true"
clientAuth="want" sslProtocol="TLSv1"

keystorePass=<removed> keystoreFile="/opt/avaya/slamon/misc/slamon-
ui-keystore.jks"

truststorePass=<removed> truststoreFile="/opt/avaya/slamon/misc/
spirit-trust-Prod.jks"

ciphers="TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_DSS_WITH_AES_256_C
BC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA
,TLS_DHE_DSS_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,SSL_R
SA_WITH_3DES_EDE_CBC_SHA,SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA" />

```

The system sets the ciphers using the `ciphers` attribute for the connector on port 4511, and sets the protocol using the `sslProtocol` attribute.

Making changes to the SSL certificates of the SLA Mon server UI

Replacing the SSL certificate of the SLA Mon server UI

About this task

Use this procedure to replace the SSL certificate of the SLA Mon UI with a self-signed certificate. You might want to replace the SSL certificate to meet custom security requirements.

 Note:

You can also import any client SSL certificates to the SLA Mon UI keystore. If you use such a certificate, you do not require to regenerate a self-signed certificate. If no client SSL certificates are available, use this procedure to use self-signed certificates for the SLA Mon UI.

 Note:

This procedure is for the interaction between the web browser of a user and the SLA Mon UI only and is independent of any other certificate-related procedures.

Procedure

1. Log on to the Linux host as the root user.
2. Run the following command to stop the SLA Mon UI service:

```
service slamonweb stop
```

3. Run the following commands to delete the current private-public key pair from the keystore:

```
cd /opt/avaya/slamon/misc/
```

```
keytool -delete -alias slamon -keystore slamon-ui-keystore.jks -  
storepass <keystore_password>
```

*** Note:**

Replace **<keystore_password>** with the current keystore password. Find the current password inside the `/opt/avaya/slamon/tomcat/conf/server.xml` file.

4. Run the following command to create a new self-signed private-public key pair:

```
keytool -genkey -alias slamon -keyalg RSA -keysize 2048 -keypass  
<keystore_password> -validity 365 -keystore slamon-ui-keystore.jks -  
storepass <keystore_password>
```

Where, replace **<keystore_password>** with the a password to generate the key pair. Ensure that the keypass and storepass values are the same.

5. Run the following command to generate a Certificate Signing Request (CSR) for the self-signed public certificate:

```
keytool -certreq -alias <alias_name> -file slamon.csr -keypass  
<keystore_password> -keystore slamon-ui-keystore.jks -storepass  
<keystore_password>
```

6. Run the following command to import the certificate chain signed by a certificate authority, such as VeriSign®, in response to the CSR:

```
keytool -importcert -alias <alias_name> -file  
<CA_response_cert_file> -keypass <keystore_password> -keystore  
slamon-ui-truststore.jks -storepass <keystore_password>
```

*** Note:**

Ensure that the keypass and storepass values are the same.

7. Edit the `/opt/avaya/slamon/tomcat/conf/server.xml` file, and change `keystorePass="XXXXXX"` to the password that you used to generate the key pair.
8. Run the following command to start the SLA Mon UI service:

```
service slamonweb start
```

Adding client SSL certificates to the truststore of the SLA Mon server UI

About this task

Use this procedure to add any client SSL certificates to the truststore of the SLA Mon server web interface.

*** Note:**

This procedure is for the interaction between the web browser of a user and the SLA Mon server user interface only and is independent of any other certificate-related procedures.

Procedure

1. Log on to the host server as the root user.
2. Run the following command:

```
keytool -importcert -alias <alias_name> -file  
<CA_response_cert_file> -keystore slamon-ui-truststore.jks -  
storepass <xxxxxx>
```

Where, replace <CA_response_cert_file> with the relevant certificate file name. The certificate must be an X.509 v1, v2, or v3 certificate or a PKCS#7-formatted certificate chain.

3. For the changes to take effect, run the following command to restart the web service:

```
service slamonweb restart
```

Chapter 6: Managing certificates for the communication between the server and the agent

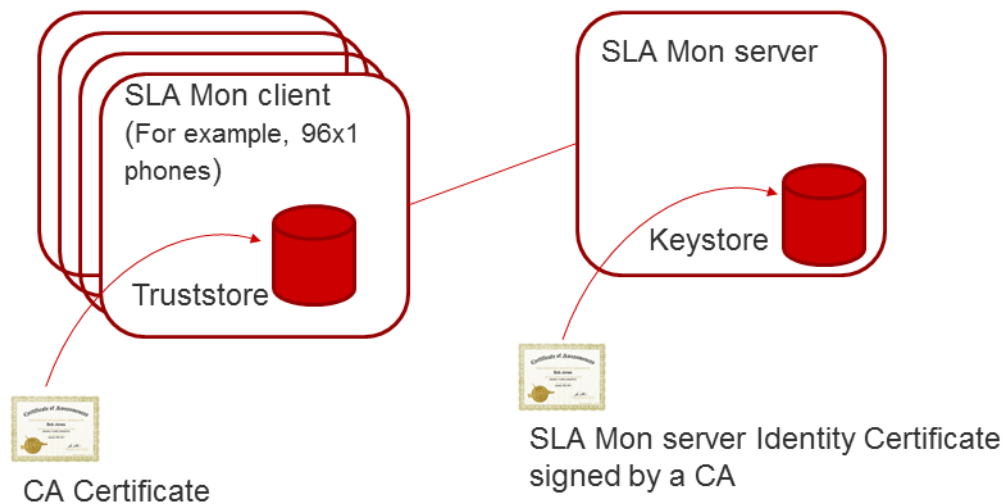
Secure communication between the server and the agent

The SLA Mon server uses digital/SSL certificates for secure communication with the agents residing in Avaya products.

During registration, the server presents its identity to the agent using a digital certificate signed by a Certificate Authority (CA). The agent uses the digital certificate to authenticate the server and register itself with the server.

The communication channel between the server and the agent is established after the certificate verification is done.

The following sample image depicts certificate usage:



Methods to obtain digital certificates

You can obtain the digital certificates by the following means:

- Certificate enrollment by a signing authority from a well-known CA, such as Symantec, Globalsign, and Verisign, or ask your in-house CA to provide you a certificate for the SLA Mon server.
- Use a self-signed certificate.
- Use the built-in Avaya demo certificate.

Based on your requirement and preference, choose one of the following options and click on the appropriate links to administer certificates on the server and the agents.

- Option 1: [Certificate enrollment by a signing authority or an in-house CA](#) on page 27
- [Prerequisite steps](#) on page 28
 - [Creating the server identity certificate on the SLA Mon server](#) on page 29
 - [Creating the CSR on the SLA Mon server](#) on page 30
 - [Installing the signed server identity certificate on the SLA Mon server](#) on page 31
 - [Installing the CA certificate on the SLA Mon agents](#) on page 32
- Option 2: [Use of a self-signed certificate](#) on page 33
- [Prerequisite steps](#) on page 33
 - [Creating a self-signed certificate authority](#) on page 35
 - [Creating the server identity certificate on the SLA Mon server](#) on page 36
 - [Creating CSR on the SLA Mon server to generate a self-signed certificate](#) on page 38
 - [Installing the self-signed server identity certificate on the SLA Mon server](#) on page 39
 - [Installing the CA certificate on the SLA Mon agents](#) on page 32
- Option 3: [Use of the Avaya demo certificate](#) on page 40
- [Installing the demo server identity certificate on the SLA Mon server](#) on page 40
 - [Installing the CA certificate on the SLA Mon agents](#) on page 32

Administering the server certificate

Certificate enrollment by a signing authority or an in-house CA

You can get the SLA Mon server identity certificate signed by any recognized certificate signing authority.

This section covers the procedures to create the server identity certificate, get the certificate signed by a signing authority, install the signed server certificate on the server, and install the CA certificate on the agents.

*** Note:**

Skip this section if you are dealing with ERS switches and Media Gateway firmware versions earlier than 35.x. ERS switches and Media Gateways earlier than 35.x do not support importing a certificate and use built-in certificates.

Prerequisite steps

Before you begin

Ensure that the keytool and the openssl commands are available on the host server console. If not, install the openssl and Java JRE packages before performing the steps.

*** Note:**

Check if the openssl package is available. Run the following command to search openssl package on the SLA Mon server console:

```
rpm -qa | grep openssl
```

If no package is found, install the latest openssl rpm.

Set the path for the commands in the PATH environment variable as the following:

```
set PATH=$PATH:$JAVA_HOME/bin
```

Note that the following procedures generate SHA256 signed certificates with a key size of 2048 bits. For more information about SHA256 support by adopting products, see [Product SHA256 and Intermediate CA support](#) on page 133.

! Important:

The 96xx H.323 Series phones with firmware versions earlier than 3.2.2 do not support SHA256 certificates. The certificate signature algorithm has to be SHA1. In the following certificate creation procedures, replace SHA256WithRSA with SHA1WithRSA and -sha256 with -sha1 for versions earlier than 3.2.2.

*** Note:**

Run the commands in the procedures from the following directory of the host server:

```
/opt/avaya/slamon/bundleconf
```

Procedure

1. Log on to the Avaya Diagnostic Server host as root, and stop the following SLA Mon services:

```
service slamonsrvr stop
```

```
service slamonweb stop
```

2. Navigate to the /opt/avaya/slamon/bundleconf directory:

```
cd /opt/avaya/slamon/bundleconf
```

3. Back up the existing `ces.jks` file.

```
mv ces.jks ces.jks.org
```

4. Administer the keystore password in the `agentcom-slamon.conf` file as the following.

The SLA Monserver is installed with a default keystore password, `avaya123`. Avaya suggests that the default password is changed to a unique password. Perform the following steps to change the password:

- a. Open the `agentcom-slamon.conf` file in a text editor, such as `vi`.

Example:

```
vi agentcom-slamon.conf
```

- b. Locate the `keyServer.keystore.password` parameter, and edit the field with a customer-specific password.

The new password you enter is the password for the keystore which contains the server certificate.

- c. Save and exit the file.

*** Note:**

If you lose your public/private key file or your password and generate a new one, your SSL certificate will no longer match. You will have to request for a new SSL certificate.

Creating the server identity certificate on the SLA Mon server

Procedure

1. Run the following command to generate an SHA256 SLA Mon server certificate:

```
keytool -genkeypair -alias slamon-keyserver -keyalg RSA -sigalg  
SHA256withRSA -keysize 2048 -validity <certificate_validity_in_days>  
-keypass <keystore_password> -storepass <keystore_password> -  
keystore ces.jks
```

Replace `<certificate_validity_in_days>` with the number of days that the certificate remains valid, and replace `<keystore_password>` with the password that you administered in step 4 of Prerequisite steps.

The command creates a server certificate in the keystore, `ces.jks`. The server uses this certificate for the communication between the server and the agent.

The command requires inputs to a number of questions for the certificate creation.

2. Enter your responses to the questions as the following:

- a. What is your first and last name?

Provide *SLA Monitor Server* as the response. The system considers this input as the common name (CN) of the server certificate. The SLA Mon server certificate *must* have this string as CN.

*** Note:**

External signing authorities mandate the CN to be the FQDN of the server and not any arbitrary name. The SLA Mon server requires the keyword *SLA Monitor Server* as the CN. Ensure that the CN is not FQDN.

The SLA Mon certificates are only used for internal communication between the server and the agent and do not provide any utility services such as HTTP, SMTP, and POP. The CN for SLA Mon is a deviation from the standard practice of providing a FQDN, which you can and must negotiate with the CA as the certificate is for internal use only.

- b. What is the name of your organizational unit?

Provide the unit name or the division name the certificate will be used for.

- c. What is the name of your organization?

Provide the registered name of the company.

- d. What is the name of your City or Locality?

Provide the full name of the city.

Example: Mountain View

- e. What is the name of your State or Province?

Provide the full name of the state.

Example: California

- f. What is the two-letter country code for this unit?

Enter the two-letter country code.

Example: US or CA

- g. Is CN=SLA Monitor Server, OU=TSD, O=AVAYA, L=Mountain View, ST=California, C=US correct?[no]

The preceding string is an example of the final question in this section.

If the output is correct and matches your earlier responses, type *yes* at the prompt, and press **Enter**. If you want to make changes, press **Enter**. The system repeats the questions with your previous answers. Correct the entries as needed.

Creating the CSR on the SLA Mon server

About this task

To generate a signed certificate, the certificate authority requires a Certificate Signing Request (CSR) containing the server certificate key pair. To generate a CSR, run the following command as explained in this procedure to create a certificate keystore and a private key.

Procedure

Run the following command to generate a CSR:

```
keytool -certreq -v -alias slamon-keyserver -keyalg RSA -sigalg
SHA256withRSA -file slamon.csr -keypass <keystore_password> -storepass
<keystore_password> -keystore ces.jks
```

Replace <keystore_password> with the password that you administered in step 4 of Prerequisite steps.

The command line option `-file slamon.csr` generates a file with the name `slamon.csr`. The `slamon.csr` file is the CSR that you need to submit to a CA to get a signed certificate.

After the CA signs the certificate, you receive a certificate chain that you need to import to the keystore, `ces.jks`, on the server. The certificate chain is a file that contains the CA root certificate and the server certificate concatenated. The certificate chain must be in the PEM/X509 format. For more information about a certificate chain, see [Identify certificate chain](#) on page 131.

*** Note:**

Ensure that the server certificate is signed by a root CA and does *not* contain any intermediate CAs. For more information about intermediate CA support by adopting products, see [Product SHA256 and Intermediate CA support](#) on page 133.

For more information about the PEM format and to verify intermediate CA, see [Viewing certificate properties](#) on page 130.

Installing the signed server identity certificate on the SLA Mon server

About this task

After you receive the signed server certificate chain from the CA, you must import the certificate chain to the keystore on the SLA Mon server.

Procedure

1. Log on to the Avaya Diagnostic Server host as root, and stop the following SLA Mon services:

```
service slamonsrvr stop
```

```
service slamonweb stop
```

2. Navigate to the `/opt/avaya/slamon/bundleconf` directory:

```
cd /opt/avaya/slamon/bundleconf
```

3. Copy the signed server certificate chain that you obtained from the CA to the SLA Mon server.

You can perform an `scp` to the `bundleconf` directory on the SLA Mon server.

4. Run the following command to import the signed server certificate chain to the server keystore:

```
keytool -importcert -v -alias slamon-keyserver -file
<signed_server_certificate_chain> -keypass <keystore_password> -
storepass <keystore_password> -keystore ces.jks
```

Replace `<keystore_password>` with the password that you administered in step 4 of Prerequisite steps.

5. When the system prompts to trust and install the certificate, type `yes`.

The command output is a signed SLA Mon server certificate in the keystore, `ces.jks`.

6. Run the following command to verify the certificate installation:

```
keytool -v -list -storepass <keystore_password> -keystore ces.jks
```

Replace `<keystore_password>` with the password that you administered in step 4 of Prerequisite steps.

The command output displays a server certificate with the alias `slamon-keyserver` and the Common Name (CN) specified during the certificate creation.

```
Keystore type: JKS
Keystore provider: SUN

Your keystore contains 1 entry

Alias name: slamon-keyserver ←
Creation date: Sep 29, 2014
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=SLA Monitor Server, OU=TSD, O=Avaya Inc., L=HR, ST=CO, C=US
Issuer: CN=SLA Monitor Server, OU=TSD, O=Avaya Inc., L=HR, ST=CO, C=US
Serial number: 4213fccb
Valid from: Mon Sep 29 08:41:40 MDT 2014 until: Sat Jun 24 08:41:40 MDT 2017
```

7. Run the following command to change the owner and the group of the keystore file to `slamonsrvr` and `eqmAdmin`:

```
chown slamonsrvr:eqmAdmin ces.jks
```

8. run the following command to change the file permissions:

```
chmod 640 ces.jks
```

9. Restart the `slamonsrvr` and the `slamonweb` services.

```
service slamonsrvr start
```

```
service slamonweb start
```

Installing the CA certificate on the SLA Mon agents

Procedure

To import the CA root certificate to the SLA Mon agents, see [Administering the CA root certificate on the SLA Mon agents](#) on page 41.

Use of a self-signed certificate

Use this section to create and use a self-signed certificate for the server-agent communication. This section covers the procedures to create a certificate authority, that is, a self-signed CA root certificate, which is used to sign the server identity certificate.

For information about getting the certificate signed by any external entity, see [Certificate enrollment by a signing authority or an in-house CA](#) on page 27.

As a security best practice, always prefer certificates signed by a recognized CA in the production environment. For guidance on the security policies of your company, contact your security team.

*** Note:**

Skip this section if you are dealing with ERS switches and Media Gateway firmware versions earlier than 35.x. ERS switches and Media Gateways earlier than 35.x do not support importing a certificate and use built-in certificates.

Prerequisite steps

Before you begin

Ensure that the `keytool` and the `openssl` commands are available on the host server console. If not, install the `openssl` and Java JRE packages before performing the steps.

*** Note:**

Check if the `openssl` package is available. Run the following command to search `openssl` package on the SLA Mon server console:

```
rpm -qa | grep openssl
```

If no package is found, install the latest `openssl` rpm.

Set the path for the commands in the `PATH` environment variable as the following:

```
set PATH=$PATH:$JAVA_HOME/bin
```

Note that the following procedures generate SHA256 signed certificates with a key size of 2048 bits. For more information about SHA256 support by adopting products, see [Product SHA256 and Intermediate CA support](#) on page 133.

! Important:

The 96xx H.323 Series phones with firmware versions earlier than 3.2.2 do not support SHA256 certificates. The certificate signature algorithm has to be SHA1. In the following certificate creation procedures, replace `SHA256WithRSA` with `SHA1WithRSA` and `-sha256` with `-sha1` for versions earlier than 3.2.2.

*** Note:**

Run the commands in the procedures from the following directory of the host server:

```
/opt/avaya/slamon/bundleconf
```

Procedure

1. Log on to the Avaya Diagnostic Server host as root, and stop the following SLA Mon services:

```
service slamonsrvr stop
```

```
service slamonweb stop
```

2. Navigate to the `/opt/avaya/slamon/bundleconf` directory:

```
cd /opt/avaya/slamon/bundleconf
```

3. Back up the existing `ces.jks` file.

```
mv ces.jks ces.jks.org
```

4. Administer the keystore password in the `agentcom-slamon.conf` file as the following.

The SLA Monserver is installed with a default keystore password, `avaya123`. Avaya suggests that the default password is changed to a unique password. Perform the following steps to change the password:

- a. Open the `agentcom-slamon.conf` file in a text editor, such as `vi`.

Example:

```
vi agentcom-slamon.conf
```

- b. Locate the `keyServer.keystore.password` parameter, and edit the field with a customer-specific password.

The new password you enter is the password for the keystore which contains the server certificate.

- c. Save and exit the file.

Note:

If you lose your public/private key file or your password and generate a new one, your SSL certificate will no longer match. You will have to request for a new SSL certificate.

5. Edit the `openssl.cnf` configuration file as the following:

- a. Open the file in a text editor, such as `vi`.

Example:

```
vi /etc/pki/tls/openssl.cnf
```

- b. In the file, ensure that the `x509_extensions` parameter for self-signed certificates is uncommented:

```
x509_extensions = v3_ca
```

- c. Under the `[v3_ca]` section in the file, set the following entries as displayed, and ensure that the lines are uncommented:

```
basicConstraints = CA:true
```

Where, the entry must be true.

```
keyUsage = cRLSign, keyCertSign
```

Where, check whether the extension `keyCertSign` is present.

Sample configuration information in the file:

```
[ v3_ca ]

# Extensions for a typical CA

# PKIX recommendation.

subjectKeyIdentifier=hash

authorityKeyIdentifier=keyid:always,issuer

# This is what PKIX recommends but some broken software chokes on critical
# extensions.
#basicConstraints = critical,CA:true
# So we do this instead.
basicConstraints = CA:true

# Key usage: this is typical for a CA certificate. However since it will
# prevent it being used as an test self-signed certificate it is best
# left out by default.
keyUsage = cRLSign, keyCertSign
```

Creating a self-signed certificate authority

Procedure

1. Create a `certs` directory in the `/opt/avaya/slamon/bundleconf` directory:

```
mkdir /opt/avaya/slamon/bundleconf/certs
```

2. Navigate to the new `certs` directory:

```
cd /opt/avaya/slamon/bundleconf/certs
```

3. Run the following command to generate the root CA private key:

```
openssl genrsa -out privKey.pem 2048
```

This command creates the signing authority private key. Ensure the safety of these keys. The output of the command is the `privKey.pem` file.

4. Run the following command to generate a root CA public key:

```
openssl req -new -x509 -key privKey.pem -out rootCA.pem -days <days> -sha256
```

Replace `<days>` with the number of days the certificate remains valid.

The command requires user inputs for some information that the command uses for the certificate creation. The responses that you enter forms a Common Name (CN).

Enter your responses for the following fields. Enter a period (.) to leave a field blank, or press **Enter** to accept the default values:

- a. Country Name (2 letter code) [XX]
Enter the two-letter country code.
Example: US or CA
- b. State or Province Name (full name) []
Enter the name of your state or province.
Example: California
- c. Locality Name (eg, city) [Default City]
Enter the name of your city or locality.
Example: Mountain View
- d. Organization Name (eg, company) [Default Company Ltd]
Enter the name of your organization.
Example: Avaya Inc.
- e. Organizational Unit Name (eg, section) []
Enter your organization unit or the section name.
Example: Customer Support
- f. Common Name (eg, your name or your server's hostname) []
Enter the host name of the server or your name.
Example: linpu005.abc.avaya.com
- g. Email Address []
Enter your email address.
Example: ads@support.com

This command creates the CA root certificate. The Public and Private Key are used to sign the server certificate. The output of the step is the `rootCA.pem` file.

Creating the server identity certificate on the SLA Mon server

Procedure

1. Run the following command to generate an SHA256 SLA Mon server certificate:

```
keytool -genkeypair -alias slamon-keyserver -keyalg RSA -sigalg  
SHA256withRSA -keysize 2048 -validity <certificate_validity_in_days>  
-keypass <keystore_password> -storepass <keystore_password> -  
keystore ces.jks
```

Replace `<certificate_validity_in_days>` with the number of days that the certificate remains valid, and replace `<keystore_password>` with the password that you administered in step 4 of Prerequisite steps.

The command creates a server certificate in the keystore, `ces.jks`. The server uses this certificate for the communication between the server and the agent.

The command requires inputs to a number of questions for the certificate creation.

2. Enter your responses to the questions as the following:

- a. What is your first and last name?

Provide *SLA Monitor Server* as the response. The system considers this input as the common name (CN) of the server certificate. The SLA Mon server certificate *must* have this string as CN.

*** Note:**

External signing authorities mandate the CN to be the FQDN of the server and not any arbitrary name. The SLA Mon server requires the keyword *SLA Monitor Server* as the CN. Ensure that the CN is not FQDN.

The SLA Mon certificates are only used for internal communication between the server and the agent and do not provide any utility services such as HTTP, SMTP, and POP. The CN for SLA Mon is a deviation from the standard practice of providing a FQDN, which you can and must negotiate with the CA as the certificate is for internal use only.

- b. What is the name of your organizational unit?

Provide the unit name or the division name the certificate will be used for.

- c. What is the name of your organization?

Provide the registered name of the company.

- d. What is the name of your City or Locality?

Provide the full name of the city.

Example: Mountain View

- e. What is the name of your State or Province?

Provide the full name of the state.

Example: California

- f. What is the two-letter country code for this unit?

Enter the two-letter country code.

Example: US or CA

- g. Is CN=SLA Monitor Server, OU=TSD, O=AVAYA, L=Mountain View, ST=California, C=US correct?[no]

The preceding string is an example of the final question in this section.

If the output is correct and matches your earlier responses, type **yes** at the prompt, and press **Enter**. If you want to make changes, press **Enter**. The system repeats the questions with your previous answers. Correct the entries as needed.

3. Run the following command to verify the certificate creation:

```
keytool -v -list -storepass <keystore_password> -keystore ces.jks
```

Replace <keystore_password> with the password that you administered in step 4 of Prerequisite steps.

The output of this command shows a server certificate with the alias `slamon-keyserver` and the Common Name (CN) specified during the certificate creation.

Creating CSR on the SLA Mon server to generate a self-signed certificate

About this task

To generate a self-signed certificate, the certificate authority requires a Certificate Signing Request (CSR) containing the server certificate key pair. To generate a CSR, run the following commands in the procedure to create a certificate keystore and a private key.

Procedure

1. Run the following command to generate a CSR:

```
keytool -certreq -v -alias slamon-keyserver -keyalg RSA -sigalg  
SHA256withRSA -file slamon.csr -keypass <keystore_password> -  
storepass <keystore_password> -keystore ces.jks
```

Replace <keystore_password> with the password that you administered in step 4 of Prerequisite steps.

The command line option `-file slamon.csr` generates a file with the name `slamon.csr`. The `slamon.csr` file is the CSR that has to be signed using the CA root certificate created in steps 3 and 4 of [Creating a self-signed certificate authority](#) on page 35.

2. Run the following command to sign the CSR:

```
openssl x509 -req -days <days> -in slamon.csr -CA rootCA.pem -CAkey  
privKey.pem -set_serial 01 -out slamon.cer -sha256
```

Replace <days> with the number of days the certificate remains valid.

The CSR is signed by the signing authority created in steps 3 and 4 of [Creating a self-signed certificate authority](#) on page 35. The command output is the `slamon.cer` file, which contains the signed server certificate.

3. Run the following command to verify the certificate created:

```
openssl x509 -in slamon.cer -text
```

The output is a signed server certificate. Check if the subject has the string `SLA Monitor Server` and the issuer is the issuer created in step 4 of [Creating a self-signed certificate authority](#) on page 35.

Installing the self-signed server identity certificate on the SLA Mon server

Procedure

1. Run the following command to create a certificate chain:

```
cat slamon.cer rootCA.pem > slamon.chain
```

The command creates a certificate chain that consists of the signed server certificate and the CA root certificate used to sign the certificate.

2. Run the following command to import the certificate chain to the SLA Mon server keystore:

```
keytool -importcert -v -alias slamon-keyserver -file slamon.chain -  
keypass <keystore_password> -storepass <keystore_password> -keystore  
ces.jks
```

Replace `<keystore_password>` with the password that you administered in step 4 of Prerequisite steps.

When the system prompts to trust and install the certificate, type `yes`.

The command output is a signed SLA Mon server certificate in the keystore, `ces.jks`.

3. Run the following command to verify the certificate installation:

```
keytool -v -list -keystore ces.jks -storepass <keystore_password>
```

Replace `<keystore_password>` with the password that you administered in step 4 of Prerequisite steps.

The output is a signed server certificate. Ensure that the entry for the alias `slamon-keyserver` has the owner as `CN=SLA Monitor Server` and the issuer is the CA used to sign the certificate.

Sample output:

```
Keystore type: JKS
Keystore provider: SUN

Your keystore contains 1 entry

Alias name: slamon-keyserver ←
Creation date: Sep 29, 2014
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=SLA Monitor Server, OU=TSD, O=Avaya Inc., L=HR, ST=CO, C=US
Issuer: CN=SLA Monitor Server, OU=TSD, O=Avaya Inc., L=HR, ST=CO, C=US
Serial number: 4213fccb
Valid from: Mon Sep 29 08:41:40 MDT 2014 until: Sat Jun 24 08:41:40 MDT 2017
```

4. Copy the keystore file, `ces.jks`, to `/opt/avaya/slamon/bundleconf`:

```
cp ces.jks /opt/avaya/slamon/bundleconf
```

5. Ensure that the keystore file owner is `slamonsrvr` and the group is `eqmAdmin`. If not, then change the ownership.

```
chown slamonsrvr:eqmAdmin /opt/avaya/slamon/bundleconf/ces.jks
```

6. Ensure that the file has read permissions.

```
chmod 640 /opt/avaya/slamon/bundleconf/ces.jks
```

7. Restart the `slamonsrvr` and `slamonweb` services.

```
service slamonsrvr start
```

```
service slamonweb start
```

Installing the CA certificate on the SLA Mon agents

Procedure

To import the CA root certificate to the SLA Mon agents, see [Administering the CA root certificate on the SLA Mon agents](#) on page 41.

Use of the Avaya demo certificate

This section covers the procedures to use the demo certificate shipped with Avaya Diagnostic Server 2.0.

Important:

As a security best practice, always prefer certificates signed by a recognized CA in the production environment. For guidance on the security policies of your company, contact your security team.

Installing the demo server identity certificate on the SLA Mon server

Procedure

1. Log on to the Avaya Diagnostic Server host as root.
2. Open a console on the host, and run the following command to install the demo certificate that Avaya ships with the software package:

```
/opt/avaya/slamon/bin/installdemocert
```

The system displays a warning message about installing the demo certificate on the server.

3. Read the certificate warning message, and type `yes` to install the demo certificate.

If you type `no`, the system stops the certificate installation process.

4. Restart the `slamonsrvr` and `slamonweb` services.

```
service slamonsrvr restart
```

```
service slamonweb restart
```

Installing the CA certificate on the SLA Mon agents

Procedure

To import the CA root certificate to the SLA Mon agents, see [Administering the CA root certificate on the SLA Mon agents](#) on page 41.

Administering the CA root certificate on the SLA Mon agents

The SLA Mon agent is shipped with 96xx and 96x1 Series phones, G450 and G430 Branch Gateways, ERS and VSP Switches. For the communication with the SLA Mon server, the agent needs to import the CA root certificate that signed the SLA Mon server certificate.

Procedure

To administer the CA root certificate on the SLA Mon agent of the adopting product, click on the appropriate link from the following:

- [The CA root certificate administration on 96x0 and 96x1 series IP deskphones](#) on page 41
- [The CA root certificate administration on G450 and G430 Media Gateways](#) on page 47
- [The CA root certificate administration on VSP switches](#) on page 50

For information about certificate management on the server, see [Administering the server certificate](#) on page 27.

The CA root certificate administration on 96x0 and 96x1 series IP deskphones

The SLA Mon agent on an endpoint requires the CA root certificate to authenticate the server during the registration. If a certificate mismatch occurs, the registration is rejected. Perform the steps listed in the following procedures to import the CA root certificate on an endpoint.

Installing a CA root certificate obtained from a signing authority or in-house CA

About this task

Use this procedure to import the CA root certificate to an endpoint when the server certificate is obtained from a signing authority by following the steps in the *Certificate enrollment by a signing authority or in-house CA* section.

Procedure

1. Run the following command to get the CA root certificate from the SLA Mon server.

```
openssl s_client -host <SLA Mon Server IP> -port 50011 -showcerts
```

2. From the command output, copy the last block of text with BEGIN CERTIFICATE and END CERTIFICATE, and paste the text in a file.

For more information on the block of text to be copied, see [Copying the CA root certificate installed on the SLA Mon server](#) on page 132.

3. Copy the file containing the block of text from the command output to the phone HTTP or HTTPS server download directory in the same location as the phone firmware.
4. Check the HTTP or HTTPS server IP on the phone using the CRAFT procedure.

To perform the CRAFT procedure on a phone, press **Mute**, followed by 27238, and then press **#**. For more information, see Avaya IP Phone administration guides on <http://support.avaya.com/>.

5. In the 46xxsettings.txt file on the phone HTTP or HTTPS server, set the TRUSTCERTS parameter as the following:

- If the parameter is null or not set:

```
SET TRUSTCERTS <ca_root_certificate>
```

- If the parameter is populated with other certificates, retain the existing certificates and *put the SLA Mon CA root certificate as the first one in the list.*

Ensure that the certificates mentioned in TRUSTCERTS are all present in the path or remove the certificate from the list. Else, the certificate download to the phone fails.

```
SET TRUSTCERTS
```

```
"<ca_root_certificate>,av_csca_pem_2032.txt,<other_certificates_if_any>"
```

Important:

For SIP telephones, if TRUSTCERTS is not set or null, ensure that the file av_sipca_pem_2027.txt is included in the HTTP or HTTPS file server directory and the file name is set in the SET TRUSTCERTS option. Else, the SIP over TLS communication with the Avaya Session Manager using the default Avaya SIP root CA certificate will not be established and users will not be able to log in. Note that Avaya no longer recommends using Avaya SIP root CA certificates for SIP/TLS signaling. Avaya recommends customers to build their own PKI and install their own certificates on Avaya Session Manager or SIP phones.

```
SET TRUSTCERTS
```

```
"<ca_root_certificate>,av_sipca_pem_2027.txt,<other_certificates_if_any>"
```

6. Reboot the phone.

The certificate gets downloaded to the phone truststore on reboot.

Installing the CA root certificate created using a self-signed certificate authority

About this task

Use this procedure to import the CA root certificate to an endpoint if the server certificate is a self-signed certificate as mentioned in the *Use of a self-signed certificate* section.

Procedure

1. Copy the root certificate, `rootCA.pem`, that you created in step 4 of [Creating a self-signed certificate authority](#) on page 35 to the phone HTTP or HTTPS server download directory in the same location as the phone firmware.

For more information on the phone settings, see Avaya IP Phone administration guides on <http://support.avaya.com/>.

2. Check the HTTP or HTTPS server IP on the phone using the CRAFT procedure.

To perform the CRAFT procedure on a phone, press **Mute**, followed by 27238, and then press **#**. For more information, see Avaya IP Phone administration guides on <http://support.avaya.com/>.

3. In the `46xxsettings.txt` file on the HTTP or HTTPS server, set the TRUSTCERTS parameter with the CA root certificate name as the following:

- If the parameter is null or not set:

```
SET TRUSTCERTS rootCA.pem
```

- If the parameter is populated with other certificates, retain the existing certificates and *put the SLA Mon CA root certificate as the first one in the list*.

```
SET TRUSTCERTS
```

```
"rootCA.pem,av_csca_pem_2032.txt,<other_certificates_if_any>"
```

! Important:

For SIP telephones, if TRUSTCERTS is not set or null, ensure that the file `av_sipca_pem_2027.txt` is included in the HTTP or HTTPS file server directory and the file name is set in the SET TRUSTCERTS option. Else, the SIP over TLS communication with the Avaya Session Manager using the default Avaya SIP root CA certificate will not be established and users will not be able to log in. Note that Avaya no longer recommends using Avaya SIP root CA certificates for SIP/TLS signaling. Avaya recommends customers to build their own PKI and install their own certificates on Avaya Session Manager or SIP phones.

```
SET TRUSTCERTS
```

```
"rootCA.pem,av_sipca_pem_2027.txt,<other_certificates_if_any>"
```

4. Reboot the phone.

The certificate gets downloaded to the phone truststore on reboot.

Installing the CA root certificate for the Avaya demo certificate

About this task

Use this procedure if the installed server certificate is the Avaya demo certificate as mentioned in the *Use of Avaya demo certificate* section.

Procedure

1. Copy the demo CA root certificate, `slamonRootCA.crt`, from the SLA Mon server location `/opt/avaya/slamon/bundleconf/` to the phone HTTP or HTTPS server download directory in the same location as the phone firmware.

For more information on the phone settings, see Avaya IP Phone administration guides on <http://support.avaya.com/>.

2. Check the HTTP or HTTPS server IP on the phone using the CRAFT procedure.

To perform the CRAFT procedure on a phone, press **Mute**, followed by 27238, and then press **#**. For more information, see Avaya IP Phone administration guides on <http://support.avaya.com/>.

3. In the `46xxsettings.txt` file on the HTTP or HTTPS server, set the TRUSTCERTS parameter as the following:

- If the parameter is null or not set:

```
SET TRUSTCERTS slamonRootCA.crt
```

- If the parameter is populated with other certificates, retain the existing certificates and *put the SLA Mon CA root certificate as the first one in the list*.

```
SET TRUSTCERTS
"slamonRootCA.crt,av_csca_pem_2032.txt,<other_certificates_if_any>"
```

! Important:

For SIP telephones, if TRUSTCERTS is not set or null, ensure that the file `av_sipca_pem_2027.txt` is included in the HTTP or HTTPS file server directory and the file name is set in the SET TRUSTCERTS option. Else, the SIP over TLS communication with the Avaya Session Manager using the default Avaya SIP root CA certificate will not be established and users will not be able to log in. Note that Avaya no longer recommends using Avaya SIP root CA certificates for SIP/TLS signaling. Avaya recommends customers to build their own PKI and install their own certificates on Avaya Session Manager or SIP phones.

```
SET TRUSTCERTS
"slamonRootCA.crt,av_sipca_pem_2027.txt,<other_certificates_if_any>"
```

4. Reboot the phone.

The certificate gets downloaded to the phone truststore on reboot.

SLA Mon agent parameters in the endpoints settings file

The SLA Mon agent is downloaded automatically on the Avaya endpoints. By default, the agent remains in a disabled state. To utilize the SLA Mon features on the endpoints, you must configure certain parameters in the endpoints settings file, `46xxsettings.txt`, on the HTTP or HTTPS server to which the endpoints point.

The following table provides the details of the parameters that you can set in the `46xxsettings.txt` file to enable the SLA Mon features on an endpoint.

Parameter	Default value	Description
SLMSTAT	0	The SLA Mon agent control flag to enable or disable the agent on the endpoint. When you enable the agent, the SLA Mon server can involve the agent in network monitoring. Valid values: • 0: To disable the agent. • 1: To enable the agent. To enable other diagnostic features on the endpoint, you must set additional parameters mentioned in this table.
SLMCAP	0	The SLA Mon agent flag to enable or disable packet capture on phones. Valid values: • 0: To disable capture of packets. • 2: To enable capture of packets including VoIP payloads.  Note: The SLA Mon server does not support SLMCAP value 1. Therefore, set SLMCAP to 2 to enable packet capture on the phone.
SLMPERF	0	The SLA Mon agent flag to enable or disable event monitoring, including button and touch events, on phones. Valid values: • 0: To disable phone event monitoring. • 1: To enable phone event monitoring.  Note: Setting SLMPERF to 1 has privacy implications.
SLMCTRL	0	The SLA Mon agent flag to enable or disable the phone remote control feature. Valid values: • 0: To disable phone remote control. • 1: To enable phone remote control.  Note: Setting SLMCTRL to 1 has privacy implications.
SLMPORT	50011	The SLA Mon agent control port to receive agent discovery and test requests. Valid values are from 6000 to 65535.

Parameter	Default value	Description
		If you change the default port in the settings file, you must also change the port number on the SLA Mon server. Change the following port values in the <code>/opt/avaya/slamon/bundleconf/agentcom-slamon.conf</code> file on the SLA Mon server host: <pre>SLMSERVER #keyServer.port=50011 SLMPORT # The UDP port on agents where commands are received. # agent.command.port=50011</pre> After the configuration changes, restart the SLA Mon services.
SLMTEST	50012	The SLA Mon agent test ports for RTP and traceroute tests. The agent uses port 50012 for RTP tests, and port 50013 for traceroute tests.  Important: Do not change the default port value of 50012.
SLMSRVR		Specifies the IP address and the port number of the SLA Mon server in the <code>aaa.bbb.ccc.ddd:n</code> format. Set the IP address of the SLA Mon server in the <code>aaa.bbb.ccc.ddd</code> format to restrict the registration of agents only to that server. Specifying a port number is optional. If you do not specify a port number, the system takes 50011 as the default port. The IP address must be in the dotted decimal format, optionally followed by a colon and an integer port number from 0 to 65535. To use a nondefault port <code>n</code>, set the value of SLMSRVR in the <code>aaa.bbb.ccc.ddd:n</code> format, where <code>aaa.bbb.ccc.ddd</code> is the IP address of the SLA Mon server. Also, change the following port number in the <code>/opt/avaya/slamon/bundleconf/agentcom-slamon.conf</code> file on the SLA Mon server. <pre>SLMSERVER #keyServer.port=n</pre> After the configuration changes, restart the SLA Mon services.
TRUSTCERTS		• A comma-separated list of certificates that the endpoint uses. • If this parameter is set, the endpoint accepts to register only with the SLA Mon server that presents a certificate that matches one of the certificates in the list. • To use the SLA Mon features on the phone, you must enter a certificate issued by a Certificate Authority (CA). Avaya Diagnostic Server also supports third-party certificates. If you choose to use Avaya SIP Root CA, Avaya Diagnostic Server continues to support this demo certificate. • You must enter the Avaya Diagnostic Server certificate as the first entry in the TRUSTCERTS parameter. Also verify that all other listed certificates

Parameter	Default value	Description
		are available for downloading to the phone. If any certificate is unavailable, comment out the original line and create a new SET TRUSTCERTS entry with the appropriate certificates in the new entry. The list can contain up to 255 characters. Values in the list are separated by commas without intervening spaces. Example configuration of the TRUSTCERTS parameter in the <code>46xxsettings.txt</code> file: <pre>SET TRUSTCERTS rootCA.pem,rootCertRNAAD.cer</pre>

*** Note:**

For information about other parameters in the settings file, see the respective documentation on Avaya endpoints.

*** Note:**

The specified initial values are used when no value is in the flash memory of an endpoint. When the endpoint starts, the endpoint retrieves the `46xxsettings.txt` file and writes the values configured in the file to the flash memory of the endpoint. To disable the agent or to disable a feature, only removal of the lines from the `46xxsettings.txt` file is not adequate. Even after the removal of the lines from the settings file, the endpoint continues to use the flash memory that still has the earlier values. To disable the agent or a feature, you must restart the endpoint after you make the required changes in the file.

The CA root certificate administration on G450 and G430 Media Gateways

The SLA Mon agent on a Media Gateway requires the CA root certificate to authenticate the server during the registration. If a certificate mismatch occurs, the registration is rejected. Perform the steps listed in the procedures to import the CA root certificate on Media Gateways.

*** Note:**

The procedures are applicable only for the Media Gateway firmware version 36.x and later.

Installing a CA root certificate obtained from a signing authority or in-house CA

About this task

Use this procedure to import the CA root certificate to Media Gateway when the server certificate is obtained from a signing authority by following the steps in the *Certificate enrollment by a signing authority or in-house CA* section.

Procedure

1. Run the following command to get the CA root certificate from the SLA Mon server.

```
openssl s_client -host <SLA Mon Server IP> -port 50011 -showcerts
```

2. From the command output, copy the last block of text with BEGIN CERTIFICATE and END CERTIFICATE, and paste the text in a file.

For more information on the block of text to be copied, see [Copying the CA root certificate installed on the SLA Mon server](#) on page 132.

3. Save the file containing the block of text from the command output in the /tmp directory on the SLA Mon server.
4. Log on to the Media Gateway CLI.
5. Run the following copy command to download the CA root certificate to Media Gateway:

```
copy scp root-ca sla /tmp/<ca_root_certificate_filename> <SLA Mon Server IP>
```

When the system prompts, provide a valid user name and password of the SLA Mon server.

6. Run the following command to view the copied certificate:

```
show root-ca sla
```

7. Run the following command to erase any existing certificate:

```
erase root-ca sla <index>
```

Replace <index> with the file index that the **show root-ca** command displays for the unwanted certificate.

8. Run the following command to enable the SLA Mon agent:

```
set sla-monitor enable
```

9. Run the following command to check whether the agent is enabled:

```
show sla-monitor
```

The output must display the SLA Mon operational mode as *Enabled*.

Installing the CA root certificate created using a self-signed certificate authority

About this task

Use this procedure to import the CA certificate to a G450 or G430 Media Gateway if the server certificate is a self-signed certificate as mentioned in the *Use of a self-signed certificate* section.

Procedure

1. On to the SLA Mon server host, open a console.
2. Copy the root certificate, `rootCA.pem`, that you created in step 4 of [Creating a self-signed certificate authority](#) on page 35 to the /tmp directory on the server.

```
cp /opt/avaya/slamon/bundleconf/certs/rootCA.pem /tmp/rootCA.pem
```

Ensure that the certificate has read permissions.

3. Log on to the Media Gateway CLI.
4. Run the following copy command to download the CA root certificate, `rootCA.pem`, to Media Gateway:

```
copy scp root-ca sla /tmp/rootCA.pem <SLA Mon Server IP>
```

When the system prompts, provide a valid user name and password of the SLA Mon server.

5. Run the following command to view the copied certificate:

```
show root-ca sla
```

6. Run the following command to erase any existing certificate:

```
erase root-ca sla <index>
```

Replace <index> with the file index that the `show root-ca` command displays for the unwanted certificate.

7. Run the following command to enable the SLA Mon agent:

```
set sla-monitor enable
```

8. Run the following command to check whether the agent is enabled:

```
show sla-monitor
```

The output must display the SLA Mon operational mode as `Enabled`.

Installing the CA root certificate for the Avaya demo certificate

About this task

Use this procedure if the installed server certificate is the Avaya demo certificate as mentioned in the *Use of Avaya demo certificate* section.

Procedure

1. Log on to the Media Gateway CLI.
2. Run the following copy command to download the CA root certificate `slamonRootCA.crt` to Media Gateway:

```
copy scp root-ca sla /opt/avaya/slamon/bundleconf/slamonRootCA.crt  
<SLA Mon Server IP>
```

When the system prompts, provide a valid user name and password of the SLA Mon server.

3. Run the following command to view the copied certificate:

```
show root-ca sla
```

4. Run the following command to erase any existing certificate:

```
erase root-ca sla <index>
```

Replace <index> with the file index that the `show root-ca` command displays for the unwanted certificate.

5. Run the following command to enable the SLA Mon agent:

```
set sla-monitor enable
```

6. Run the following command to check whether the agent is enabled:

```
show sla-monitor
```

The output must display the SLA Mon operational mode as `Enabled`.

The CA root certificate administration on VSP switches

The SLA Mon agent on a VSP switch requires the CA root certificate to authenticate the server during the registration. If a certificate mismatch occurs, the registration is rejected. Perform the steps listed in the procedures to import the CA root certificate to VSP switches.

Important:

Perform the steps in the procedures on the VSP console.

Installing a CA root certificate obtained from a signing authority or in-house CA

About this task

Use this procedure to import the CA root certificate to a VSP switch when the server certificate is obtained from a signing authority by following the steps in the *Certificate enrollment by a signing authority or in-house CA* section.

Procedure

1. Log on to the VSP console as an administrative user.
2. Ensure that FTP is enabled on the VSP switch, and perform the following steps to copy the CA root certificate from the SLA Mon server to the VSP switch.
3. Run the following command to get the CA root certificate from the SLA Mon server.

```
openssl s_client -host <SLA Mon Server IP> -port 50011 -showcerts
```

4. From the command output, copy the last block of text with BEGIN CERTIFICATE and END CERTIFICATE, and paste the text in a file.

For more information on the block of text to be copied, see [Copying the CA root certificate installed on the SLA Mon server](#) on page 132.

5. Copy the file containing the block of certificate text from the SLA Mon server to any server that has the `ftp` command.
6. Run the following command from the server where you copied the certificate to connect to the switch through FTP:

```
ftp <ip_address_of_vsp_switch>
```

At the FTP prompt, type `bin`.

7. Run the **put** command to transfer the certificate:

```
put <path_to_ca_root_certificate> <path_to_copy_certificate>
```

For example:

```
put /tmp/root_certificate /tmp/rootcert.pem
```

8. After a successful transfer, run the following command to end the FTP session:

```
bye
```

9. On the VSP console, run the following command to install the certificate:

```
slamon install-cert-file <path_to_copied_root_certificate>
```

For example:

```
slamon install-cert-file /tmp/rootcert.pem
```

Installing the CA root certificate created using a self-signed certificate authority

About this task

Use this procedure to import the CA root certificate to a VSP switch if the server certificate is a self-signed certificate as mentioned in the *Use of a self-signed certificate* section.

Procedure

1. Log on to the VSP console as an administrative user.
2. Ensure that FTP is enabled on the VSP switch, and perform the following steps to copy the CA root certificate from the SLA Mon server to the VSP switch.
3. Download the CA root certificate, `rootCA.pem`, that you created in step 4 of [Creating a self-signed certificate authority](#) on page 35 from the SLA Mon server to any server that has the **ftp** command.
4. Run the following command from the server where you copied the certificate to connect to the switch through FTP:

```
ftp <ip_address_of_vsp_switch>
```

At the FTP prompt, type `bin`.

5. Run the **put** command to transfer the certificate:

```
put rootCA.pem /tmp/rootCA.pem
```

6. After a successful transfer, run the following command to end the FTP session:

```
bye
```

7. On the VSP console, run the following command to install the certificate:

```
slamon install-cert-file /tmp/rootCA.pem
```

Installing the CA root certificate for the Avaya demo certificate

About this task

Use this procedure to import the CA root certificate to a VSP switch if the server certificate is a Avaya demo certificate as mentioned in the *Use of the Avaya demo certificate* section.

Procedure

1. Log on to the VSP console as an administrative user.
2. Ensure that FTP is enabled on the VSP switch, and perform the following steps to copy the CA root certificate from the SLA Mon server to the VSP switch.
3. Download the CA root certificate, `slamonRootCA.crt`, from the SLA Mon server to any server that has the `ftp` command.
4. Run the following command from the server where you copied the certificate to connect to the switch through FTP:

```
ftp <ip_address_of_vsp_switch>
```

At the FTP prompt, type `bin`.

5. Run the `put` command to transfer the certificate:

```
put slamonRootCA.crt /tmp/slamonRootCA.crt
```

6. After a successful transfer, run the following command to end the FTP session:

```
bye
```

7. On the VSP console, run the following command to install the certificate:

```
slamon install-cert-file /tmp/slamonRootCA.crt
```

Enabling the SLA Mon agent on the VSP and ERS switches

About this task

For the VSP and ERS switches to respond to the requests from the SLA Mon server, you must enable the SLA Mon agent on the switches. Use this procedure to enable and configure the SLA Mon agent on a VSP or ERS switch.

* Note:

Run the commands in the procedure on the device console.

Procedure

1. Log on to the switch through a Telnet connection with the valid credentials of an administrative user.

```
telnet <switch_ip_address>
```

2. Run the following command to check the application status of the agent:

```
show application slamon agent
```

3. Perform the following to enter the application configuration for configuring the agent:

- a. Run the following command to enable configuration:

enable

- b. Run the following command to enter the configuration mode:

configure terminal

- c. Run the following command to enter the application configuration mode:

application

The SLA Mon agent runs as an application on the ERS and VSP switches. Therefore, you must run the SLA Mon agent specific commands from the application mode.

4. Run the following command to enable the SLA Mon agent on the switch:

slamon oper-mode enable

5. Run the following command to disable the SLA Mon agent on the switch:

no slamon oper-mode

6. Run the following command to configure the agent IP address:

slamon agent ip address <A.B.C.D>

Replace <A.B.C.D> with the IP address that you want to configure for the agent.

 Note:

The agent automatically acquires the device address. Run the command only to use a different IP address than the automatically acquired agent address.

7. Run the following command to configure the SLA Mon server IP address on the switch:

slamon server ip address <A.B.C.D>

Replace <A.B.C.D> with the SLA Mon server IP address.

Chapter 7: Initial administration

Initial administration

After you implement the SLA Mon server, you must discover the test agents residing in adopting Avaya products on your network. After you discover the agents and the agents register themselves with the SLA Mon server, you can use the SLA Mon features for controlling and monitoring Avaya endpoints.

You can administer the SLA Mon server through the SLA Mon web interface and through the command line interface (CLI) of the server. This chapter covers administration of the SLA Mon server through the web interface. For information about CLI-based administration, see Chapter 8, Administering SLA Mon Server through CLI.

Important:

The SLA Mon web interface is unavailable on Services-VM. You must use the SLA Mon CLI to perform all tasks for SLA Mon on Services-VM.

Logging on to the SLA Mon web interface

About this task

Use this procedure to log on to the SLA Mon web interface.

Procedure

1. In your web browser, type the URL of the SLA Mon web interface as the following:

```
https://<hostname or IP address of Avaya Diagnostic Server>:4511/  
slamon
```

2. On the login page, enter the credentials of an administrator user, and click **Login**.

The system displays the SLA Mon web interface with the navigation menu options for endpoint diagnostics and network monitoring.

Note:

For the actions you perform on a web page of the SLA Mon web interface, the system displays the status of the action at the top of the particular page, just below the

navigation menu. For any successful operation, the status message is displayed in green. In case of errors, the message is displayed in red.

Administering SLA Mon agents on the SAL Mon server

Discovering SLA Mon agents

About this task

Use this procedure to discover the SLA Mon agents present in a location or subnet address range and register the agents with the SLA Mon server. The SLA Mon agent that resides in an endpoint becomes active only when the SLA Mon server discovers the agent.

Procedure

1. Log on to the SLA Mon web interface as an administrator.
2. Click the **DISCOVERY** tab.
3. On the Agent Discovery page, complete the following fields to add the address range of a subnet:

- **Country**
- **State**
- **City**
- **Range To Add**

Specify the address range in the network/CIDR format, for example, 111.234.222.123/22.

Note:

Here, '/22' means that the mask has 22 bits. The mask would be 11111111.11111111.11111100.00000000, that is 255.255.252.000, which means that the server can discover a maximum of 1024 agents with the use of the mask.

- **Zone**

If you do not want to add the subnet to a zone, you must enter **NO ZONE**.

4. Click **Add/Update**.

The system adds the subnet to the table in the Agent Discovery section.

5. Repeat steps 3 to 4 to add more subnets to the list.
6. From the list of subnets, select one or more subnets, and click **Run Discovery**.

The system searches for test agents present on the selected subnets and displays the discovered agents in the Discovered Test Agents table.

When the SLA Mon server discovers a test agent, the server automatically registers that agent.

7. To stop an agent discovery process that is in progress, click **Stop Discovery**.
8. If you want to remove a subnet, select the appropriate row, and click **Remove**.

The system removes the selected subnet.

Agent Discovery field and icon descriptions

Using the Agent Discovery page, you can discover SLA Mon agents in a particular location or address range. You can add and update the search criteria for discovering agents. The Agent discovery page also displays the discovered agents and the respective router details.

The field and icon descriptions for the Agent Discovery page is as follows:

Name	Description
Add Address Range section	
Country	The country in which you want to discover the SLA Mon agents.
State	A drop-down list box to select the state in which you want to discover the SLA Mon agents.
City	A drop-down list box to select the city in which you want to discover the SLA Mon agents.
Range To Add	An input field to enter the subnet address range in which you want to discover the SLA Mon agents. Specify the address range in the network/CIDR format, for example, 111.234.222.123/22.  Note: Here, '/22' means hat the mask has 22 bits. The mask would be 11111111.11111111.11111100.00000000 , that is 255.255.252.000, which means that the server can discover a maximum of 1024 agents with the use of the mask.
Zone	An input field to enter a zone under which you want to place the subnet. When you type the first few letters of a zone name, the system displays the available zone names that start with the letters. You can select from the suggested zones. You must enter a value in this field. If you do not want the subnet to belong to a particular zone, you must select NO ZONE.

Name	Description
Agent Discovery section	
Select	A check box to select the subnet for discovering agents.
Subnet	The subnet address range where you want to discover test agents.
Country	The country in which the subnet address is located.
State Province	The state province of the subnet.
City	The city where the subnet address is located.
Zone	The zone where you added the subnet.
Discovered Test Agents	
Address	The IP address of the discovered agent.
Router	The router details of the discovered agent.

Button	Description
Add/Update	Adds or updates the details of the subnet where you want to discover agents.
Clear	Clears the subnet details you enter.

Icon	Name	Description
	Run Discovery	Runs the agent discovery command and displays the discovered agents for the given address range.
	Stop Discovery	Stops an active agent discovery process.
	Remove	Removes the selected subnet.
	Select All	Selects all available subnets.
	Clear All	Clears the selection of all subnets.

Viewing agent details through a search

About this task

Through specific search criteria, you can get a list of agents that are registered with the SLA Mon server and view agent details. You require the agent information to remotely control and monitor the endpoints hosting the agents.

Procedure

1. Log on to the SLA Mon web interface as an administrator.

2. Click **AGENTS**.

The system displays the Agents Search page.

3. In the Search section, enter one or more search criteria in the following fields:

- **Country**
- **State**
- **City**
- **Hardware**
- **Firmware**
- **IP Address**
- **Extn**

4. Click **Search**.

The system displays the details of the agents that match the criteria in the search result section.

Related Links

[Agent Search field descriptions](#) on page 59

Viewing agent details through the location tree

About this task

Using the location tree, you can find agents that are registered with the SLA Mon server and view agent details. You require the agent information to remotely control and monitor the endpoints hosting the agents.

Procedure

1. Log on to the SLA Mon web interface as an administrator.
2. Click **AGENTS**.

The system displays the Agents Search page.

3. In the location tree, on the left pane, click a zone or location to view agents that are present in that location.

You can expand a zone to view the locations under the zone. You can expand locations to country, state, and city level to further narrow the search for agents.

The system displays the details of the agents present in the selected location in the search result section.

Changing the status of an agent

About this task

You can disable an active SLA Mon agent or enable an inactive agent through the web interface. An agent can participate in network monitoring, remote phone control, and other diagnostics only when you enable the agent.

Procedure

1. Log on to the SLA Mon web interface as an administrator.

2. Click **AGENTS**.

The system displays the Agents Search page.

3. Find agents using the search option or the location tree.

The search result table displays the agent details along with the status.

4. To enable an inactive agent, select the agent, and click **Enable**.

The system activates the selected agent.

5. To disable an agent, select the agent, and click **Disable**.

The system deactivates the selected agent.

Note:

In the search result table, the status indicator of the agents acts as a button. You can click the status indicator to enable or disable an agent.

6. To delete agents, select the agents you want to delete, and click **Delete**.

The system deletes the selected agents.

Related Links

[Viewing agent details through a search](#) on page 57

[Viewing agent details through the location tree](#) on page 58

Agent Search field descriptions

You can use the Agent Search page to search and view the details of the agents that are registered with the SLA Mon server. On this page, you can enable, disable, or delete the registered agents .

Search section

In this section, you can enter one or more criteria in the following fields to search an agent.

Name	Description
Country	The country in which you want to search agents.
State	The state in which you want to search agents.

Name	Description
City	The city in which you want to search agents.
Hardware	Particular of hardware for which you want to search agents.
Firmware	The firmware version for which you want to search agents.
IP Address	The IP address of the agent that you want to search.
Extn	The extension of the endpoint where the agent resides.

Button	Description
Search	Searches the SLA Mon agents that match the criteria you enter and displays the agent details in the table.
Reset	Clears the search criteria you entered.

Location tree

The location tree pane displays the locations and zones in the network in a tree structure that organizes the zones and locations in the following way:

- The zones are at the first level in the tree.
- If a location is part of a zone, the location is under the zone at the second level in the tree.
- If a location is not part of any zone, the tree displays the country in which the location is situated at the first level.
- If a location has multiple subnets, the tree displays the subnets at the sublevel under the location.

To see the location selector pane, you must click **Show Tree** in the upper-left corner of the page. You can use the location tree to search and view the details of agents discovered in a particular location. When you click a location in the tree, the search result table displays the agents that the SLA Mon server discovered in that location.

Search result section

Name	Description
IP Address	The IP address of the agent.
Extn	The extension number of the endpoint where the agent resides.
MAC	The MAC address of the endpoint where the agent resides.
Subnet	The subnet address.
Status	The status of the agent. A registered agent can be in one of the following two statuses: • Enable: The agent can participate in network monitoring, remote phone control, and other diagnostics.

Name	Description
	• Disable: The agent cannot participate in network monitoring, remote phone control, and other diagnostics.
Hardware	The hardware details of the endpoint where the agent resides.
Firmware	The firmware details of the endpoint where the agent resides.
Build	The version number of the SLA Mon agent that resides in the endpoint.
Country	The country in which the agent is located.
State Province	The state or province in which the agent is located.
City	The city in which the agent is located.
Select	Check box to select the agent.

Icon	Name	Description
	Enable	Enables the selected agents.
	Disable	Disables the selected agents.
	Delete	Deletes the selected agents.
	Select All	Selects all agents.
	Clear All	Clears all selection of agents.

Administering the SLA Mon server properties

Administration of the SLA Mon Server properties

You can use the Properties page to control global SLA Mon Server properties for configuring SNMP trap receivers, alarm ID and default country for agent discovery. The page consists of three tabs, each containing a group of related properties.

Configuring SNMP traps

Adding an SNMP trap receiver

About this task

The SLA Mon server generates a number of alarms in the form of Simple Network Management Protocol (SNMP) traps to report events. The server sends the alarms to the configured SNMP trap receivers. Use this procedure to add an SNMP trap receiver.

Procedure

1. On the SLA Mon web interface, click **ADMIN > PROPERTIES > SNMP Traps**.
The **SNMP Traps** tab displays the details of the devices that receive traps from the server.
2. In the **Destination IP/Host Name** field next to the **Add New** button, enter the IP address or host name of the device you want to add as a receiver of the SNMP traps from the SLA Mon server.
The system displays the SNMP Trap Detail dialog box to configure the trap destination and the traps details.
3. Select the **Enable** check box to enable the SNMP trap receiver.
4. Select the appropriate options to complete the following fields:
 - **Severity**
 - **Transport Protocol**
 - **SNMP Version**
 - **Notification Type**The **IP/Host Name** field populates the IP address or host name that you enter in the **Destination IP/Host Name** field in the **SNMP Traps** tab.
5. Complete the following fields as appropriate:
 - **Port**
 - **Community**
Only for SNMP version 1 or 2c.
6. If you selected v3 as the SNMP version, complete the following additional fields for the v3 receiver:
 - **Security Name**
 - **Authentication Protocol**
 - **Authentication Password**
 - **Privacy Protocol**
 - **Privacy Password**

7. Select the check boxes beside the alarm types you want the server to send to the SNMP trap destination.
8. For the selected alarm types, select one of the following notification level for the alarms the destination will receive:
 - **Warning**
 - **Major**
 - **Minor**
 - **Critical**
9. Click **Save Changes**.

The **SNMP Traps** tab displays the new trap receiver in the table.

Related Links

[SNMP Traps](#) on page 63

[SNMP Trap Detail](#) on page 64

SNMP Traps

The **SNMP Traps** tab displays the configured destinations of SNMP traps that the SLA Mon server generates. In this tab, you can add, modify, or delete the SNMP trap receivers.

The following tables provide the field and icon descriptions for the SNMP Traps tab.

Name	Description
Destination IP/Host Name	An input field for entering the host name or IP address of the device that receives the SNMP traps from the SLA Mon server.
Select	A check box to select the SNMP trap receiver.
Destination	The host name or IP address of the SNMP trap receiver.
Port	The port number that the receiver uses to receive traps.
Severity	The severity of the notifications that the server sends to the trap receiver .
Version	The SNMP protocol version configured for the receiver.
Notification Type	The type of notification sent to the receiver.

Icon	Name	Description
	Add New	Adds a new SNMP trap receiver and displays the fields to configure the details of the new receiver.

Icon	Name	Description
	Copy To	Copies the configuration details of a selected SNMP trap receiver to another receiver.
	Remove	Deletes selected SNMP trap receivers.
	Start Tests	The SLA Mon server sends a test SNMP trap to the configured trap receiver.
	Select All	Selects all available SNMP trap receivers in the table.
	Clear All	Clears the selection of SNMP trap receivers.

SNMP Trap Detail

Name	Description
Enable	A check box to enable or disable the SNMP trap receiver without deleting it. By default, the configuration is enabled.
Severity	The severity of the notifications that the server sends to the receiver. You can select one of the following options: • Warning and above: The server sends all the notifications, that is, warning, major, minor, and critical. • Minor and above: The server sends only the major, minor, and critical notifications. • Major and above: The server sends only the major and critical notifications. • Critical only: The server sends only the critical notifications.
Transport Protocol	The transport protocol that the server uses to send notifications to the trap receiver. You can select one of the following transport protocols: • UDP • TCP
SNMP Version	The SNMP version that the receiver device supports. You can select one of the following three SNMP versions: • 1

Name	Description
	• 2c • 3
Notification Type	The type of notifications that the server sends to the receiver. You can select one of the following notification types: • Trap: The server sends notifications using the SNMP Trap command. No handshake happens with the receiver to verify whether the notification is received. You can use traps with all versions of SNMP. By default, the server sends the trap notifications to the receiver. • Inform: The server sends notifications using the SNMP Inform command. The receiver sends a response packet to acknowledge the receipt of notification. You can use the Inform notifications only with SNMP versions 2c and 3.
IP / Host Name	The IP address or host name of the trap destination. The system populates this field with the value you entered in the Destination IP/Host Name field in the SNMP Traps tab.
Port	The port number that the receiver device uses to receive SNMP traps. The default value is 162.
Community	The community string of the receiver device. This field is required only if you select the version of the SNMP entity of the receiver as 1 or 2c.
Security Name	The security name or user name configured in the SNMP entity of the receiver device. This field is available only if you selected the SNMP version 3.
Authentication Protocol	The authentication protocol configured in the SNMP entity of the receiver to authenticate the SNMP version 3 messages. This field is available only if you selected the SNMP version 3. You can select one of the following protocols: • MD5 • SHA
Authentication Password	The password for authentication protocol that the receiver uses to authenticate SNMP version 3 messages.
Privacy Protocol	The privacy protocol the server uses to encrypt SNMP version 3 messages. This field is available only if you selected the SNMP version 3.

Name	Description
	You can select one of the following protocols: • DES • AES 128 • AES 192 • AES 256
Privacy Password	The privacy password for encrypted SNMP version 3 messages.
License Alarms	A check box to indicate that you want the server to send license-related alarms to the SNMP trap receiver.
QoS Alarms	A check box to indicate that you want the server to send QoS alarms to the SNMP trap receiver when test results of the last 1 hour exceed the configured strike rate of a QoS parameter.
Start or Stop Alarms	A check box to indicate that you want the server to send alarms to the SNMP trap receiver when a user starts or stops the SLA Mon server.
DSCP Change Alarms	A check box to indicate that you want the server to send alarms to the SNMP trap receiver when the DSCP value changes from the first hop to the last hop between a pair of subnets.
Test Failure Alarms	A check box to indicate that you want the server to send alarms to the SNMP trap receiver when test calls to a subnet fails more than 10% in an hour.
Agent Registration Alarms	A check box to indicate that you want the server to send alarms to the SNMP trap receiver when an agent registration process is successful.
Config Change Alarms	A check box to indicate that you want the server to send alarms to the SNMP trap receiver when any configuration changes are done on the SLA Mon UI.
Agent Discovery Alarms	A check box to indicate that you want the server to send alarms to the SNMP trap receiver when an agent does not respond to the agent discovery request.
Drop-down lists	Severity level assigned to each selected alarm type. The list become available only when you select the respective alarm type. You can assign one of the following four severity levels to an alarm type: • Warning • Major • Minor

Name		Description
		• Critical The default severity for the alarms is Warning .

Icon	Name	Description
	Save Changes	Saves the configuration changes.

Related Links

[Alarms that the SLA Mon server generates](#) on page 128

Editing SNMP trap receiver details**About this task**

Use this procedure to edit and update the details for a SNMP trap receiver.

Procedure

1. In the SNMP traps tab, select the trap receiver which you want to edit and update.
2. Click the row of the selected trap receiver.
The system displays the details of the selected SNMP trap receiver.
3. Make the required changes in the appropriate fields.
4. To save the changes made, click **Save Changes**.

The system updates the SNMP trap receiver details.

Deleting SNMP trap receivers**About this task**

Use this procedure to delete the existing SNMP trap receivers configured in the system.

Procedure

1. In the SNMP Traps tab, select the trap receivers which you want to delete.
You can select multiple receivers.
2. To delete the selected SNMP trap receivers, click the **Remove** button.

The system removes the selected SNMP trap receivers.

Configuring alarming properties

Configuring the alarm ID of the SLA Mon server

Before you begin

Keep the alarm ID, also known as product ID, you received from Avaya for the SLA Mon server handy. You receive a unique alarm ID when you register the server with Avaya for the remote servicing and alarm transfer facilities through SAL.

Note:

If you do not register the SLA Mon server, the SAL remote access and alarm transfer facilities become unavailable for the SLA Mon server.

About this task

To utilize the alarm transfer facility through SAL Gateway from the SLA Mon server to Avaya, you must configure the SLA Mon server with the correct alarm ID. Automated alarm management tools and service engineers at Avaya Data Center can distinguish the alarms received from the server through the alarm ID. Identification of the alarm generating device is critical for servicing the product. Use this procedure to configure the alarm ID on the SLA Mon server.

Procedure

1. On the SLA Mon web interface, click **ADMIN > PROPERTIES > Alarming**.
2. In the **ADS SLA Mon Server AlarmID** field, enter the alarm ID of the SLA Mon server.
3. Click **Save Changes**.

Changing the thresholds of the QoS parameters

About this task

You can control the QoS thresholds that the SLA Mon server applies during the network performance tests. The server compares the test results of each QoS parameter against the configured threshold value for performance analysis. If the frequency of a parameter exceeding the threshold during the last 1 hour is greater than the configured strike limit, the SLA Mon server generates an alarm.

Procedure

1. On the SLA Mon web interface, click **ADMIN > PROPERTIES > Alarming**.
2. Make changes to the threshold values for the following QoS parameters for audio, video, and data traffic as required:
 - **Round Trip Delay**
 - **Jitter**
 - **Packet Loss**
 - **e-MOS**
3. Click **Save Changes**.

Related Links

[Alarming tab](#) on page 69

Changing the strike limits of the QoS parameters

About this task

You can also control the maximum strike limit for alarm generation. The SLA Mon server analyzes the data from the test results every hour to determine whether they constitute an alarm. If the number of responses for the tests in the last 1 hour that exceed a configured QoS threshold is greater than the configured strike limit, the SLA Mon server generates an alarm.

Procedure

1. On the SLA Mon web interface, click **ADMINISTRATION > PROPERTIES > Alarming**.
2. Make changes to the strike limit of the following QoS parameters as required:
 - **Round Trip Delay**
 - **Jitter**
 - **Packet Loss**
 - **e-MOS**
3. Click **Save Changes**.

Related Links

[Alarming tab](#) on page 69

Alarming tab

Through the **Alarming** tab, you can control the QoS thresholds that the SLA Mon server applies to the test sessions. You can also control the maximum strike limit for alarm generation.

Name	Description
Thresholds for round-trip delay:  Note: The SLA Mon agent cannot receive a packet when the one-way delay is greater than 500 ms because the agent times out before receiving the packet. The delay results in 100% test failure and, as a result, the server cannot collect the summary data. Therefore, you must set the threshold value for round-trip delay between 0 to 999 ms.	
Audio	The threshold for round-trip delay in audio traffic. If the round-trip delay measured for a test of audio traffic is greater than this configured value, the SLA Mon server considers the occurrence to generate a QoS alarm. You must enter a value between 0 to 999 ms. The default value is 250 ms.
Video	The threshold for round-trip delay in video traffic. If the round-trip delay measured for a test of video traffic is greater than this configured value, the SLA Mon server considers the occurrence to generate a QoS alarm.

Name	Description
	You must enter a value between 0 to 999 ms. The default value is 350 ms.
Data	The threshold for round-trip delay in data traffic. If the round-trip delay measured for a test of data traffic is greater than this configured value, the SLA Mon server considers the occurrence to generate a QoS alarm. You must enter a value between 0 to 999 ms. The default value is 1000 ms.
Thresholds for jitter:	
Audio	The jitter threshold for audio traffic. If the jitter measured for a test of voice traffic is greater than this configured value, the SLA Mon server considers the occurrence to generate a QoS alarm. You must enter a value between 0 to 10000 ms. The default value is 50 ms.
Video	The jitter threshold for video traffic. If the jitter measured for a test of video traffic is greater than this configured value, the SLA Mon server considers the occurrence to generate a QoS alarm. You must enter a value between 0 to 10000 ms. The default value is 150 ms.
Data	The jitter threshold for data traffic. If the jitter measured for a test of data traffic is greater than this configured value, the SLA Mon server considers the occurrence to generate a QoS alarm. You must enter a value between 0 to 10000 ms. The default value is 500 ms.
Thresholds for packet loss:	
Audio	The packet loss threshold for audio traffic. If the packet loss percentage measured for a test of voice traffic is greater than this configured value, the SLA Mon server considers the occurrence to generate a QoS alarm. You must enter a value between 0 to 100%. The default value is 1%.
Video	The packet loss threshold for video traffic. If the packet loss percentage measured for a test of video traffic is greater than this configured value, the SLA Mon server considers the occurrence to generate a QoS alarm. You must enter a value between 0 to 100%. The default value is 0.5%.
Data	The packet loss threshold for data traffic. If the packet loss percentage measured for a test of data traffic is greater

Name	Description
	than this configured value, the SLA Mon server considers the occurrence to generate a QoS alarm. You must enter a value between 0 to 100%. The default value is 2.5%.
Thresholds for e-MOS:	
Audio	The Estimated mean opinion score (e-MOS) threshold for audio traffic. If the Network Voice Quality (NVQ), an estimation of MOS, measured for a test of audio traffic is less than this configured value, the SLA Mon server considers the occurrence to generate a QoS alarm. You must enter a value between 1.0 to 5.0. The default value is 3.6.
Video	The e-MOS threshold for video traffic. If the NVQ measured for a test of video traffic is less than this configured value, the SLA Mon server considers the occurrence to generate a QoS alarm. You must enter a value between 1.0 to 5.0. The default value is 3.6.
Data	The e-MOS threshold for data traffic. If the NVQ measured for a test of data traffic is less than this configured value, the SLA Mon server considers the occurrence to generate a QoS alarm. You must enter a value between 1.0 to 5.0. The default value is 1.
Strike:	
Round Trip Delay	Strike rate for delay. In the tests for the last 1 hour, if the occurrence of delays that exceed the delay threshold is equal to or greater than this configured strike rate, the SLA Mon server generates a QoS alarm. You must enter a value between 1 to 50. The default value is 2.
Jitter	Strike rate for jitter. In the tests for the last 1 hour, if the occurrence of jitters that exceed the jitter threshold is equal to or greater than this strike rate, the SLA Mon server generates a QoS alarm. You must enter a value between 1 to 50. The default value is 2.
Packet Loss	Strike rate for packet loss. In the tests for the last 1 hour, if the occurrence of packet losses that exceed the loss threshold is equal to or greater than this strike rate, the SLA Mon server generates a QoS alarm.

Name	Description
	You must enter a value between 1 to 50. The default value is 2.
e-MOS	Strike rate for e-MOS. In the tests for the last 1 hour, if the occurrence of NVQ measurements that did not reach NVQ threshold is equal to or greater than this strike rate, the SLA Mon server generates QoS alarm. You must enter a value between 1 to 50. The default value is 2.
SLA Mon Server AlarmID	The unique 10-digit ID, also known as Product ID, assigned to the SLA Mon server when you register the server with Avaya for SAL remote access and alarm transfer facilities. The Alarm ID is used to report alarms to Avaya. The Alarm ID helps Avaya Services to identify the product that raises an alarm. You must set this property if you want SAL Gateway to transfer alarms from the SLA Mon server to Avaya.

Icon	Name	Description
	Save Changes	Saves the modifications to the properties.

Modifying DSCP values

About this task

The test session properties that you can modify are the three default DSCP values used for the three traffic types, voice, video, and data.

Procedure

1. In the SLA Mon web interface, click **ADMIN > PROPERTIES > Test Setup**.
2. Modify the following field values as required:
 - **Default Voice DSCP**
 - **Default Video DSCP**
 - **Default Data DSCP**
3. To simulate video traffic during test sessions, select the **Is Video Enabled** check box.

*** Note:**

After selecting this check box, if you edit a manual test pattern to add test calls between two subnets, the system adds three test calls for data, voice, and video traffic to the **Table of Tests in Pattern**.

4. Click **Save Changes**.

Related Links

[Test Setup](#) on page 73

Test Setup

In the Test Setup tab, you can modify the Differentiated Services Code Point (DSCP) values to be used in test calls for voice, video, and data traffic.

Name	Description
Default Voice DSCP	The DSCP value for voice traffic. The default value is 46.
Default Video DSCP	The DSCP value for video traffic. The default value is 26.
Default Data DSCP	The DSCP value for data traffic. The default value is 0.
Is Video Enabled?	A check box to indicate that the SLA Mon server simulates video traffic during test sessions.

Icon	Name	Description
	Save Changes	Saves the modifications.
	Restore Defaults	Restores the default DSCP values for audio, video and data traffic.

Configuring system properties

About this task

Use the System Properties tab of the Administration page, to configure the default country for the SLA Mon agent discovery.

Procedure

1. Go to **ADMIN > PROPERTIES > System Properties**.
2. Select the appropriate country option from the **Default Country for Discovery** drop-down list box.
3. Click **Save Changes** to set the selected country as a default country for discovery.

 Note:

The country configured in the system properties is populated by default in the **Country** field of the Agent Discovery page.

System Properties

In the System Properties tab, you can select a country name to set it as the default country for discovering SLA Mon agents.

Name	Description
Default Country for Discovery	The name of the country that appears as default on the Agent Discovery page. You can select a default country for discovering the SLA Mon agents.

Administering zones

Zone management

Using the zone management feature, you can group subnets and the SLA Mon agents present in the subnets within a zone. The grouping of agents within zones is helpful in managing agents. While discovering agents, you can assign the agents to a specific zone.

To test the network quality between two zones, SLA Mon Server runs the test between two agents, one from each zone, instead of involving all agents present in the two zones. In addition, SLA Mon Server carries out agent to agent tests within a zone.

Creating a zone

Procedure

1. In the SLA Mon web interface, click **ADMIN > ZONE MANAGEMENT**.
2. In the Zones section on the Zone Management page, type a zone name in the text field, and click **Create New Zone** () beside the field.

The system displays the new zone in the Zones section.

Renaming a zone

Procedure

1. In the SLA Mon web interface, click **ADMIN > ZONE MANAGEMENT**.
2. In the Zones section on the Zone Management page, click the **Edit Zone Name** () icon beside the zone you want to rename.
3. In the Edit Zone Name dialog box, type the new zone name, and click **Save**.

The system renames the zone and displays the new zone name in the Zones section.

Deleting a zone

Procedure

1. In the SLA Mon web interface, click **ADMIN > ZONE MANAGEMENT**.
2. In the Zones section on the Zone Management page, click the **Delete Zone** (✖) icon beside the zone you want to delete.
3. In the Confirm Zone Deletion dialog box, click **Proceed**.

The system deletes the zone. However, the subnets and the agents remain registered with the SLA Mon server. You can add the agents to some other zone.

Adding a subnet location to a zone

Procedure

1. In the SLA Mon web interface, click **ADMIN > ZONE MANAGEMENT**.
2. In the Subnet Locations section on the Zone Management page, from the **Add to Zone** field, select the zone within which you want to add a subnet location.
3. Click **Expand All** to expand the tree view structure of the subnet locations.
4. Click the **Add to Selected Zone** (➤) icon beside the subnet location you want to add to the selected zone.

The system adds the subnet location under the selected zone in the Zones section.

5. To view the tree view structure of the zones and the subnets added under the zones, Click **Expand All** in the Zones section.

Removing a subnet location from a zone

Procedure

1. In the SLA Mon web interface, click **ADMIN > ZONE MANAGEMENT**.
2. In the Zones section on the Zone Management page, click **Expand All** to view the tree view structure of the zones and the subnets under the zones.
3. Click the **Remove Zone Location** (✖) icon beside the subnet location you want to remove from the zone.

The system removes the subnet location from the zone.

Chapter 8: Administering the SLA Mon server through CLI

Administration of SLA Mon through CLI

You can use the command line interface (CLI) of the SLA Mon server to administer and use the SLA Mon features, including phone remote control and packet capture. The CLI of the SLA Mon server provides a number of commands to perform the administrative tasks. If the SLA Mon web interface is unavailable for some reason, you can still use the SLA Mon CLI to continue using the SLA Mon features.

Important:

The SLA Mon web interface is unavailable on Services-VM. You must use the SLA Mon CLI to perform all tasks for SLA Mon on Services-VM.

Starting a CLI session on the SLA Mon server

About this task

Use CLI of the SLA Mon server to discover agents, start a remote control session, start event monitoring, enable packet capture, and perform other tasks.

Procedure

1. Log on to the Avaya Diagnostic Server host as a privileged user to run the SLA Mon CLI.
2. Perform one of the following:
 - If `/usr/local/bin/` is the present working directory path, run the following command:
`slamoncli`
 - Run the following command:
`/usr/local/bin/slamoncli`

Result

The system switches you to the `slamon` prompt. You can now run the CLI commands available for the SLA Mon server.

*** Note:**

- The SLA Mon server allows only three parallel CLI sessions.
- You can run the **help** command to view the details of the available commands for remote control, packet capture, or other CLI-based tasks. To get help for a specific command, run the **help <command name>** command. The system displays the description and use of that command.

For example, to view the details of the **remove** command, run the **help remove** command. The system displays the use and syntax for **remove**.

CLI commands for the SLA Mon server

The following table lists the CLI commands available through CLI of the SLA Mon server.

Command	Description	Syntax
help	Displays the help information for the available commands in the CLI mode.	help help <command_name> Example: help agent
exit	Exits the SLA Mon CLI.	exit
agent	Starts a remote control session to an SLA Mon agent residing on an endpoint.	agent <IP MAC Extension of agent> Examples: agent 1234 agent 192.178.23.1
remove	Removes packet capture instances or agents according to the parameters you pass with the command.	To remove all agents: remove agents all To remove a specific agent: remove agents <CIDR IP Extension MAC of agent> To remove all packet capture instances: remove sniffer all To remove packet capture instances related to a specific agent: remove sniffer <IP Extension MAC of agent> [captureInstanceId] Where, <i>captureInstanceId</i> is optional. Examples:

Command	Description	Syntax
		<pre>remove agents 1234</pre> <pre>remove sniffer 1234 3</pre> To remove a SNMP destination for SLA Mon: - To remove all the SNMP destinations: <pre>remove snmpdest <ip-address hostname all></pre> Where, replace <ip-address hostname all> with the IP address or the host name of the destination server. For example: <pre>remove 192.123.211.232 all</pre> - To remove a particular SNMP destination: <pre>remove snmpdest <ip-address hostname></pre> Where, replace <ip-address hostname> with the IP address or the host name of the destination server For example: <pre>remove snmpdest 192.123.211.232</pre>
list	Displays the following based on the parameters you pass with the command: - List of agents registered with the SLA Mon server. - List of agents for which event monitoring is enabled. - List of all subnet ranges you used for agent discovery. - List of all packet capture instances. - List of packet capture instances related to a specified agent.	To list all agents registered with the SLA Mon server: <pre>list agents</pre> To list all capture instances: <pre>list sniffer</pre> To list all capture instances for a specific agent: <pre>list sniffer <IP Ext MAC of agent></pre> To list all agents for which you enabled event monitoring: <pre>list eventmon</pre> Example: <pre>list sniffer 1234</pre> To list the SNMP destinations configured for the SLA Mon server:

Command	Description	Syntax
		list snmpdest
show	Displays the details of an agent registered with the SLA Mon server.	show agent <CIDR IP Ext MAC of agent> Example: show agent 1234 To display the details for a SNMP destination for the SLA Mon server: show snmpdest <ip-address hostname> Where replace <ip-address hostname> with the IP address of the destination and replace <ip-address hostname> with the host name of the destination server. For example: show snmpdest 192.123.211.232
discover	Runs agent discovery on the CIDR range that you specify.	To run manual discovery on an address range: discover agents <subnet range in CIDR format> Examples: discover agents 192.223.22.32/32  Note: The agents discovered using the CLI do not appear in the Agents page of the Web UI. If you want to use the same agents in the Web UI, you must run the agent discovery again from the Web UI for the particular agent or range of agents.
enable	Starts the packet capture or the event monitoring functionality on an agent based on the parameters you pass.	To start packet capture on an agent: enable sniffer <IP Ext MAC of agent> To start event monitoring on an agent: enable eventmon <IP Ext MAC of agent> Examples: enable sniffer 1234 enable eventmon 1234

Command	Description	Syntax
disable	Stops the packet capture or the event monitoring functionality on an agent based on the parameters you pass.	To stop packet capture on an agent: <pre>disable sniffer <IP Ext MAC of agent></pre> To stop event monitoring on an agent: <pre>disable eventmon <IP Ext MAC of agent></pre> Examples: <pre>disable sniffer 1234</pre> <pre>disable eventmon 1234</pre>
copy	Copies the captured instance of an agent during a packet capture process to a file you specify.	<pre>copy sniffer <IP Ext MAC of agent> <captureInstanceID> file: // <filepath></pre> Where, <i>captureInstanceID</i> is the ID assigned to a packet capture instance and <i>filepath</i> is the absolute file path where the data is to be saved. Example: <pre>copy sniffer 1234 2 file: // root/captures/A1234Apr9.pcap</pre>
execute	Runs the bulk call or bulk terminate commands.	To make bulk calls: <pre>execute -bulk call file: // <filepath> [call_duration] [call_answer_duration]</pre> Where, <i>filepath</i> is the absolute file path of the file that contains the pairs of telephone numbers to make bulk calls. The <i>call_duration</i> and the <i>call_answer_duration</i> parameters are optional and in seconds. To terminate bulk calls: <pre>execute -bulk terminate</pre> Example: <pre>execute -bulk call file: //root/temp/bulkcall.txt</pre>
setweblmipadd	Sets the IP addresss or host name of the WebLM server.	To configure the WebLM IP address or host name: <pre>setweblmipadd <IP Address></pre> Where, <IP Address> is the IP address of the WebLM server to be configured Example:

Command	Description	Syntax
		setweblmipadd 192.132.233.232  Note: If you change the IP address of the WebLM server after the installation of Avaya Diagnostic Server using the setweblmipadd command, you must restart the slamonsrvr and slamonweb services. Use the following commands to restart the services: <pre>/sbin/service slamonsrvr restart /sbin/service slamonweb restart</pre>
setalarmid	Sets the alarm ID.	To configure the Alarm ID: setalarmid <Alarm ID> Where <Alarm ID> is the Alarm ID of the Example: setalarmid <Alarm ID> Where, the Alarm ID is a ten-digit number acceptable within the range of 1000000000 to 9999999999.
add	Adds SNMP destination for the SLA Mon server. Here <SNMP version> can be either 1, 2c, or 3.	To add SNMP destination for the SLA Mon server: add snmpdest <ip-address hostname> <SNMP version> Where, replace <ip-address hostname> with the IP address or the host name of the destination server and replace <SNMP version> with the SNMP version 1, 2c, or 3.

 Note:

You cannot modify or disable the added SNMP destinations from CLI.

Viewing the CLI commands for the SLA Mon server

About this task

Use this procedure to view the descriptions of the CLI commands available for the SLA Mon server.

Procedure

1. On the CLI prompt of the SLA Mon server, run the **help** command.
The system displays the available commands and the brief descriptions of the commands.
2. To view the detailed help information for a specific command, run the following command:

help <command name>

The system displays the command description and the syntax to run the command.

Discovering SLA Mon agents through CLI of the SLA Mon server

About this task

Use this procedure to discover agents in a network range and to register the agents with the SLA Mon server.

Procedure

1. Log on to the SLA Mon server host as a user with administrative privilege, and start a CLI session for the SLA Mon server.
2. On the SLA Mon CLI prompt, run the following command to discover and register agents with the SLA Mon server:

discover agents <subnet range in CIDR format>

Example:

discover agents 192.123.211.232/32

The system searches for agents present on the specified network range and registers the discovered agents with the SLA Mon server.

Chapter 9: Administering test patterns

Test patterns

A test pattern defines a set of test calls that Avaya Diagnostic Server with the SLA Mon technology runs on the customer network for network monitoring. The SLA Mon server supports two types of test patterns:

- **Manual.** For a manual test pattern, you, as an administrator, can create the list of the tests to be run.
- **Automatic.** For an automatic test pattern, you define the criteria to be used to create the list of test calls. The SLA Mon server uses these criteria to create the list of tests considering the network topology, if available, and the available and enabled agents.

The SLA Mon server initially has one automatic test pattern, named `default`, which the server runs if you do not define and run any other pattern. The default pattern uses all available and enabled subnets for the test calls. That is, the server runs the test for all subnet combinations.

Adding a test pattern

About this task

You can add and customize test patterns according to the requirements.

Procedure

1. Log on to the SLA Mon web interface as an administrator.
2. Click **TEST ADMINISTRATION > TEST PATTERNS**.
3. In the **New Pattern Name** field, type a name for the new pattern.
4. **(Optional)** To specify the test pattern as automatic, select the **Auto** check box.
5. Click **Add New**.

The system displays the new pattern in the Test Pattern table.

Next steps

Edit the test pattern to customize it.

Related Links

[Customizing a manual test pattern](#) on page 85

[Customizing an automatic test pattern](#) on page 85

Copying a test pattern

About this task

You can copy an existing test pattern to create a new test pattern.

Procedure

1. On the SLA Mon web interface, click **TEST ADMINISTRATION > TEST PATTERNS**.
2. In the **New Pattern Name** field beside the **Copy To** button, type a name for the new pattern.
3. In the Test Pattern table, click on the pattern you want to copy.

You cannot copy the default test pattern.

4. Click **Copy To**.

The system displays a message about the result of the copy action.

If the copy action is successful, the system displays the new pattern in the Test Pattern table.

Next steps

Edit the test pattern to customize it.

Related Links

[Customizing a manual test pattern](#) on page 85

[Customizing an automatic test pattern](#) on page 85

Deleting a test pattern

About this task

You can delete the test patterns you do not require.

Procedure

1. On the SLA Mon web interface, click **TEST ADMINISTRATION > TEST PATTERNS**.
2. In the Test Pattern table, select the **Remove** check box beside the test pattern you want to remove.

You can select multiple test patterns for deletion.

3. Click **Remove**.

You cannot delete the default test pattern.

The system displays a message about the remove action and removes the test pattern from the table.

Customizing an automatic test pattern

About this task

The strategy used by automatic test patterns you create is the same as the default test pattern. You can edit an automatic test pattern to specify the criteria for creating a list of tests. When the pattern is running, The SLA Mon server periodically uses these criteria to create the list of tests automatically. While creating the list of tests, the SLA Mon server also takes into consideration the current network topology, availability of test agents on the network, and the subnets discovered with test agents.

Procedure

1. On the SLA Mon web interface, click **TEST ADMINISTRATION > TEST PATTERNS** .
2. In the table of test patterns, click the automatic test pattern you want to customize.
3. In the Detail section on the right side of the page, make the required changes to the following attributes:
 - **Max Tests/Subnet**
 - **Max Tests/Network**
 - **Default Codec**
4. Click **Save Changes**.

Related Links

[Test Patterns field descriptions](#) on page 88

Customizing a manual test pattern

About this task

For a manual test pattern, you explicitly create the list of tests to simulate. You can add either a single test or multiple tests to a manual test pattern.

Procedure

1. On the SLA Mon web interface, click **TEST ADMINISTRATION > TEST PATTERNS** .
2. In the table of test patterns, click the manual test pattern you want to customize.
3. In the Detail section on the right side of the page, make the required changes to the following attributes:
 - **Max Tests/Subnet**

- **Max Tests/Network**
- **Default Codec**

4. To add a single test to the manual test pattern, perform the following:
 - a. In the **Subnet 1** and the **Subnet 2** fields, enter two subnet addresses for testing. To view the subnets you can choose, click the **Search** icon.
 - b. Click **Add Test**.

If you enable video traffic in the **ADMIN > PROPERTIES > Test Setup** tab, the system adds three tests for data, voice, and video traffic to the table of tests. Otherwise, the system adds two tests for data and voice.
 - c. Repeat steps 3.a and 3.b to add more tests to the test pattern.
5. To use a predefined algorithm to add multiple tests to the test pattern at one go, perform the following:
 - a. From the **Test Generation Algorithm** list, select **All Subnet Combinations**.
 - b. If required, make changes to the attributes mentioned in step 2.
 - c. Click **Generate**.

Based on the selected algorithm and the subnets discovered, the system adds multiple tests that involve all the subnets that are available and enabled.
6. If you have an Excel file of valid tests, click **Import Test Pattern** to import and add the tests to the test pattern.
7. To remove individual tests from the test pattern, select the **Remove** check box beside the test in the table of tests, and click **Remove Tests**.
8. Click **Save Changes**.

Related Links

[Test Patterns field descriptions](#) on page 88

[Importing data to a test pattern](#) on page 87

[Exporting a test pattern](#) on page 86

Exporting a test pattern

About this task

You can export a test pattern that has a valid set of tests. You can save the exported tests as an Excel worksheet to a local folder. You can change the data in the worksheet and reuse the tests in other test patterns.

Procedure

1. On the SLA Mon web interface, click **TEST ADMINISTRATION > TEST PATTERNS**.
2. In the table of test patterns, click the manual test pattern that you want to export.

3. In the Detail section on the right side of the page, ensure that the test pattern has some valid tests.
4. Click **Export Test Pattern**.
The system opens a File Download dialog box.
5. Click **Save** , and save the Excel file containing the tests to a local folder on your computer.

Next steps

You can open the excel file to make the following changes before importing the tests to another test pattern:

- Change the values in the existing rows.
- Add a new row to represent a new test.
- Delete a row.

Importing data to a test pattern

Before you begin

Ensure that you already have an Excel worksheet where you exported a test pattern with a valid set of tests.

Ensure that you made required changes to the test data, such as changing a subnet address and adding new rows, according to your network requirement.

Ensure that the subnet addresses you entered in the worksheet are available and enabled in the SLA Mon server.

About this task

If you have an Excel worksheet containing a valid set of tests, you can import the tests to a manual test pattern.

Procedure

1. On the SLA Mon web interface, click **TEST ADMINISTRATION > TEST PATTERNS** .
2. In the table of test patterns, click the manual test pattern that you want to change.
3. In the Detail section on the right side of the page, click **Import Test Pattern**.
The system displays the Import Test Pattern dialog box.
4. Click **Browse**, find the Excel file containing the tests, and click **Open**.
5. On the Import Test Pattern dialog box, click **Upload**.

The system uploads the file and starts validating the tests. The subnets must be available and enabled on the system to pass the validation.

If the validation is successful, the dialog box displays a upload successful message and the **Import** button.

6. Click **Import**.

The system imports the tests to the test pattern and displays the tests in the table.

7. Click **Save Changes**.

Test Patterns field descriptions

Summary section

In the summary section, you can create, copy, and delete test patterns. You can also view the list of test patterns.

Name	Description
New Pattern Name (Beside Add New)	Text box to enter the name of the new test pattern you want to create.
New Pattern Name (Beside Copy To)	Text box to enter the name of the new test pattern to which you want to copy the configuration of an existing pattern.
Auto	Check box to indicate whether the call pattern is automatic.
Fields in the Test Patterns table:	
Test pattern	The name of the test pattern.
Auto	The test pattern type. The field displays one of the following two values: • true: Indicates that the test pattern is automatic. • false: Indicates that the test pattern is manual.
Remove	Check box to select the test pattern for deletion.

Icon	Name	Description
	Add New	Adds the new test pattern and displays the pattern in the Test Patterns table.
	Copy To	Copies the details of the selected test pattern to the new test pattern.
	Remove	Removes the selected test patterns.
	Select All	Selects all test patterns in the table.
	Clear All	Clears the selection of test patterns in the table.

Detail section

In the Detail section, you can view the configuration details of a selected test pattern and change the details. For a manual test pattern, you can explicitly create the list of tests to simulate.

Name	Description								
Name	The name of the test pattern.								
Test Duration (sec)	The duration of each test call in seconds. The value is 1 second and the field is read-only.								
Max Tests/Subnet	The maximum number of simultaneous tests that can run to or from a subnet. The default value is 5.								
Max Tests/Network	The maximum number of simultaneous tests through the network. The SLA Mon server uses this criterion for all types of test patterns. The default value is 2000.								
Default Codec	The codec to be used for simulating the traffic for test sessions. You can select one of the following two: • G.729 • G.711u The default codec is G.729. The sample size for G.729 and for G.711 is the same, 20 milliseconds. However, G.729 is a smaller packet because of compression and hence uses lower bandwidth. Bandwidth consumption by G.729 is approximately 24 kbps and by G.711 is approximately 80 kbps. If you run video tests along with voice and data, then bandwidth consumption is 72 kbps and 240 kbps per test, respectively. Therefore, the maximum bandwidth consumption by test traffic at any point in time can be: <table> <tr> <td>In a subnet</td><td>G.729: Max Tests/Subnet multiplied by 72 kbps</td></tr> <tr> <td></td><td>G.711: Max Tests/Subnet multiplied by 240 kbps</td></tr> <tr> <td>On the network</td><td>G.729: Max Tests/Network multiplied by 72 kbps</td></tr> <tr> <td></td><td>G.711: Max Tests/Network multiplied by 240 kbps</td></tr> </table>	In a subnet	G.729: Max Tests/Subnet multiplied by 72 kbps		G.711: Max Tests/Subnet multiplied by 240 kbps	On the network	G.729: Max Tests/Network multiplied by 72 kbps		G.711: Max Tests/Network multiplied by 240 kbps
In a subnet	G.729: Max Tests/Subnet multiplied by 72 kbps								
	G.711: Max Tests/Subnet multiplied by 240 kbps								
On the network	G.729: Max Tests/Network multiplied by 72 kbps								
	G.711: Max Tests/Network multiplied by 240 kbps								
Default DSCP	The Differentiated Services Code Point (DSCP) values to be used in test calls for voice, video, and data traffic. The default values are 46, 26, and 0 for voice, video, and data, respectively. The field is read-only. However, you can change the default DSCP values on the ADMIN > PROPERTIES > Test Setup page.								
The following fields are available only for a manual test pattern.									
Subnet 1	Address of the first subnet from the pair of subnets that you want to involve in the test.								
Subnet 2	Address of the second subnet from the pair of subnets that you want to involve in the test.								

Name	Description
Test Generation Algorithm	The name of the predefined algorithm that you can use to add tests to the test pattern. The valid value in this field is: • All Subnet Combinations The All Subnet Combinations algorithm adds tests that connect each available and active subnet to all other subnets.
Fields in the tests table:	
Subnet 1	Address of the first subnet from the pair of subnets that is involved in the test.
Zone	The zone to which Subnet 1 belongs, if any.
Subnet 2	Address of the second subnet from the pair of subnets that you want to involve in the testing.
Zone	The zone to which Subnet 2 belongs, if any.
Codec	The codec to be used for simulating the test traffic.
DSCP	The DSCP value to be used in the test.
Remove	Check box to select the test for deletion.

Icon	Name	Description
	Add Test	Adds tests involving the entered subnet pair. If you selected video traffic for testing on the ADMIN > PROPERTIES > Test Setup page, the system adds three tests for data, voice, and video traffic. Otherwise, the system adds two tests for data and voice traffic.
	Generate	Adds multiple tests that involve all subnets that are available and active.
	Remove Tests	Removes the selected tests.
	Select All	Selects all tests in the table.
	Clear All	Clears the selection of tests in the table.
	Save Changes	Saves the changes.

Button	Description
Export Test Pattern	Exports the set of tests that exist for the selected test pattern to an Excel worksheet.
Import Test Pattern	Imports and adds tests to the selected test pattern from an Excel worksheet that you have exported and changed.

Test Execution

Through the Test Execution page, you can start test calls, stop test calls, choose a test pattern to run, and see the status of the selected test pattern. The following tables provides the icon and field descriptions for the page.

Test Control section

Name	Description
Current Test Pattern	The currently selected test pattern.
Status	The status of the selected test pattern.

Icon	Name	Description
	Start Tests	Starts the tests of the selected test pattern.
	Stop Tests	Stops the currently running tests.
	View Test List	Displays the subnet pairs used in the currently running tests in a popup window.
	Refresh Data	Refreshes data on the page.
	Validate Pattern	Validates the selected test pattern and displays the validation summary in a popup window.

Test Summary section

This section displays two tables that displays the summary of the test tests made in the last 1 hour. The first table lists the time the tests are executed, the number of attempted tests, and the number of failed tests. The second table displays the rate of failed test attempts for the subnets included in the selected test pattern.

Running a user-defined test pattern

About this task

When you do not select any customized test pattern to run, the SLA Mon server runs the default test pattern to check the network condition. You can stop the default test pattern and run another test pattern to check the network.

Procedure

1. Log on to the SLA Mon web interface as an administrator.
2. Click **TEST ADMINISTRATION > TEST EXECUTION** .
3. If a test pattern is already in the Running status, click **Stop Tests**.
4. In the **Current Test Pattern** field, select the test pattern you want to run.

5. Click **Start Tests**.

Viewing the list of subnet pairs in a test pattern

About this task

You can view the subnet pairs between which the tests are run based on the currently running test pattern.

Procedure

1. On the SLA Mon web interface, click **TEST ADMINISTRATION > TEST EXECUTION**.
2. Click **View Test List**.

The system displays the Running Test List For dialog box. The dialog box displays the subnet pairs that the currently running test pattern uses for the tests.

Chapter 10: Remotely controlling Avaya endpoints

Remote control of Avaya endpoints

As a serviceability engineer, you can remotely control Avaya endpoints that have an SLA Mon agent configured and registered with the SLA Mon server. The remote control feature of the SLA Mon agent is useful in remote troubleshooting, testing, and administering Avaya endpoints.

Through the phone remote control feature, you can perform the following:

- Monitor the screen of Avaya endpoints.
- Monitor the events, such as button presses or touch events, occurring on a phone.
- Perform remote activities on an endpoint, such as pressing buttons or performing touch events.
- Make a call from an endpoint.
- Answer a call from an endpoint.
- Make bulk calls.

You can gain remote access to Avaya endpoints in two ways:

- Using the SLA Mon server web interface.
- Using the command line interface (CLI) of the SLA Mon server.

For you to be able to control an Avaya endpoint remotely, the endpoint must meet the following criteria:

- The version of the SLA Mon agent present on the endpoint is release 2 or later.
- The SLA Mon agent is configured and registered with the SLA Mon server.
- The remote control feature is enabled on the SLA Mon agent.

! Important:

- The Avaya 9610 endpoints do not support phone remote control.
- The Avaya H.323 3.1.4 firmware does not support event monitoring.

Remotely controlling Avaya endpoints through the SLA Mon web interface

Starting a remote control session from the SLA Mon web interface

Before you begin

Ensure that the SLA Mon agent on the endpoint to which you want to establish a remote control session is registered with the SLA Mon server. If the required agent is not registered with the SLA Mon server, run the agent discovery process on the Agent Discovery page of the SLA Mon web interface.

About this task

Use this procedure to establish a remote control session with an endpoint for monitoring the phone events and for performing remote activities on the endpoint.

Note:

Two users can log on to the SLA Mon web interface simultaneously. Each user can control maximum six remote control sessions simultaneously.

Procedure

1. On the SLA Mon web interface, click **DIAGNOSTICS > AGENT REMOTE**.
2. On the Agent Remote page, in the **Agent Extension / IP** field, enter the IP address or the extension of the endpoint.

You can use the **Search** () button to search and select from multiple agents that are registered with the SLA Mon server.

3. Click **Start**.

The system establishes the remote control session to the specified endpoint and starts monitoring events on the endpoint.

The Agent Remote page displays a tab for the remotely controlled endpoint. You can use the button controls and the fields in the tab to control and monitor the endpoint.

4. Repeat steps 2 and 3 to start more remote control sessions.

You can select maximum six agents for simultaneous remote control sessions. However, at a time, only one remote control session is possible on one endpoint.

Note:

After you establish a remote control session with an endpoint, the agent is locked for 3 minutes for other users. That is, no one else can establish a remote control session with the same endpoint during that 3 minutes. If you perform any action within that period, such as a button press, the locking period gets extended by another 3 minutes. Inactivity

of 3 minutes after you start the remote session or perform the last remote action, the agent becomes available to other users through both CLI and web interface.

Next steps

Close the remote session tabs before you sign out of the SLA Mon web interface. Otherwise, the agents remain locked for the next 2 minutes and remain unavailable for any other user. When you try to access a locked agent, you get an exception that states that another user is accessing the agent through the UI.

Agent Remote page

General section

When you first navigate to the Agent Remote page, the page displays the following fields and buttons.

Name	Description
Agent Extension / IP	The IP address or the extension of the Avaya endpoint with which you want to establish a remote control session.
Button	Description
Start	Establishes a remote control session with the Avaya endpoint you specify.
 (Search Agent)	Displays the Agent Search dialog box to search and select registered SLA Mon agents.

* Note:

You can select maximum six agents for simultaneous remote control sessions.

Agent tab

For each remote control session, the Agent Remote page displays an agent tab. For example, if you have three remote control sessions running simultaneously, then the page provides three tabs for three different agents.

The agent tab has fields and buttons for performing remote activities on an endpoint. The tabs also have sections for monitoring event logs, LED status, and the display on the endpoint.

Common field and button descriptions:

Name	Description
Agent Monitoring	The state of the phone remote monitoring sessions. The field displays one of the following two states: • Active: In this state, the Agent Remote page keeps refreshing to display the real-time LED status, the events, and the status of the endpoint by updating the page. • Idle: After 5 minutes of inactivity on the Agent Remote page, the state of the open remote control sessions change from

Name	Description
	Active to Idle. In this state, the Agent Remote page stops refreshing. The LED status, the event logs, and the screen capture of the endpoint stop reflecting the latest activities occurring on the endpoint. To bring the remote control sessions back to the Active state, you must perform some input actions, such as a button press or a touchscreen event. After the action, one of the following two scenarios might occur: - Another user took over the phone remote control session through a different interface, CLI or web interface. In such a case, the system displays a dialog box instructing you to close the current agent tab. - The agent is still available for remote control. In such a case, the state of the agent monitoring process changes from Idle to Active. The screen capture, the LED status, and the event log of the endpoint resume reflecting the latest endpoint activities. The time out on the Agent Remote page is applicable to all the open remote session tabs collectively. For example, if you have five open tabs, then all the five tabs become idle or active at the same time.
Text box	The telephone number or the extension of the destination telephone to which you want to call from the remotely controlled endpoint. The telephone number can be an external number.

Button	Description
Call	Calls from the remotely controlled endpoint to the destination specified in the text box.
Clear	Clears the entry in the text box.
Refresh Image	Refreshes the image of the endpoint screen to reflect the current status on the endpoint.
Enable Event Monitoring	Starts event monitoring on the endpoint and starts displaying events in the Event log section.
Disable Event Monitoring	Stops event monitoring on the endpoint. The Event log section stops displaying events that occur on the endpoint.

Deskphone buttons:

The agent tab has a section for the buttons that are available on the endpoint. According to the Avaya endpoint model type, the set of buttons available on the tab differs.

When you click an endpoint button displayed on the tab, the corresponding button on the remote endpoint is pressed.

LED Status section:

The section displays the list of LED buttons and the status of the buttons.

Name	Description
 (Red)	Off
 (Green)	On

Event Log section:

When event monitoring is enabled for the deskphone, this section displays events that occur on the deskphone with the latest events at the top of the list.

For a button press event, the system records two events, one for button press and another for button release.

Sample of log records for button press events:

```
Button Event [ State: RELEASE, Key: 1, Code: 81, Format:
VXWORKS_KEYBOARD ]
```

```
Button Event [ State: RELEASE, Key: 1, Code: 81, Format:
VXWORKS_KEYBOARD ]
```

```
Button Event [ State: PRESS, Key: SPEAKER, Code: 84, Format:
VXWORKS_KEYBOARD ]
```

```
Button Event [ State: RELEASE, Key: SPEAKER, Code: 84, Format:
VXWORKS_KEYBOARD ]
```

Deskphone screen section:

In this section, you can monitor what the actual screen of the Avaya endpoints display in real time.

Phone Refresh Interval:

- For all endpoints, the refresh interval for screen capture, LED status, and the event logs is set to 5 seconds.

*** Note:**

For 9670 endpoints, there might be a little delay in the screen refresh due to bigger screen size.

Using the SLA Mon web interface to remotely control touch screen interactions

About this task

After establishing a remote control session with an Avaya touch screen endpoint, you can perform touch events remotely on the endpoint through the SLA Mon web interface.

Procedure

1. On the Agent Remote page, start a remote control session to the touch screen endpoint you want to use.
2. Perform the following:
 - a. Navigate to the endpoint screen capture section in the tab.

- b. On the screen capture of the endpoint, click the keys that you want to press.

The mouse click actions on the screen capture reflect as a touch event on the touch screen endpoint. In addition, the event logs reflect the touch events.

Using the SLA Mon web interface to make a call from a remotely controlled Avaya endpoint

About this task

Use this procedure to make a call from a remotely controlled Avaya endpoint using the SLA Mon web interface.

Procedure

1. On the Agent Remote page, start a remote control session to the endpoint.

The system displays a new agent tab on the Agent Remote page.

2. In the text box in the agent tab, enter the phone number or the extension that you want to call.
3. Click **Call**.

The remotely controlled endpoint calls the destination number. You can see the `Calling` message on the screen capture of the endpoint.

Remotely controlling Avaya endpoints through CLI

Starting a phone remote control session from CLI of SLA Mon Server

Before you begin

Ensure that the agent on the endpoint for which you want to start a remote control session is registered with SLA Mon Server.

Note:

If the required agent is not registered with SLA Mon Server, you can run the `discover` command to discover and register the agent. For more information, see [Discovering SLA Mon agents through CLI of the SLA Mon server](#) on page 82.

About this task

Start a remote control session to an agent to remotely control the activities on the endpoint where the agent resides.

Procedure

1. Log on to the Avaya Diagnostic Server host as a privileged user, and start the CLI session.
See [Starting a CLI session on the SLA Mon server](#) on page 76.

2. On the CLI prompt for SLA Mon Server, run the following command to view the agents registered with SLA Mon Server:

```
list agents
```

3. Run the following command:

```
agent <IP|MAC|extension of the agent>
```

For example, if the extension number of the agent is 1234, type the command as:

```
agent 1234
```

4. If you want to enable event monitoring for the agent, type `y`.

The system starts the remote control session for the specified agent on the endpoint and displays the extension of the agent in the CLI prompt. After you establish a remote control session to an endpoint, a new set of CLI commands become available. You can now use these commands to remotely control the activities on the endpoint.

CLI commands for the phone remote control mode

The following table lists the CLI commands that are available after you establish a remote control session to an endpoint.

Command	Description	Syntax
help	Displays the help information for the available commands in the remote control mode.	help help <command_name> Example: help copyscreen
press	Presses one or more buttons on the endpoint.	press <#> press <#,#,...> Where, replace # with the button labels. Examples: press speaker press 1,2,3,4
ledstatus	Retrieves and displays the status of LEDs of the endpoint. For the LED buttons, the status can be one of the following: • ON • OFF	ledstatus

Command	Description	Syntax
list-buttons	Displays the list of available buttons on the endpoint.	list-buttons
call	Makes a call to a destination telephone number you specify for a specified duration.	call<phonenumber> <call_duration> Where, the call duration is in seconds. Example: Call121051 60
terminate	Ends an active call on the remotely controlled endpoint.	terminate
answercall	Answers an incoming call at the remotely controlled endpoint.	answercall
copyscreen	Retrieves a screenshot of the latest display on the endpoint. The system saves the image of the phone screen at the location that you pass as a parameter to the command.	copyscreen file:// <file_path_to_save> Example: copyscreen file://root/ phone_displays/ test20Mar9670.png
exitremotectl	Exits the remote control session.	exitremotectl

Initiating a call remotely using CLI of SLA Mon Server

About this task

Use this procedure to make a call remotely using the SLA Mon Server CLI.

Procedure

1. On the CLI prompt for SLA Mon Server, run the following command to start a remote control session to the agent:

```
agent <IP|MAC|extension of the agent>
```

The system starts the remote control session and displays the extension of the agent in the CLI prompt. After you establish a remote control session to an Avaya endpoint, a new set of CLI commands becomes available. You can now use these commands to remotely control the activities on the endpoint.

2. Run the following command to make a call from the remotely controlled endpoint agent to another telephone number:

```
call <Telephone number of the destination> <call duration in seconds>
```

The system ends the call after the specified duration.

3. To end an active call, run the **terminate** command.

Answering a call coming to a remotely controlled endpoint through CLI of SLA Mon Server

About this task

When you are remotely controlling an endpoint through CLI of SLA Mon Server, use this procedure to answer an incoming call to the endpoint.

Procedure

1. On the CLI prompt for SLA Mon Server, run the following command to start a remote control session to the agent:

```
agent <IP|MAC|extension of the agent>
```

The system starts the remote control session and displays the extension of the agent in the CLI prompt.

2. Run the following command to view the LED status on the endpoint:

```
ledstatus
```

For an incoming call, the LED status for a call line shows `BLINKING`.

Note:

Blinking LED status is not available for Avaya SIP endpoints.

3. Run the following command to answer the incoming call:

```
answercall
```

The remotely controlled endpoint attempts to answer the call. If the system establishes the call, the CLI prompt displays the `Incoming call answered` message.

4. To end the call from the remotely controlled endpoint, run the **terminate** command.

Pressing buttons on an endpoint remotely controlled by CLI

About this task

Use this procedure to press one or more buttons on a remotely controlled endpoint using the SLA Mon CLI.

Procedure

1. On the CLI prompt for SLA Mon Server, run the following command to start a remote control session to the Avaya endpoint:

```
agent <IP|MAC|extension of the agent>
```

2. Run the following command to list the buttons available on the endpoint:

```
list-buttons
```

3. Run the following command to press one button on the endpoint:

```
press <button_label>
```

Example: **press speaker**

The speaker on the physical endpoint is on.

4. Run the following command to press more than one buttons on the endpoint:

press <button_label,button_label,button_label,...>

Example: **press 1,2,3,4**

The endpoint dials the number 1234.

Getting a screenshot of the current display on an endpoint

About this task

If you cannot use the SLA Mon web interface, use this procedure to retrieve a screenshot of the latest display on an Avaya endpoint through CLI.

Procedure

1. On the CLI prompt on the SLA Mon server, run the following command to start a remote control session to the endpoint:

agent <IP|MAC|extension of the agent>

2. Run the following command:

copyscreen file://<file_path_to_save>

Example: **copyscreen** file://root/phone_displays/test20Mar9670.png

The system retrieves the screenshot of the latest display on the endpoint and saves the image as the file specified in the folder path.

Monitoring events on an endpoint through CLI

About this task

Use this procedure to monitor the events on an Avaya endpoint using the SLA Mon Server CLI.

Procedure

1. On the CLI prompt for SLA Mon Server, run the following command to view the agents registered with SLA Mon Server:

list agents

2. Run the following command to start monitoring the events on an endpoint agent:

enable eventmon <IP|MAC|extension of the agent>

The system starts monitoring the events on the specified endpoint and displays the events on CLI.

Stopping event monitoring through CLI of SLA Mon Server

About this task

Use this procedure to stop the event monitoring on a remotely controlled Avaya endpoint using the SLA Mon Server CLI.

Procedure

1. On the CLI prompt for SLA Mon Server, run the following command to view the agents that SLA Mon Server is currently monitoring:

```
list eventmon
```

2. Run the following command to stop monitoring the events on an endpoint agent:

```
disable eventmon <IP|MAC|extension of the agent>
```

Making bulk calls from CLI

About this task

Make sure that an SLA Mon agent is present in the firmware of the Avaya endpoint from where you want to make the call. However, the receiving telephone does not require to have an SLA Mon agent.

Using CLI of SLA Mon Server, you can make bulk calls from more than one endpoints to other telephone numbers at one time.

Procedure

1. Log on to Avaya Diagnostic Server as a user with administrative privilege.
2. Create a new text file using a text editor.
3. In the file, enter each pair of source and destination telephone numbers to be used for making bulk calls as new line items. Create file as following:

```
<extension of caller agent1>,<extension|phone number of receiver1>  
<extension of caller agent2>,<extension|phone number of receiver2>
```

Example:

```
210101,210104
```

```
210105,8910
```

4. Save the file.
5. Start the CLI session for SLA Mon Server.
6. Run the following command to make the bulk calls:

```
execute -bulk call file://<file-path> [call_duration]  
[call_answer_duration]
```

Where, replace <file-path> with the absolute file path of the text file you created. The call_duration and the call_answer_duration parameters are optional and in

seconds. The default value for `call_duration` is 300 seconds and `call_answer_duration` is 7 seconds.

For example, if you saved the file as `bulkcall.txt` in the `/root/temp` directory, run the command as the following:

```
execute -bulk call file:///root/temp/bulkcall.txt
```

SLA Mon Server tries to make calls from the caller agents listed in the file to the receiver telephone numbers.

7. Run the following command to end bulk calls before the specified duration:

```
execute -bulk terminate
```

Chapter 11: Packet capture

Packet capture overview

Packet capture is the process of capturing network traffic over the network. The SLA Mon agent on Avaya endpoints can send a copy of all packets that the endpoint sends and receives to the server in real time. The packet capture feature is useful in servicing Avaya endpoints. Service engineers can analyze the packets flowing in and out of Avaya endpoints on a customer network for diagnostic and troubleshooting purposes.

For you to be able to capture packets that an Avaya endpoint sends and receives, the endpoint must meet the following criteria:

- The packet capture feature is enabled on the agent.
- The agent is registered with the SLA Mon server.

You can run packet capture on multiple agents through the SLA Mon web interface and command line interface (CLI). The capture of in call packets does not make any noticeable impact on the regularity of the media stream.

The data captured during a packet capture session is saved as a Pcap file. You can download the Pcap files through the SLA Mon web interface for analysis. The Pcap files are compatible with Wireshark and Avayashark.

You can run a maximum of five concurrent packet capture sessions using the web interface and CLI. The captured packets are available in the system for 90 days. The system stores the latest five capture instances of each agent.

Packet capture through the SLA Mon web interface

Starting a packet capture session through the SLA Mon web interface

Before you begin

Ensure that the SLA Mon agent is configured on the Avaya endpoint from which you want to capture the packets.

Ensure that the agent is registered with the SLA Mon server. If the agent is not registered with the server, you can run the agent discovery process to discover and register the agent.

About this task

Use this procedure to start a packet capture session on an Avaya endpoint through the SLA Mon web interface.

Procedure

1. On the SLA Mon web interface, click **ENDPOINT DIAGNOSTICS > PACKET CAPTURE**.
2. If you have the IP address, extension, or MAC address of the agent, type the value in the **IP/Extn./MAC** field, and click **Add Agent**.

The system adds the agent to the table in the Agent Working Set section.

3. If you do not have the agent details, perform the following actions:
 - a. Click the **Search** icon beside the **IP/Extn./MAC** field.
 - b. In the Agent Search dialog box, enter one or more search criteria in the respective fields, and click **Search**.
 - c. From the search results, select the agent for which you want to start a packet capture session, and click **Continue**.

The system adds the selected agents to the table in the Agent Working Set section.

4. From the agents table in the Agent Working Set section, select the agent for which you want to start a packet capture session.

You can select one or more agents from the table.

5. Click **Start Capture**.

The Packet Captures section displays the progress and other details of the packet capture instances that run on the selected agents.

6. Click **Refresh** to display the latest details of the packet capture instances.

Note:

A packet capture session runs for approximately 60 seconds. To capture packets for longer duration, run another packet capture session on the agent.

7. **(Optional)** To stop a packet capture session before 60 seconds, click **Stop Capture**.

The packet capture session stops. The table in the Packet Captures section is refreshed to display the final details of the capture instance.

Important:

When you click **Stop Capture**, the system stops all active packet capture sessions. Although the normal capture duration is approximately 60 seconds, the captured packets take approximately two minutes to reach the SLA Mon server. However, the amount of time an agent takes to transfer all the captures to the server might vary. Click **Refresh**

repeatedly to update the capture details. If the packet count and file size details remain the same after clicking **Refresh**, the capture process is complete.

Related Links

[Packet Capture field descriptions](#) on page 107

[Discovering SLA Mon agents](#) on page 55

Packet Capture field descriptions

Agent Working Set section

The Agent Working Set section lists all the available agents for packet capture. You can start and stop a packet capture session from the Agent Working Set section.

Name	Description
IP/Extn./MAC	An input field for entering the IP address, extension number, or MAC address of an agent.
Select	A check box to select the corresponding agents.
Agent IP	The IP address of an agent.
Extn	The extension number of the Avaya endpoint where the agent resides.
Gateway	The network gateway details of the agent.
Type	The type of the agent, usually SLA MON.

Icon	Name	Description
	Add Agent	Adds the agent specified in the IP/Extn./MAC field.
	Remove	Removes selected agents from the Agent Working Set table.
	Search	Opens the Agent Search dialog box where you can specify criteria to search agents.
	Start Capture	Starts packet capture sessions for the selected agents.
	Stop Capture	Stops all active packet capture sessions.
	Select All	Selects all agents in the list.
	Clear All	Clears the selection of agents in the list.

Packet Captures section

The Packet Captures section displays the details of the completed and in progress packet capture sessions. You can refresh, delete, display, and download the capture instances available in the Packet Captures section.

Name	Description
Select	A check box to select the corresponding capture instance.

Name	Description
ID	The index number assigned to the packet capture instance of the agent.
Agent IP	The IP address of the agent.
Start Time	The start time of the capture instance.
Last update	The last time the details of the packet capture instance was updated.
Packet count	The number of packets captured during the capture instance.
File Size (bytes)	The file size of the captured data in bytes.

Icon	Name	Description
	Refresh	Refreshes the packet capture details in the table.
	Delete	Deletes the selected packet capture instances.
	Get All Captures	Displays all stored capture instances along with the listed instances. * Note: The system stores packet capture data for 90 days. The system also stores the last five capture instances for each agent.
	Download	Downloads a selected capture instance to a file on the local machine. This icon is available only when you select a packet capture instance.

Downloading captured packets through the SLA Mon web interface

About this task

Use this procedure to download the captured data from a packet capture instance to your local machine using the SLA Mon web interface.

Procedure

1. On the SLA Mon web interface, click **ENDPOINT DIAGNOSTICS > PACKET CAPTURE**.
2. In the Packet Captures section, select the packet capture instance that you want to download.

The **Download** icon becomes available.

3. Click **Download**.

The system displays the File Download dialog box.

4. Click **Save** to save the data file of the capture instance to your local computer.

The system saves the captured data to the specified path on your local computer as a .pcap file.

*** Note:**

You can use Wireshark or Avayashark to open the .pcap file and analyze the captured data packets.

Packet capture through the SLA Mon CLI

Starting a packet capture session through CLI

Before you begin

Make sure that the SLA Mon agent is configured on the Avaya endpoint from which you want to capture the packets.

Ensure that the agent is registered with the SLA Mon server. If the agent is not registered with the server, you can run the agent discovery process through CLI to discover and register the agent.

About this task

Use this procedure to start a packet capture session on an Avaya endpoint through the SLA Mon server CLI.

Procedure

1. Log on to the Avaya Diagnostic Server host as a privileged user, and start an SLA Mon CLI session.
2. On the CLI prompt, run the following command to start a packet capture session for an endpoint:

```
enable sniffer <ip-address|extension|mac-address>
```

Where, replace <ip-address|extension|mac-address> with the IP address, the extension number, or the MAC address of the endpoint for which you want to capture packets.

For example, if you want to capture packets to and from the extension number 67890, run the command as the following:

```
enable sniffer 67890
```

The system starts capturing the packets sent and received by the specified agent.

*** Note:**

The system runs a packet capture session for approximately 60 seconds. To capture packets for longer duration, run another packet capture session on the agent.

3. Run the following commands to view the details of the capture instances that are complete or in progress:

- To list the capture instances of an agent:

```
list sniffer <ip-address|extension|mac-address>
```

The system displays the details of the packet capture instances available for the specified agent. The system stores the latest five capture instances for an agent.

- To list all available capture instances:

```
list sniffer
```

The system displays the details of all available capture instances. The system retains capture instances up to 90 days.

+ Tip:

Run the **list sniffer** command repeatedly during an active packet capture process to view the latest packet counts and file size of the capture instance. If the details of the capture instance remain unchanged even after running the **list sniffer** command repeatedly, the packet capture process is complete.

4. Run the following command to stop a packet capture session before the normal duration of 60 seconds:

```
disable sniffer <ip-address|extension|mac-address>
```

Where, replace <ip-address|extension|mac-address> with the IP address, the extension number, or the MAC address of the endpoint for which you want to stop the packet capture session.

The system stops packet capture for the specified agent.

Related Links

[Discovering SLA Mon agents through CLI of the SLA Mon server](#) on page 82

[Starting a CLI session on the SLA Mon server](#) on page 76

[Downloading captured packets through CLI](#) on page 110

Downloading captured packets through CLI

About this task

Use the following procedure to download and save a packet capture instance in a specific location for packet analysis.

Procedure

1. On the CLI prompt for the SLA Mon server, run one of the following commands as appropriate:
 - To list the capture instances of an agent:

```
list sniffer <ip-address|extension|mac-address>
```

The system displays the details of the packet capture instances available for the specified agent. The system displays the latest five capture instances for an agent.

- To list all the available capture instances:

```
list sniffer
```

The system displays the details of all available capture instances. The system retains capture instances up to 90 days.

2. Run the following command to download a capture instance of an agent:

```
copy sniffer <ip-address|extension|mac-address>  
<captureInstanceindex> file://<file-path>
```

Where, replace <ip-address|extension|mac-address> with the IP address, the extension number, or the MAC address of the endpoint for which you want to download the packet capture instance. Replace <captureInstanceindex> with the index number of the capture instance. Replace <file-path> with the absolute path and the file name where you want to save the .pcap file.

Example:

```
copy sniffer 1234 2 file://root/captures/A1234Apr9.pcap
```

The system downloads the captured packets to the specified location.

Removing packet capture instances through CLI

About this task

Use this procedure to remove packet capture instances. When you remove a packet capture instance, the system deletes the captured data from the SLA Mon server.

Procedure

1. On the Avaya Diagnostic Server host, start an SLA Mon CLI session.
2. On the CLI prompt, run the following command to remove all packet capture instances of an agent:

```
remove sniffer <ip-address|extension|mac-address>
```

Where, replace <ip-address|extension|mac-address> with the IP address, the extension number, or the MAC address of the deskphone for which you want to remove the sniffer.

Example:

```
remove sniffer 67890
```

3. Run the following command to remove a specific packet capture instance of an agent:

```
remove sniffer <ip-address|extension|mac-address>  
[captureInstanceId]
```

Where, replace <ip-address|extension|mac-address> with either the IP address, extension number, or MAC address of the deskphone, and replace [captureInstanceId] with the index number of the capture instance you want to remove.

Example:

```
remove sniffer 67890 3
```

4. Run the following command to remove all packet capture instances:

```
remove sniffer all
```

When you run the **remove sniffer** commands, the system prompts you to confirm the remove action.

Type **y** to confirm the remove action.

Chapter 12: Network Monitoring

Overview

The Network Monitoring features provide vendor agnostic, end-to-end network insight into conditions that might have an impact on your voice, video, and data applications. The feature provides an easy-to-understand visual representation of your network performance data. Using the network performance and call-trace data, you can proactively identify and troubleshoot network issues.

The Network Monitoring feature displays the results of the network performance tests that the SLA Mon server runs between source and destination test endpoints on the network. The test pattern that you configure and run through the SLA Mon web interface controls the nature of the test calls. Based on the Quality of Service (QoS) levels or thresholds that you configure for each traffic type, the SLA Mon server analyzes the test results for each source-destination pair. Based on the analysis, the Network Monitoring feature presents the network performance information using colored grids and graphs.

Related Links

[Test patterns](#) on page 83

[Changing the thresholds of the QoS parameters](#) on page 68

Network Summary page

On the Network Summary page, you can view real-time traffic performance between selected sites in your network. The page displays the performance data based on the traffic type and the network performance parameter that you select. The following sections explain the features on the page in detail.

The summary grid



Figure 1: Network Summary grid

The colored grid represents the network performance between selected sites in your network for a selected traffic type and a selected network performance parameter. By default, the summary grid displays the performance results of the audio traffic for the packet loss parameter. Also, the default grid displays the zones and locations that are at the top level. The grid represents the traffic performance for selected sites in the following way:

- Each row represents the outgoing connections of a site *to* the other sites in the grid.
- Each column represents the incoming connections to a site *from* the other sites.
- Each row has the site name and a number as the label of the row. The same numbers represent the site names along the top of the grid.
- Each cell in the grid represents an outgoing or incoming network performance between two sites.

For example, row 3 in the figure represents a location in Bangalore, India. When you move from left to right, each cell represents the outbound traffic performance from the Bangalore location to other sites on the grid. In column 3, each cell from top to bottom represents the incoming traffic performance from other sites on the grid to the Bangalore location.

The colored cells in the grid indicate the performance of your network. From the color of the cells, you can determine whether the network is performing within the threshold limits or has exceeded certain threshold limits. The following table explains what each color represents:

Color	Description
 Green	Indicates that traffic is moving from the source to the destination without encountering any error conditions. All tests in the past hour are within the threshold, indicating good network condition.
 Amber	Indicates that no error condition is encountered in the last test, but the traffic condition deteriorated at some points in the past 1 hour. Therefore, Amber indicates that the network has recovered but might require attention.
 Red	Indicates that the value of the selected performance parameter exceeded the threshold in the last test, and the network condition is poor.
 Black	Indicates that no data is available for the past 1 hour. Unavailability of test data means that the SLA Mon server administered a test pattern but could not run the tests, probably because of agent issues. Another reason for data unavailability might be a server and agent connectivity issue.
 Blue	Indicates intrazone cells that represent the relationship of a zone to itself. When you click an intrazone cell, the page refreshes to display the performance grid for all locations within the zone.
 Grey	Indicates that the SLA Mon server has not administered a test pattern for this location pair in the past hour.
White	Represents relationship of a location to itself.

Traffic and parameter options

Name	Description
Traffic	The traffic types whose network performance you can view. You can select one of the following traffic types: • Audio • Video • Data
Parameter	The parameters based on which the SLA Mon technology measures the network performance. You can select one of the following parameters to view the network performance based on that specific parameter: • Remarking: Changes in Differentiated Services Code Point (DSCP) markings en route might cause occasional call drops and unintelligible speech. Unexpected DSCP values result in inconsistent call quality. Probable causes of unexpected DSCP values might be incorrect configuration of routers and no Quality of Service (QoS) control on one or more routers. In the grid, Red indicates that the DSCP values of the RTP packets were changed en route from source to destination. • Loss: The voice quality problems that you might observe because of packet loss are call drops and unintelligible speech. A probable cause of packet loss might be that routers on the path are overloaded. Remarking problems also can cause packet loss.

Name	Description
	In the grid, Red indicates that the recent value of the parameter crossed the configured threshold. Amber indicates that at some point in the past 1 hour, the value of the parameter crossed the configured threshold. However, the recent value is within the threshold. • Jitter: The voice quality problems that jitter might cause are identical to packet loss. • Delay: Delay might cause frequent talk-over during calls where one listener starts talking before the previous speaker has finished talking. Probable causes of delay might be slow routers, long complicated router paths, or geographical distance. • e-MOS: Estimated mean opinion score (e-MOS) is a summary of the combined effects of delay, jitter, and loss. • Alarms: This parameter indicates whether a site is raising alarms for any condition that might affect network performance. Red indicates that the site sent SNMP traps to configured destinations, such as Avaya and customer NMS, when a QoS parameter crossed the configured threshold. • Misordered: Misordered is an anomaly where packets arrive at an agent out of order. Misordered packets are unlikely to cause any problems but might cause increased jitter. Some probable causes are multiple routes in the network, route flapping, that is routing algorithm instability, or an unreliable router rebooting. Red indicates that misordered packets were present in the traffic between the two sites. • Duplicate: Duplicate is an anomaly when multiple identical packets arrive at an agent. Duplicate packets are unlikely to cause any problems. Some probable causes are multiple routes in the network, route flapping, or an unreliable router rebooting. Red indicates that duplicate packets were present in the traffic between the two sites. • Failed: This parameter indicates connection issue with a site. Red indicates a problem with the Avaya device, such as agent down or loss of connectivity from the server to agent on the network.

The Selector pane

The Selector pane displays the locations and zones in the network in a tree structure. To see the location selector pane, you must click **Selector** in the upper-left corner of the page. The tree structure organizes the zones and locations in the following way:

- The zones are at the first level in the tree.
- If a location is part of a zone, the location is under the zone at the second level in the tree.

- If a location is not part of any zone, the tree displays the country in which the location is situated at the first level.
- If a location has multiple subnets, the tree displays the subnets at the sublevel under the location.

Check boxes are available beside each location in the tree. The grid changes according to the locations and zones that you select in the tree.

Viewing the network summary for a traffic type and a performance parameter

About this task

You can view the network performance summary of a selected traffic type for a selected parameter.

Procedure

1. On the SLA Mon web interface, click **NETWORK MONITORING**.
2. From the **Traffic** types, select one of the following options:

- **Audio**
- **Video**
- **Data**

The grid is refreshed to display the results of the selected traffic type.

3. From the **Parameter** options, select one of the following network parameters:

- **Loss**
- **Jitter**
- **Delay**
- **e-MOS**
- **Alarms**
- **Protection**
- **Remarking**
- **Misordered**
- **Duplicate**
- **Failed**

The grid is refreshed to display the results for the selected parameter.

Related Links

[Network Summary page](#) on page 113

Viewing network summary based on selected zones and locations

About this task

You can select specific zones and locations to view the network performance between the selected sites.

Procedure

1. On the SLA Mon web interface, click **NETWORK MONITORING**.
2. Click **Selector**.

The system displays the location selector pane with the locations and zones in the network in a tree structure. All zones and locations at the top level are selected by default, and the grid accordingly displays the performance summary for the top-level sites.

3. Expand the zones and locations at the top level to view the locations at the next level.
4. To select a particular site, select the check box beside the site.
5. To remove a site from the network summary grid, clear the check box beside the site.

Result

The grid is refreshed to display the performance results of the selected sites.

Related Links

[Network Summary page](#) on page 113

Viewing the intrazone network summary grid

About this task

Use this procedure to view the network relationship between the locations within a zone. The default summary matrix displays the network relationship of a zone to other locations and zones at the top level.

Procedure

1. On the SLA Mon web interface, click **NETWORK MONITORING**.
2. In the grid, find the intrazone cell that represents the relationship of a zone to itself.

Blue indicates the intrazone cells, and you can find the intrazone cells when you move diagonally from left to right on the grid.

3. Click the intrazone cell.

The grid is refreshed to display the performance summary for the locations within the zone. In the location selector pane, the tree structure changes to display the location tree for the zone.

Viewing the network performance graphs between two locations

About this task

From the network summary grid, you can further analyze the detailed test results between two locations. Use this procedure to view the statistical and graphical representation of network performance between two locations.

Procedure

1. On the SLA Mon web interface, click **NETWORK MONITORING**.
2. Expand the tree in the location selector pane, and select the sites for which you want to view the detailed performance results.
3. In the grid, find the cell that represents the relationship between the two locations, and click the cell.

The Chart Detail page opens in a new window. The page displays the test results between the two sites through graphs and tables.

4. To view the performance graphs for a specific time frame, perform the following tasks:
 - a. Enter the time frame in the **Start Date Time** and **End Date Time** fields.
 - b. Click **Update**.

You can select a time frame of maximum 5 days and minimum 5 minutes. You can view historical test data of maximum 60 days.

If the disk space usage reaches 80% and above, the SLA Mon server deletes the oldest one day data from the SLA Mon database.

For example, if you have not used hard disk drive size as recommended and the disk space usage reaches above 80% with data of 40 days only, then the SLA Mon server deletes the oldest one day data to reuse space from the database and thus always maintains historical data of 40 days.

5. To view the performance graphs of a specific parameter, select a parameter, and click **Update**.

Related Links

[Chart Detail page](#) on page 119

Chart Detail page

When you click a grid cell on the Network Summary page, the Chart Detail page displays the performance measures between the two sites that the cell represents. You can view the network performance of all types of traffic traversing both directions, from source to destination and vice

versa. The page contains tables and graphs to represent the network performance for a selected period.

Performance measurement tables

The first table contains the performance measures for traffic from the originating site to the destination. The second table contains the performance measures for traffic to the originator site. The tables contain the measures of the following performance parameters for audio, video, and data traffic:

- Loss
- Jitter
- Delay
- e-MOS
- Alarms
- Remarking
- Misordered
- Duplicate
- Failed

For each traffic type, the table displays the following performance measures of each parameter:

- The last value recorded for the parameter in the selected period.
- The maximum or the minimum value recorded for the parameter in the selected period.

QoS performance graph



The graphs display performance of all three traffic types, voice, data, and video. The first graph displays the performance of traffic from the source to the destination. The second graph displays the performance of returning traffic from the destination to the source. In the graph, you can distinguish each traffic type by the color used to represent the traffic type. For each traffic type, a colored dotted line matching the color of the traffic type marks the threshold value in the graph.

The graphs change according to the options that you select. You can:

- View the traffic performance of a selected parameter. The graph also displays the threshold for the selected parameter as dotted lines for each traffic type.
- Select or remove a traffic type from the graph. By default, the graph displays all three traffic types.
- Change the time frame for which you want to view the performance data.
- Zoom in to a particular section of the graph.

When you keep the cursor at a specific point on the graph, the DSCP Details tables display the DSCP results of that particular time represented in the graph.

DSCP Details tables

The DSCP Details tables display the hop-by-hop DSCP marking results for traffic traversing both directions. The table is refreshed to display the DSCP results at a particular time based on the position of the cursor on the graph.

*** Note:**

Through DSCP markings, the SLA Mon server assigns a priority marking to packets for time-sensitive data, such as voice and video. When the marking at the final and the initial hop is the same, the priority is maintained even if the marking changes on the way. If the marking is not the same at the final hop as at the initial hop, then QoS is not maintained.

The following table describes the data that each column represents in the DSCP Details table.

Column	Description
Hop #	The sequential number assigned to each hop that the traffic encounters.
Audio Path	The IP address of each hop that the audio traffic encounters.
Audio Marking	The DSCP value for audio traffic at each hop.
Data Path	The IP address of each hop that the data traffic encounters.
Data Marking	The DSCP value for data traffic at each hop.
Video Path	The IP address of each hop that the video traffic encounters.
Video Marking	The DSCP value for video traffic at each hop.

Chart Detail page field and button descriptions

Name	Description
Start Date Time	The start time and date of the time frame for which you want to view the performance results. You can view performance results of maximum 5 days and minimum 5 minutes.
End Date Time	The end time and date of the time frame for which you want to view the performance results.
Parameter	The parameters for which you can view the detailed graph. You can select one of the following parameters at one time: • Loss • Jitter • Delay • MOS • Misordered • Duplicate
Audio	The check box to indicate whether you want to view the audio traffic performance on the graph.
Video	The check box to indicate whether you want to view the video traffic performance on the graph.
Data	The check box to indicate whether you want to view the data traffic performance on the graph.

Button	Description
Update	Refreshes and displays the results of the network performance tests for the selected time frame, parameter, or traffic types in the graphs and tables.

Chapter 13: Troubleshooting

Agents stop responding to commands, and “BAD_KEY” errors are seen in any of the /var/log/slamon/* log files

Problem

The agent registration process involves an encryption key exchange over an Avaya certificate authenticated SSL/TLS connection as well as a capabilities information exchange over UDP. The key is used to encrypt all future communication between the server and the agent. The agent initiates this key exchange only at a maximum rate of once every 10 minutes, that is, if a secondary discovery is done again within 10 minutes of a previous discovery, no second key exchange will take place. This does not normally cause any issues, but there is a small possibility of this problem occurring after server restarts when a discovery was run within 10 minutes of the restart, or other unusual combinations of discovery, server restarts and agent restarts or lost network connections.

Workaround

Stop using the CLI and Web UI for at least 10 minutes, and then run a discovery again either using the Web UI or CLI.

Tests failing, or remote control and packet capture not working after successful discovery

Even after a successful discovery of some agents, tests fail, or the remote control and packet capture features do not work for the agents. The reason could be missing certificate or mismatch of certificate. You must ensure that the server-agent certificate is administered in the SLA Mon server keystore and on the Avaya products where the agent resides.

Resolution

Procedure

1. On the SLA Mon server host, check if the server keystore has the server certificate with the alias `slamon-keyserver`:

```
keytool -v -list -keystore /opt/avaya/slamon/bundleconf/ces.jks -  
alias slamon-keyserver -keypass <keystore_password> -storepass  
<keystore_password>
```

Where, replace <keystore_password> with the password you administered for the SLA Mon server keystore.

2. Ensure that the owner CN of the server certificate is `SLA Monitor Server`.
3. Check whether the root certificate is administered on the product where the agent resides.
4. If the root certificate is not administered for the agent, administer the certificate.

For more information about administering certificates, see Chapter 6, Managing certificates for the communication between the server and the agent.

Unable to remote control the 9641 SIP phones after a reboot

After a reboot of the 9641 SIP phones, remote control of the phones through Avaya Diagnostic Server does not work. Remote control of the phones works after you manually stop the test, rediscover the agents, and then start the test.

Resolution

Agents do not automatically reregister with the server after a restart, which is an expected behavior with the current design of Avaya Diagnostic Server. So the server has to rediscover them. If tests are running when the agent restarts, the server attempts to rediscover the agent after 20 failed tests. Rediscovery of agents by the server takes several minutes depending on the test pattern. You can see the agent reregistered and ready for use in diagnostics again after some time.

You can manually stop any running tests, rediscover the agent, and then start the test again.

FAQs

Q

How does SLA Mon Server uses the subnet information on the Agent Discovery page?

A:

SLA Mon Server uses the subnet information on the Agent Discovery page only during agent discovery. SLA Mon Server does not use it again for any other purpose, except during a manual rediscovery. SLA Mon Server does not use the subnet from the Agent Discovery page for automatic

rediscovery. Instead, SLA Mon Server uses the address and subnet mask of an agent to try to find agents in the same subnet.

A user can initiate a rediscovery manually and can select on which address ranges to run discovery again. Therefore, if the user does not wish to run a discovery over one of the address ranges again, then they should not select that address range in the list. The server also automatically re-runs a discovery if agents at a site start failing. This is the only reason why the server needs to keep the data on the Agent Discovery page. If the user wishes to change the location of an agent, they should edit the existing address range and rediscover the agents in that address range.

Q

If you update the location information on the Agent Discovery page after a discovery, will the location information associated with the discovered agents also change?

A:

Updating the location information on the Agent Discovery page after a discovery makes no difference to an agent location until you run the discovery process again.

Q

How do you stop using a subnet in the test patterns?

A:

To stop using a subnet in the test patterns, you can go to the Test Agents page and use the arrow buttons to move the subnet from the **Selected** list to the **Available** list.

Q

Where are the log files for SLA Mon stored?

A:

The log files for SLA Mon are stored in the `/var/log/eqm` directory.

Q

Is the output from the install and the uninstall scripts saved anywhere?

A:

Yes, the results from the install and the uninstall scripts are stored in `/tmp/slamon-install.log` and `/tmp/uninstall.log` respectively.

Q

How long do we store test results from agents?

A:

We retain test data that are maximum two days old in the SLA Mon database. A background process runs periodically to remove test results older than two days.

Q

Why cannot I find a particular city in the selection box on the Agent Discovery page?

A:

To keep the size of the database reasonable and the installation time as short as possible, the City options are limited based on population. First, make sure that you have selected the correct Country and State values. If you still do not see the city you are looking for, select the best nearby city presented in the list. You may submit a request through Avaya support channels to add a particular city to the list, but the new addition process might take a few days. Therefore, selecting an alternate city is your best short term solution.

Q

Why does not an agent respond to a registration request?

A:

There might be several reasons for this problem. Assuming that the agent is installed and operational, which is not covered in this guide, there might be two reasons why the agent would not respond to a registration request. First, if the agent has recently (within the past 5 to 10 minutes) been discovered by the SLA Mon Server, the agent will not respond to another request. Only after a period of no registration, the agent responds to the server to which the agent is registered. The second reason is that the agent might be registered to another server. In this case, you should check any other SLA Mon Servers to see if the agent in question is in fact registered to the server. If the agent is registered to another server, remove the agent from any tests on your server. After a period of about 10 to 15 minutes of no activity, the agent should be available to be registered to another server.

Q

What happens to agents when you uninstall?

A:

A deregister command is sent to all registered agents when you uninstall the application, immediately freeing the agents for use by another SLA Mon Server.

Appendix A: Alarms that the SLA Mon server generates

The SLA Mon server generates a number of alarms in the form of SNMP traps to report events. The server sends the alarms to the configured SNMP trap receivers.

The SLA Mon server Object ID (OID) is .1.3.6.1.4.1.6889.2.62. The following table provides the details of the alarms that the SLA Mon server generates.

Alarm type	Alarms	OID	Description
License alarms	avSLAMonLicenseTrap	.1.3.6.1.4.1.6889.2.62.1.2.0.4.0.15	Generates this alarm when the SLA Mon license state is expired or in grace period. The following are the license states for which the server raises this alarm: • If the grace period expires in a week. • If the license state of the diagnostics or the monitoring feature is expired. • If the license state of the diagnostics or the monitoring feature expires in a week. The frequency of the alarm is once a day until the license is renewed.
	avSLAMonLicenseServerNotReachableTrap	.1.3.6.1.4.1.6889.2.62.1.2.0.4.0.16	Generates this alarm when the SLA Mon server is not able to reach the WebLM server. Frequency of the alarm is once a day until the WebLM server is reachable.
QoS alarms	avSLAMonTrapQoSJitter This alarm is for jitter.	.1.3.6.1.4.1.6889.2.62.1.2.0.2.0.7	Generates a QoS alarm if the number of test responses for a QoS parameter that exceed the configured threshold in the last 1 hour is N or greater. N is the configured strike rate for the QoS parameter.
	avSLAMonTrapQoSDelay This alarm is for delay.	.1.3.6.1.4.1.6889.2.62.1.2.0.2.0.8	
	avSLAMonTrapQoSPacketLoss	.1.3.6.1.4.1.6889.2.62.1.2.0.2.0.9	After the server raises a QoS alarm for a subnet, the server does not generate the same QoS alarm until the network

Alarm type	Alarms	OID	Description
	This alarm is for packet loss..		condition changes. If the QoS of the network deteriorates again after the network recovers from the earlier state, the SLA Mon server raises the next QoS alarm.
	avSLAMonTrapQoSSEMOS This alarm is for e-MOS.	1.3.6.1.4.1.6889.2.62.1.2.0.2.0.10	For more information about configuring thresholds and strike rates, see the Configuring alarming properties section in this guide.
Start or Stop alarms	avSLAMonServiceColdStart	1.3.6.1.4.1.6889.2.62.1.2.0.1.0.2	Generates this alarm when a user starts the SLA Mon server using the <code>service slamonsrvr start</code> command.
	avSLAMonServiceStopped	1.3.6.1.4.1.6889.2.62.1.2.0.1.0.3	Generates this alarm when a user stops the SLA Mon server using the <code>service slamonsrvr stop</code> command.
DSCP Change alarms	avSLAMonTrapDSCPChange	1.3.6.1.4.1.6889.2.62.1.2.0.2.0.11	Generates this alarm for a pair of subnets if the DSCP value changes from the source to the destination. The server compares the DSCP value at the first hop of the path a packet traversed between the subnets with the value at the last hop. If the values at both hops are not same, the server raises the alarm. The SLA Mon server does not generate a DSCP Change alarm for the next 1 hour for the pair of subnets. After 1 hour, if the DSCP values are still different at the first and the last hops, the server generates another DSCP Change alarm.
Test Failure alarms	avSLAMonTrapTestFailure	1.3.6.1.4.1.6889.2.62.1.2.0.2.0.12	Generates this alarm for a subnet if test calls to the subnet fails by more than 10% in the last 1 hour.
Agent Discovery alarms	avSLAMonTrapAgentDiscovery	1.3.6.1.4.1.6889.2.62.1.2.0.3.0.14	Generates this alarm if an agent does not respond to the agent discovery request.
Agent Registration alarms	avSLAMonTrapAgentRegistration	1.3.6.1.4.1.6889.2.62.1.2.0.3.0.13	Generates this alarm if an agent gets registered to the SLA Mon server successfully.
SNMP Configuration Change alarm	avSLAMonTrapConfigChange		Generates this alarm if any configuration parameters in the Administration pages of the UI is changed.

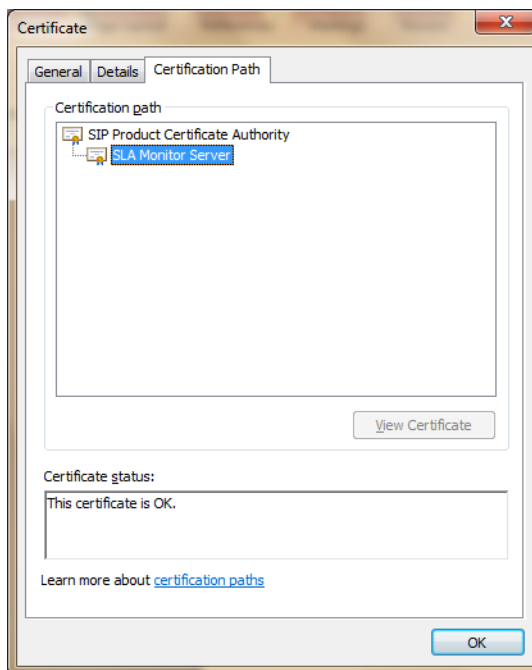
Appendix B: Additional certificate-related information

Viewing certificate properties

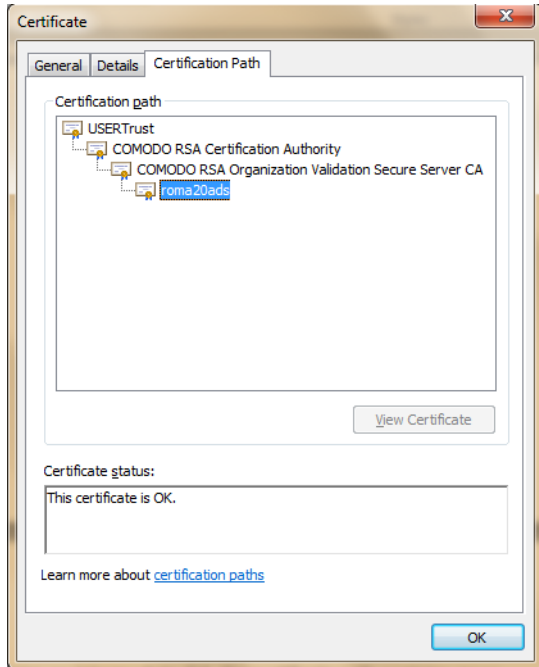
Procedure

1. Download the certificate from the link provided by the CA and store it on the desktop with a `.cer` extension.
2. Open the certificate, and click the **Certificate Path** tab to verify if the signed certificate contains an Intermediate CA.

The following image shows a sample certificate without Intermediate CA:



The following image shows a sample certificate with Intermediate CA:



If the signed certificate contains an Intermediate CA, the certificate path contains more than two entries as shown in the image.

Identify certificate chain

The Certificate Authority after signing the server identity certificate provides links to download the server identity certificate and the CA root certificate. The download link also contains a link to the certificate chain which has both the server identity certificate and the CA root certificate concatenated in a single file.

The following is an example of a link to a certificate chain:

X509 Intermediates/root only, Base64 encoded:
<https://certificate-authority.com/customer/test/ssl?action=download&sslId=368321&format=x509IO>

PEM/X509 format certificate

The PEM format certificate contains the information in the following format:

```
-----BEGIN CERTIFICATE-----
MIIE1DCCA7ygAwIBAgIBADANBgkqhkiG9w0BAQUFADBEMQswCQYDVQQGEwJVUzET
MBEGA1UEChMKQXZheWEgSW5jLjEaMBGGA1UECzMhZheWEgUHJvZHVjdCBQSQ0kx
```

```
HjAcBgNVBAMTFUF2YXlhIFByb2R1Y3QgUm9vdCBDQTAEFw0wMzA4MjIxMTI1MzZa
Fw0zMzA4MTQxMTI1MzZaMF4xCzAJBgNVBAYTA1VTMRMwEQYDVQQKEwpBdmF5YSBJ
bmMuMRowGAYDVQQLEExFBdmF5YSBQcm9kdWN0IFBLSTEeMBwGA1UEAxMVQXZheWEg
UHJvZHVjdCBSb290IENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
+EpellesygWvwACRNRh/6FbkPYDGrf5jppqIzgd3KG1w7gvvQ/ID953REm2DS7DEI
4y71+zY0MLtNv+I3rASpdxufsFwkHa5zR1FjpkiaP7XhMKXNpSY7No78rko9uiGt
xCx9VdW20kcP4IiEN23jQWfKjGFzkZItCl/aOf2+peh8bSS2MIprGx4rnCMZN1dU
Nnw8nJFGu7IxRlGDA2XqJ7BWBn/pvPMLdaVU60oI1/4IT9lHPUCaRVAC56jJdtxq
F9sNW0ZsBy05/vtopUiStfq8aMtMWCqGkSwjWB2VDWhWj6HTuGk27YsTsFIREJuT
i7rXYBQqRJN0o15aERM6BwIDAQABo4IBmzCCAzcwHQYDVR0OBBYEFMKatvFzIYIm
xz27CykJXlmexi5qREs+MLV0jrduRE50nTHMhkHKZBX7yKIgEb9GwQ==
-----END CERTIFICATE-----
```

Copying the CA root certificate installed on the SLA Mon server

Procedure

1. Run the **openssl** command as the following to display the certificate installed on the SLA Mon server:

```
openssl s_client -host <slamon_server_ip> -port 50011 -showcerts
```
2. From the command output, copy the last block of text that starts with BEGIN CERTIFICATE and ends with END CERTIFICATE.
3. Paste the content to a file, and copy the file to the required location.

The following is a sample output of the command with the last block that needs to be copied highlighted:

Additional certificate-related information

96x0 3.2.2 and later	Yes	No	The server certificate cannot have intermediate CA.
96x0 3.2.4 (Planned)	Yes	Yes	The 3.2.4 version supports server certificate signed by an Intermediate CA.
96x1 H.323 6.4	Yes	No	Server certificate cannot have intermediate CA
96x1H.323 6.6 (Planned)	Yes	Yes	
96x1 SIP 6.4 and earlier	Yes	No	
96x1 SIP 6.4.1 and later	Yes	Yes	
G450/G430 36.7 and earlier	Yes	No	Server certificate cannot have intermediate CA
G450/G430 36.8 and later	Yes	Yes	

Index

A

adding	
SNMP trap receiver	62
agent	
change status	59
agent search	
field descriptions	59
agent-server communication	
certificate usage	26
alarm ID	69
configure	68
Alarming tab	69
alarms	128
Avaya demo certificate	40

B

Branch Gateway	
import CA root certificate	
demo certificate	49
for self-signed server certificate	48
for signed server certificate	47

C

CA root certificate	
import to SLA Mon agents	32 , 40 , 41
certificate enrollment	
by signing authority or in-house CA	
prerequisite steps	28
certificate format	
PEM/X509	131
certificates	
methods to obtain	27
certificate signing request	30 , 38
certificate usage	
agent-server communication	26
change	
agent status	59
threshold values	68
change IP address of WebLM	20
change WebLM IP address	21
Chart Detail	119
CLI-based administration	76
configure	
alarm ID	68
configuring	
system properties	73
create	
self-signed certificate authority	35
zone	74
create CSR	30

for self-signed certificate	38
create server certificate	
SLA Mon server	29
create server identity certificate	
for self-signed certificate	36
CSR	30 , 38

D

delete	
packet capture instances	111
demo certificate	40
install on /SLA Mon server	40
discovering	
SLA Mon agent	55
document changes	8
document purpose	8
download data packets	
through CLI	110
download packets	
through web interface	108
DSCP details	119

E

enable SLA Mon agent	
on ERS 8800 and VSP 9000 switches	52
ERS 8800	
enable SLA Mon agent	52
export test pattern	86

G

graph, network performance	119
----------------------------------	---------------------

I

import CA certificate	
to SLA Mon agents	32 , 40 , 41
import CA root certificate	
on Media Gateway	47–49
import signed server certificate on SLA Mon server	31
import test pattern	87
initial administration	54
install demo certificate	40
install SLA Mon server license	18
intermediate CA support	133
intrazone summary grid	
view	118

L

license installation	
SLA Mon server	18

M

Media Gateway	
import CA root certificate	47–49

N

network monitoring	
overview	113
network performance between sites	
view	119
network summary page	113

O

obtaining certificates	27
overview	
network monitoring	113

P

packet capture	
download data through web interface	108
download through CLI	110
overview	105
start through CLI	109
start through web interface	105
Packet Capture page	
field descriptions	107
packet captures	
delete	111
PEM/X509	131
performance graph	119
phone remote control	
start phone remote control	
through CLI	98
start session through web interface	94
start through CLI	98

R

registering	
SLA Mon agent	55
related documentation	9
remote control not working on 9641 SIP phones	125
remove	
packet capture instances	111
rename	
zone	74

S

search	
agent	57, 58
self-signed certificate	33
create server identity certificate	36
self-signed certificate authority	
create	35
self-signed certificate creation	
prerequisite steps	33
self-signed server identity certificate	
install	39
server identity certificate	
create	29, 36
install signed certificate	31
SHA256 support	133
SLA Mon	
overview	11
security	13
SLA Mon administration	
CLI based	76
SLA Mon agent	
discovering	55
search	57, 58
SLA Mon server	
alarm ID	68
SLA Mon server license	
install	18
SLA Mon server licensing	18
SNMP trap receiver	
add	62
SNMP traps	64, 128
deleting	67
editing	67
SNMP Traps tab	63
start	
packet capture through CLI	109
packet capture through web interface	105
strike rate	69
change	
strike rate	69
subnet	
add to zone	75
summary grid	113
summary matrix	113
support	10
supported products	15
System Properties tab	73

T

Test Execution	91
test failure	
after successful discovery	124
test pattern	
add	83
delete	84

test pattern (<i>continued</i>)	
export	86
import	87
test patterns	
field descriptions	88
Test Setup tab	73
thresholds	69
change values	68

V

videos	10
view network summary	
for locations	118
for traffic type and parameter	117
for zones	118
intrazone	118

W

WebLM	
change IP address	20 , 21

Z

zone	
add subnet	75
create	74
rename	74