Deploying Avaya Diagnostic Server

Release 2.5
Issue 5
September 2016

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

Licenses

THE SOFTWARE LICENSE TERMS OR SUPPORT TOOLS LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, 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 each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of 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 EQUYIPMENT (E.G., SAL, SLA MON, AVAYA DIAGNOISTIC 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: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

Service Provider

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Contents

Chapter 1: Introduction

Purpose of the document

The guide provides information about the following:

- Overview of Avaya Diagnostic Server.
- Procedures for installing and uninstalling Avaya Diagnostic Server.
- Post-install validations and configuration for Avaya Diagnostic Server.

Intended audience

The audience for this document is anyone who installs and configures Avaya Diagnostic Server at a customer site. The audience includes and is not limited to implementation engineers, support personnel, and network engineers from Avaya, business partners, and customers.

New in this release

Avaya Diagnostic Server Release 2.5 is built on the previous release and has the following new features and enhancements:

Automatic Solution Element ID generation through the SAL Gateway UI

With Avaya Diagnostic Server Release 2.5, the SAL Gateway automatic Solution Element ID generation capability is now available through the SAL Gateway UI. The facility was until now available only in the attended mode of installation of SAL Gateway. The automatic Solution Element ID generation facility becomes available on the SAL Gateway UI only when you install SAL Gateway with the default ID.

Important:

For the SAL Gateway services to start, you must replace the default Solution Element ID with the correct ID.

Automatic software update enhancement

In Release 2.5, the automatic software update feature is enhanced. You can now apply a downloaded software update immediately or in the next available time frame through the SAL Gateway UI.

Ease of managed device administration on the SAL Gateway UI

The registration information of the products that are registered through Global Registration Tool (GRT) 4 for a designated SAL Gateway now becomes available to the designated SAL Gateway. Therefore, the SAL Gateway UI now automatically populates the available registration information of such a product in the device administration pages of the UI. With this enhancement, you need not manually enter the registration data on SAL Gateway, avoiding typographic errors and achieving better efficiency in the device onboarding process.

Agent-to-agent test support

On the SLA Mon server, you can now define and perform agent-to-agent tests, which is one level deeper than the subnet-to-subnet tests. Accordingly, the network summary matrix now displays the network performance data at the inter-subnet and intra-subnet levels.

Import and export facilities of subnet data on the SLA Mon server

Through the SLA Mon web interface, you can now export the subnet entries available on the server to an Excel worksheet. You can also import a subnet list from an Excel worksheet on the local drive to the server.

SSO access to the SLA Mon web interface

Avaya Diagnostic Server now supports a single sign on (SSO) access to the SLA Mon web interface from Avaya Configuration and Orchestration Manager and System Manager. When you open the SLA Mon web interface from Avaya Configuration and Orchestration Manager or System Manager, you need not enter the user name and the password to log in. The system directly logs you on to the web interface with the SSO credentials that you use to log on to Avaya Configuration and Orchestration Manager or System Manager.

SLA Mon web interface enhancements

- The Agents tab is enhanced with the following:
  - Displays the current status of the registered agents.
  - Displays the network monitoring, the phone remote control, and the packet capture support statuses of the registered agents.
  - Provides a button to rediscover specific agents.
- The Network Summary page is enhanced with the following:
  - Displays intra-subnet cells as purple cells, which represent availability of agent-to-agent test data in that subnet.
  - Provides a facility to search for nodes in the location tree by typing the full or part of the address string.
  - Provides options to collapse, expand, select, and clear selection of nodes in the location tree.

- The Chart Detail page is enhanced with the following:
  - Distinguishes an agent pair involved in tests from a subnet pair by displaying the addresses of the subnet pair differently than the agent pair.
  - For subnet-to-subnet tests, displays the list of agent pairs that were involved in the tests for the selected period in a drop-down list.

Change history

Issue	Date	Summary of changes
1	February 2015	Avaya Diagnostic Server 2.5 GA release.
2	October 2015	• Added a note related to when the installer checks for the recommended hardware requirements in an upgrade scenario in the *Upgrading Avaya Diagnostic Server in the attended mode* section and in the *ADS_Response.properties file* section. • Added a caution about removing the `avaya-base.loc` file while cleaning up the SAL Gateway files in the *Troubleshooting* section.
3	April 2016	Added the upgrade path from SAL Gateway 2.2 virtual appliance to Avaya Diagnostic Server 2.5 in the *Upgrade paths to Avaya Diagnostic Server 2.5* section.
4	May 2016	• Modified the steps to validate the downloaded software package in the *Downloading the Avaya Diagnostic Server installer* section. • Added Appendix E, Configuring TLS1.2 on the SLA Mon Server. • Added Appendix F, Configuring the SLA Mon Server UI timeout settings.
5	September 2016	Added notes about not using the saluser login to upgrade Avaya Diagnostic Server in *Chapter 7, Upgrading Avaya Diagnostic Server*.

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
Administration		

Table continues…

Title	Description	Audience
Administering Avaya Diagnostic Server SLA Mon™	Provides information about configuring and administering Avaya Diagnostic Server for the remote diagnostics of Avaya endpoints and network condition monitoring through the SLA Mon server.	Solution architects, implementation engineers, support personnel, and customers
Administering Avaya Diagnostic Server SAL Gateway	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		
Avaya Diagnostic Server Additional Security Configuration Guidance	Provides information on the additional measures that can be taken on the Avaya Diagnostic Server host to meet customer security requirements and policies.	Implementation engineers, support personnel, and customers
Avaya Diagnostic Server Port Matrix	Provides information on the ports 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
Supported products interoperability list for Avaya Diagnostic Server with SLA Mon™	Provides a list of products that support the SLA Mon™ technology.	Solution architects, implementation engineers, support personnel, and customers

Related links

Finding documents on the Avaya Support website on page 11

Finding documents on the Avaya Support website

About this task

Use this procedure to find product documentation on the Avaya Support website.

Procedure

1. Use a browser to navigate to the Avaya Support website at http://support.avaya.com/.
2. At the top of the screen, enter your username and password and click **Login**.
3. Put your cursor over **Support by Product**.
4. Click **Documents**.
5. In the **Enter your Product Here** search box, type the product name and then select the product from the drop-down list.
6. If there is more than one release, select the appropriate release number from the **Choose Release** drop-down list.

7. Use the **Content Type** filter on the left to select the type of document you are looking for, or click **Select All** to see a list of all available documents.

   For example, if you are looking for user guides, select **User Guides** in the **Content Type** filter. Only documents in the selected category will appear in the list of documents.

8. Click **Enter**.

Related links

Documentation on page 10

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.

Related links

Using the Avaya InSite Knowledge Base on page 13

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips
- Information about service packs
- Access to customer and technical documentation
- Information about training and certification programs
- Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base at no extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base to look up potential solutions to problems.

1. Go to http://www.avaya.com/support.
2. Log on to the Avaya website with a valid Avaya User ID and password.

   The Support page appears.
3. Under **Support by Product**, click **Product-specific support**.
4. Enter the product in **Enter Product Name** text box and press Enter.
5. Select the product from the drop down list and choose the relevant release.
6. Select the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Related links

Support on page 12

Chapter 2: Avaya Diagnostic Server Overview

Avaya Diagnostic Server overview

Avaya Diagnostic Server is an Avaya serviceability solution for advanced diagnostic services and remote support to Avaya products. Avaya Diagnostic Server leverages the capabilities of Secure Access Link (SAL) with the addition of a patented technology, SLA Mon™. With the SLA Mon™ technology, Avaya Diagnostic Server takes the serviceability approach to an advanced level by adding remote phone control, phone event monitoring, and network diagnostic capabilities. Avaya Diagnostic Server provides faster time-to-resolution and better performance visibility across the network compared to the traditional approach of network diagnostics.

Avaya, BusinessPartner, and customer service personnel can use the customer-controllable troubleshooting and diagnostic tools of Avaya Diagnostic Server to improve problem verification and resolution times. With remote access, alarm transfer, remote phone control, remote phone event monitoring, and network monitoring capabilities, Avaya Diagnostic Server reduces onsite dispatches and customer engagement requirements.

Features of Avaya Diagnostic Server

The following table lists the support and diagnostic capabilities that Avaya Diagnostic Server provides to Support Advantage Preferred customers.

Feature	Avaya Diagnostic Server component	Description
Remote access	SAL Gateway	• Secure remote connection to Avaya products on the customer network for troubleshooting and remote implementation services. • Centralization of remote inventory management, logging, and authorization.
Alarm transport	SAL Gateway	• Aggregation and secure transport of alarms from Avaya products to Avaya. • Alarm logging and filtering.

Table continues…

Feature	Avaya Diagnostic Server component	Description
Automatic software update	SAL Gateway	• Automatic download of available software updates including major, minor, and service pack releases. • Automatic installation of downloaded software updates after a grace period. • Email notifications related to software updates, including download status, installation status, and availability.
Advanced diagnostics	SLA Mon	• Phone remote control to remotely troubleshoot Avaya endpoints. • Packet capture to capture network traffic in and out of Avaya endpoints. • Event monitoring to monitor events occurring on Avaya endpoints. • Phone screen capture to monitor the screen of Avaya endpoints and verify customer comments. • Bulk calls to stress test the communication system and the network.
Network monitoring	SLA Mon	• Network performance tests to monitor the network for conditions that might have an impact on voice, video, and data applications. • Hop-by-hop analysis of the network. • Easy-to-understand visual representation of network performance data through colored grids and graphs.

Benefits of Avaya Diagnostic Server

User type	Benefits
Customer	• Effective and efficient remote support and diagnostic services. • Improved resolution time. • Reduction in effort on complex issues. • Reduction in customer site dispatches and customer engagement requirements. • Self-service tools. • Full visibility to audit information for self diagnosis and review.

Table continues…

User type	Benefits
	• Options to enable or disable diagnostics features as required.
BusinessPartner	Authorized partners get the following additional benefits: • Assistance in troubleshooting up to 62% of issue types. • Ability to replicate customer problem for precise troubleshooting. • Reduction in customer site dispatches and remote engineering cycles through remote control, packet sniffing, event monitoring, and screen capture.

Components of Avaya Diagnostic Server

SAL Gateway

SAL Gateway centralizes remote access, alarm transfer, and access control policies for Avaya devices across the customer network. SAL Gateway provides a secure remote access connection between Avaya and Avaya devices on the customer network. Through SAL, Avaya Services tools and engineers can access customer devices to resolve network and product-related issues.

The key feature of SAL is simple network integration. Instead of opening numerous inbound and outbound ports between the customer and the service provider, SAL consolidates the entire traffic and uses a single outbound firewall port to facilitate secure HTTP communication. Therefore, SAL minimizes network impact.

SAL uses public certificate based authentication for remote access requests. You can intelligently establish access policies using an optional Policy Server.

SLA Mon server

The SLA Mon server provides diagnostic capabilities such as remote control of Avaya deskphones, event monitoring, packet capture from devices, and network monitoring. With the SLA Mon technology, you can improve remote troubleshooting by reducing the need for onsite technicians and time-consuming deployment of onsite monitoring tools.

The SLA Mon server 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 the phone remote

Table continues…

Feature	Description
	control feature enabled. You can 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. • Monitor the overlay of the actual phone screen on the SLA Mon web interface to verify events displayed on the phone screen.
Event monitoring	You can use the event monitoring feature to monitor events occurring on Avaya endpoints, such as button presses or touch events.
Phone screen capture	Through the SLA Mon server command line interface (CLI), you can retrieve the real-time screen capture of the phone display area. Service personnel can use the screen capture feature to verify user comments and monitor the screen of the endpoints.
Bulk calls	Through the SLA Mon server CLI, you can make bulk calls 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.
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. You can analyze the packets to identify issues with the device.
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.

Avaya Diagnostic Server architecture

The following is an illustration of the Avaya Diagnostic Server architecture:

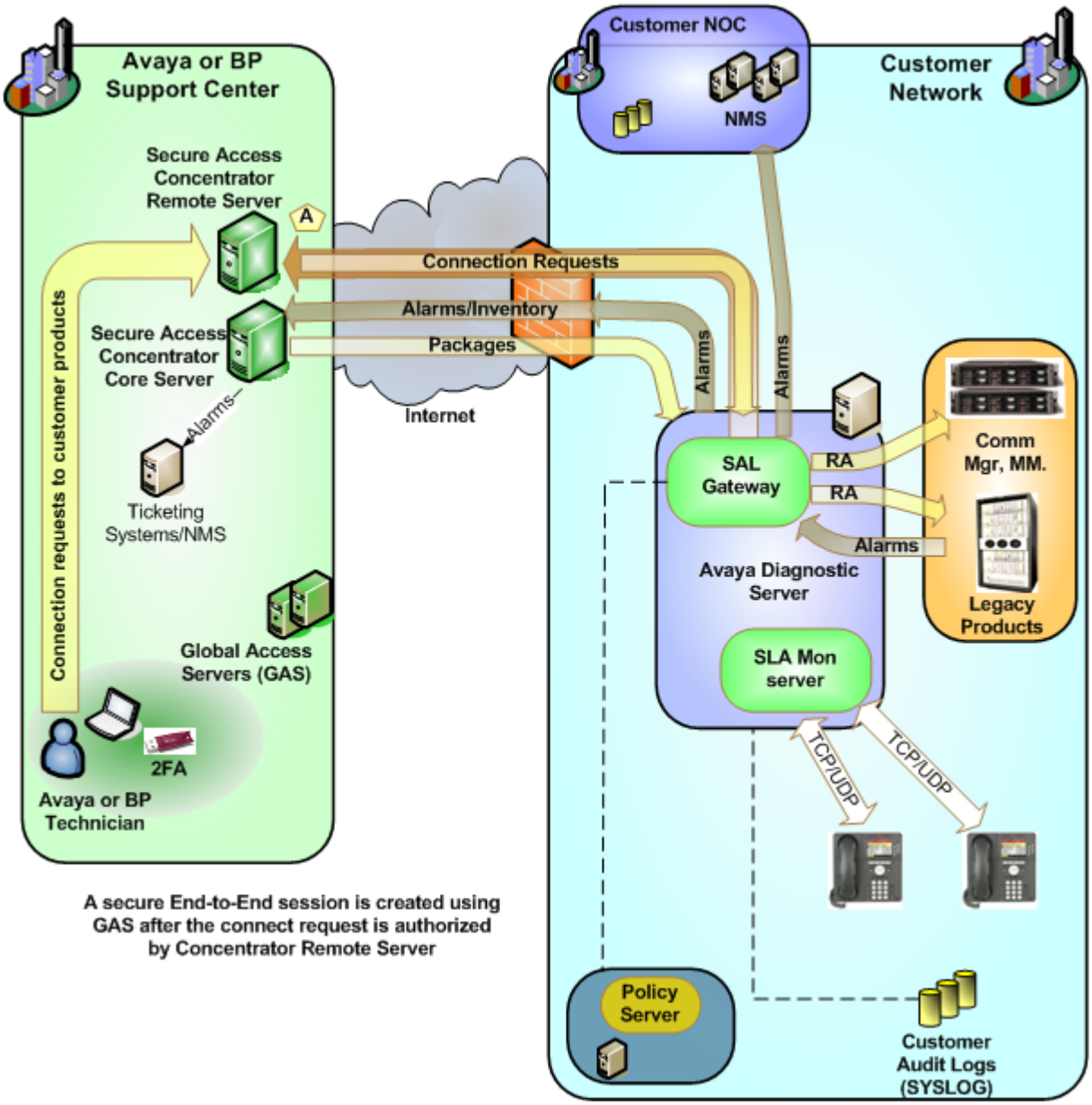

Figure 1: Avaya Diagnostic Server architecture

Capacity of Avaya Diagnostic Server

The following table provides the maximum capacity of Avaya Diagnostic Server 2.5 according to the hardware specification of the host and the components installed on the server:

Hardware specification	Maximum load		
	SAL Gateway only	SLA Mon only	Cohosted components
Standalone server: 4-GB RAM and dual core processor with 2.2 GHz speed	• 50 alarms/minutes • 50 simultaneous remote sessions • 500 managed elements	• 150 bidirectional links for data, voice, and video together • 3000 registered agents • 3 simultaneous packet capture sessions • 3 simultaneous phone remote control sessions	• 50 alarms/minutes • 50 simultaneous remote sessions • 500 managed elements • 100 bidirectional links for data, voice, and video together • 2000 registered agents • 3 simultaneous packet capture sessions • 3 simultaneous phone remote control sessions
Standalone server: 8-GB RAM and quad core processor with 2.2 GHz speed	• 50 alarms/minutes • 50 simultaneous remote sessions • 500 managed elements	• 250 bidirectional links for data, voice, and video together • 5000 registered agents • 3 simultaneous packet capture sessions • 5 simultaneous phone remote control sessions	• 50 alarms/minutes • 50 simultaneous remote sessions • 500 managed elements • 200 bidirectional links for data, voice, and video together • 4000 registered agents • 3 simultaneous packet capture sessions • 5 simultaneous phone remote control sessions
ION: 4-GB RAM and dual core processor with 1.2 GHz speed	• 50 alarms/minutes • 50 simultaneous remote sessions • 500 managed elements	• 50 bidirectional links for data, voice, and video together • 500 registered agents • 2 simultaneous packet capture sessions • 2 simultaneous phone remote control sessions	• 50 alarms/minutes • 50 simultaneous remote sessions • 500 managed elements • 25 bidirectional links for data, voice, and video together • 500 registered agents • 2 simultaneous packet capture sessions

Table continues…

Hardware specification	Maximum load		
	SAL Gateway only	SLA Mon only	Cohosted components
			• 2 simultaneous phone remote control sessions
Open Virtual Appliance (OVA): 8-GB RAM and quad core processor with 2.2 GHz speed	• 50 alarms/minutes • 50 simultaneous remote sessions • 500 managed elements	• 250 bidirectional links for data, voice, and video together • 5000 registered agents • 3 simultaneous packet capture sessions • 5 simultaneous phone remote control sessions	• 50 alarms/minutes • 50 simultaneous remote sessions • 500 managed elements • 200 bidirectional links for data, voice, and video together • 4000 registered agents • 3 simultaneous packet capture sessions • 5 simultaneous phone remote control sessions
Avaya Common Server: 4-GB RAM and quad core processor with 2.4 GHz speed	• 50 alarms/minutes • 50 simultaneous remote sessions • 500 managed elements	• 150 bidirectional links for data, voice, and video together • 3000 registered agents • 3 simultaneous packet capture sessions • 3 simultaneous phone remote control sessions	• 50 alarms/minutes • 50 simultaneous remote sessions • 500 managed elements • 100 bidirectional links for data, voice, and video together • 2000 registered agents • 3 simultaneous packet capture sessions • 3 simultaneous phone remote control sessions

Chapter 3: Installation prerequisites

Preinstallation tasks checklist

Before you install Avaya Diagnostic Server, complete the following tasks to ensure a successful installation of Avaya Diagnostic Server.

#	Task	Description	Notes	✔
1	Ensure that the host computer on which you want to install Avaya Diagnostic Server meets the minimum hardware requirements, such as memory size, disk space, and processor.	See Hardware and software requirements on page 33.		
2	Install a supported version of Red Hat Enterprise Linux (RHEL) with a default package set.	Ensure that the ISO or DVD that you use to install the RHEL version is downloaded or issued from Red Hat, Inc. only. • To know the RHEL versions that are compatible with Avaya Diagnostic Server, see Hardware and software requirements on page 33. • To learn about RHEL installation, see the installation documentation for the specific RHEL version at https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/.		
3	If hard disk partitioning exists on the RHEL host, check whether the `/opt` and the `/var` directories are mounted on different file systems.	If the `/opt` and the `/var` directories are on different file systems, ensure that the directories meet the minimum disk space requirements for Avaya Diagnostic Server installation and upgrade.	You can use the **`df -h`** command to check disk partitioning and free space.	

Table continues…

#	Task	Description	Notes	✔
		See Hardware and software requirements on page 33.	For more information about the commands that you can use to check disk partitioning, see Commands to check disk partitioning on the operating system on page 152.	
4	Ensure that you have root privileges to the host computer and that you log in as the root user to install Avaya Diagnostic Server.			
5	Ensure that the Bash shell, `/bin/bash`, exists on the host computer.			
6	Ensure that the SAL Gateway user, if preexists on the host, has the execute permissions to the Bash shell.	During the Avaya Diagnostic Server installation, the installer accepts a user name that owns the file system and the services associated with SAL Gateway. For the SAL Gateway services to run successfully, the preexisting SAL Gateway user must have the execute permissions to the Bash shell.	The default SAL Gateway user is *saluser*.	
7	Install Oracle Java Runtime Environment (JRE) 1.7.0_x, where x is update 10 or later.	For a clean installation, you can remove any earlier JRE version, and install Oracle JRE 1.7. See Installing Java 1.7 using an RPM binary on page 145. If some other software on the server uses a different version of JRE, you must maintain more than one version of JRE. You can install the new JRE version at a different path. See Installing Java 1.7 using an archive binary on page 144.	Ensure that the installed JRE is Oracle JRE. Avaya Diagnostic Server supports only Oracle JRE. For Avaya Diagnostic Server 2.5, do not update to JRE 1.8.0 or later.	
8	Export the JAVA_HOME environment variable in `/root/.bash_profile` or `/root/.bashrc`.	See Updating the Java environment variable after a JRE upgrade on page 147.		

Table continues…

#	Task	Description	Notes	✔
9	If the SAL Gateway user already exists, ensure that the JAVA_HOME variable is updated in the `.bashrc` file of the user after you upgrade the JRE version.	See Updating the Java environment variable after a JRE upgrade on page 147.	The default SAL Gateway user is *saluser*.	
10	Ensure that the host computer meets all other software requirements for Avaya Diagnostic Server.	See Hardware and software requirements on page 33.		
11	Ensure that your browser is set to establish an HTTPS session.	Avaya Diagnostic Server supports the TLS 1.2 protocol for HTTPS sessions. Enable TLS 1.2 in the browser settings to establish an HTTPS session using the TLS 1.2 protocol.		
12	Ensure that you have an Avaya Sold-To number, also known as Functional Location (FL).	A Sold-To number is your primary account number with Avaya for a specific location, for example, the location where you are deploying Avaya Diagnostic Server. You require the Sold-To number while registering SAL Gateway or the SLA Mon server to obtain the identifying numbers, Product ID and Solution Element ID, of the components.	If you do not know your Sold-To number, contact your Avaya or Partner Account Manager.	
13	Ensure that you have an Avaya single sign on (SSO) login that is associated with the Sold To number that identifies the installation location of Avaya Diagnostic Server.	You require the SSO login to download the Avaya Diagnostic Server software and to generate the SAL Gateway identifying numbers automatically.	You can obtain this login by going to https://support.avaya.com and clicking **REGISTER NOW**.	
14	Download the Avaya Diagnostic Server software from Product Licensing and Delivery System (PLDS).	See Downloading software from PLDS on page 39.		
15	Copy and extract the downloaded `ADS-Installer-2.5.0.0-<xxx>.tar.gz` file to a local directory on the host server.	See Extracting the Avaya Diagnostic Server software files to a local directory on page 40.		
16	**(Optional)** Obtain the SAL Gateway identifying numbers, Solution	Obtaining the IDs in advance is not mandatory. You have	If you use the default IDs to install SAL Gateway, you must	

Table continues…

#	Task	Description	Notes	✔
	Element ID and Product ID, from Avaya.	the following additional options: • Generate the IDs automatically during the installation. This option is available only for an attended installation. • Accept the default IDs during the installation. After the installation, update or generate the IDs through the SAL Gateway UI. To obtain these numbers in advance, see Registering SAL Gateway on page 41.	configure the correct IDs after the installation. Otherwise, SAL services cannot start. To install the SLA Mon server component, you do not require Product ID and Solution Element ID.	
17	Ensure that the RHEL host is configured to use a valid DNS server that resolves external host names.			
18	If the managed devices are configured with IPv6 settings, ensure that the host is configured for IPv6.		The SLA Mon server component of Avaya Diagnostic Server works only on IPv4. If you plan to install Avaya Diagnostic Server with SLA Mon, configure the host for IPv4.	
19	Configure the host server to use Network Time Protocol (NTP) to synchronize the clock of the system.	For proper functioning of the Avaya Diagnostic Server features, the Avaya Diagnostic Server components rely on the accurate setting of system clocks. Use NTP to ensure stability and reliability of alarm transfer and remote access to devices through Avaya Diagnostic Server. To configure NTP settings, see the operating system documentation at https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/.	The certificate-based authentication mechanisms of Avaya Diagnostic Server rely on accurate clocks to check the expiration and signatures of the remote access requests. When clocks are synchronized to standard NTP servers, you can correlate events from different servers when auditing log	

Table continues…

#	Task	Description	Notes	✔
		For the Avaya Diagnostic Server virtual appliance deployment, follow the timekeeping best practices that are recommended for the virtualized environment.	files from multiple servers. For more information about NTP, visit http://www.ntp.org or http://www.ntp.org/ntpfaq/NTP-a-faq.htm.	
20	Obtain the locations of the Concentrator Servers.	During the SAL Gateway installation, you require the locations of Concentrator Core Enterprise Server and Concentrator Remote Enterprise Server. You must provide the following fully qualified host names and port numbers to the installer so that Avaya Diagnostic Server can successfully communicate with Avaya: • Secure Access Concentrator Core Server: *secure.alarming.avaya.com* and port 443 • Secure Access Concentrator Remote Server: *remote.sal.avaya.com* and port 443		
21	Ensure that you have network access to the SAL Global Access Server host names from the Avaya Diagnostic Server host.	SAL Global Access Server host names: • sas[1-4].sal.avaya.com • sas[21-22].sal.avaya.com • sas[31-32].sal.avaya.com You need not administer the Global Access Server host names on SAL Gateway or the host sever. However, you might need to configure the firewall and outbound proxies on your network to allow access to these host names.	You can test the connections to each host name by using either the **`curl`** or **`wget`** utility available on Linux operating systems. For more information, see *PSN004098u - Mandatory Administrative Update for SAL Remote Access Infrastructure Improvement*.	

Table continues…

#	Task	Description	Notes	✔
22	Enable the firewall of the host by running the `/sbin/service iptables start` command.			
23	Ensure that no firewall between the browser of the administrator and Avaya Diagnostic Server blocks the ports 7443 and 4511.			
24	Ensure that the `/etc/hosts` and `/etc/sysconfig/network` files have host name entries that match the values the system displays when you run the **`hostname`** command.			
25	Ensure that the server host name does not resolve to the loopback address, 127.0.0.1. Add the host name to IP address mapping entry as the first line in the `/etc/hosts` file.			
26	To enable remote agent logging on the local server in an RHEL 5.x host system, ensure that the syslogd option in the `/etc/sysconfig/syslog` file reads as `SYSLOGD_OPTIONS="-r -m 0"`.	You must set this option to enable logging for remote access activities. After making this change, you must restart the syslog service using the `service syslog restart` command to make this change effective. For more information about editing the syslog file, see Editing the syslog configuration file for RHEL 5.x on page 76.	If the host is an RHEL 6.x system, update the `/etc/rsyslog.conf` file. For more information, see the next task in the checklist.	

27	To enable remote agent logging on the local server in an RHEL 6.x host system, ensure that the following two lines in the `/etc/rsyslog.conf` file are uncommented. That is, ensure that no pound (#) sign remains at the start of the following lines:
	`$ModLoad imudp.so`
	`$UDPServerRun 514`
		After making this change, you must restart the rsyslog service using the **`service rsyslog restart`** command to make the changes effective.
		For more information about editing the rsyslog file, see Editing the syslog configuration file for RHEL 6.x on page 76.		

Table continues…

#	Task	Description	Notes	✔
28	To generate Solution Element ID for SAL Gateway automatically during installation, ensure that the host server has FireFox 3.x or later as the default web browser.	The GUI-based installer opens the Automatic Registration Tool (ART) website on the default browser for SAL Gateway registration. Other web browsers available with RHEL might not support the ART website.	To obtain the Solution Element ID and Product ID prior to the SAL Gateway installation, see Registering SAL Gateway on page 41.	
29	Ensure that the minimum set of RPMs required for the installation and correct functioning of Avaya Diagnostic Serverare installed on the RHEL host.	See Recommended RPMs on page 35. If the default package set you installed with RHEL does not include the required RPMs, install the RPMs before the installation of Avaya Diagnostic Server. **Note:** While installing the RPMs, ensure that the RPMs match the architecture of the server, that is, 32 bit or 64 bit.	For more information about installing RPMs using the Yum installer, see the problem statement *Avaya Diagnostic Server installation fails because of missing dependent RPMs* in Chapter 11, Troubleshooting Diagnostic Server.	
30	Ensure that you have the latest yum version on the RHEL host.	For a successful installation or upgrade of Avaya Diagnostic Server, the yum version must be at least 3.2.x.		
31	Ensure that Security-Enhanced Linux (SELinux) is disabled on the Avaya Diagnostic Server host.	See Disabling the SELinux protection on page 149	SAL Gateway and SLA Mon might not function properly if SELinux on the host server is enabled and in the enforcing mode.	
32	If you plan to install Avaya Diagnostic Server on a virtual machine that is on ESXi 5.0, ensure that patch 04 is applied on ESXi 5.0.	You must apply patch 04 on ESXi 5.0 for correct functioning of the SLA Mon server.		

Preinstallation information gathering checklist

During the installation of Avaya Diagnostic Server and its components, specially SAL Gateway, you must provide appropriate values in several fields. Get the required information in advance to make the installation faster and accurate.

Use the following checklist to ensure that you have gathered the required data before you start the Avaya Diagnostic Server installation:

Field	Description	Required to proceed	Value provided by	Value
To identify SAL Gateway:				
Solution Element ID	A unique identifier in the (NNN)NNN-NNNN format, where N is a digit from 0 to 9 that identifies SAL Gateway. Get this value from Avaya. See Registering SAL Gateway on page 41.	Yes	Avaya	
Alarm/Inventory ID	A unique 10-digit identifier, also known as Product ID, assigned to a customer device, in this case SAL Gateway. SAL or other alarm management systems uses this ID to identify devices that report alarms to Avaya. Get this value from Avaya. See Registering SAL Gateway on page 41.	Yes	Avaya	
IP Address	The IP address of the host server. SAL Gateway takes both IPv4 and IPv6 addresses as input.	Optional	Customer	
To configure the SAL Gateway user:				
User Name	The user who owns the SAL Gateway file system. During installation, you can accept the default user name, *saluser*, or provide a new user name. For the SAL Gateway services to run successfully, ensure that the SAL Gateway user, if preexists on the host, has the execute permissions to the Bash shell.	Yes	Customer	
User Group	The SAL Gateway user group. During installation, you can accept the default user group or provide a new user group name.	Yes	Customer	
To identify Secure Access Concentrator Core Server:				

Table continues…

Field	Description	Required to proceed	Value provided by	Value
Platform Qualifier	The platform qualifier that SAL Gateway uses to communicate with Concentrator Core Server located at Avaya. Unless you are explicitly instructed, you must use the default value provided by the installer.	Yes	Avaya	
Primary destination	The host name of the Concentrator Core Server that SAL Gateway first contacts for alarming. Default destination: secure.alarming.avaya.com	Yes	Avaya	
Primary destination port	The port number that the primary destination, that is Concentrator Core Server, uses to listen in. Default port: 443	Yes	Avaya	
To identify Secure Access Concentrator Remote Server:				
Primary destination	The host name of the primary Concentrator Remote Server that provides remote connectivity through SAL Gateway. Default destination: remote.sal.avaya.com	Yes	Avaya	
Primary destination port	The port number that the primary Concentrator Remote Server uses for remote connectivity. Default port: 443	Yes	Avaya	
(Optional) To configure a proxy server:				
Proxy type	The proxy server type that you want to use.	Optional	Customer	
Proxy host name	The host name or IP address of the proxy server.	Optional	Customer	
Proxy port	The port number that the proxy server uses.	Optional	Customer	
(Optional) To configure Secure Access Policy Server: **Note:** In Release 3.0 Phase I, you do not need to configure Policy Server. Therefore, ignore any Policy Server related configuration information mentioned in this document.				
Host name	The host name or IP address of Policy Server.	Optional	Customer	

Table continues…

Field	Description	Required to proceed	Value provided by	Value
port	The port number that Policy Server uses.	Optional	Customer	
To configure an SMTP mail server to receive email notifications:				
SMTP host name	The host name or the IP address of the SMTP server.	Yes	Customer	
SMTP port	The port number of the SMTP server	Yes	Customer	
Administrator email address	The email address of the administrator to whom email notifications must be sent.	Yes	Customer	
SMTP user name	The name of the user to be authenticated in the SMTP server. Required only when the SMTP server is configured to authenticate users.	Optional	Customer	
SMTP password	The password of the user to be authenticated. Required only if you must provide a user name for authentication.	Optional	Customer	
Secondary email address	The secondary email address where you want to receive email notifications.	Optional	Customer	
To configure SNMP subagent:				
Master agent host name	The host name or IP address of the SNMP master agent.	Yes	Customer	
Master AgentX Port	The listener port that the master agent uses with AgentX.	Yes	Customer	
To use a remote WebLM server for SLA Mon license configuration:				
WebLM server IP address **Note:** This information is required only for theSLA Mon server.	The IP address or host name of the remote WebLM server that you want to use for SLA Mon license configuration. If you choose to install WebLM locally during the Avaya Diagnostic Server installation, this value is not required.	Optional	Customer	

Customer responsibilities

When you install Avaya Diagnostic Server on customer-provided hardware with a customer-installed operating system, the customer owns the control and care of the hardware and the operating system. To ensure that Avaya Diagnostic Server functions properly, the customer must take on certain responsibilities of maintaining the host server before and after the installation.

Preinstallation customer responsibilities

The following table provides a list of mandatory and optional preinstallation tasks that a customer has the responsibility to perform to ensure that Avaya Diagnostic Server operates properly on the customer-provided system.

Task	Required?	Notes
Install a supported version of RHEL with a default package set.	Yes	See Hardware and software requirements on page 33. To learn about RHEL installation, see the installation documentation for the specific RHEL version at https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/.
Install JRE 1.7.	Yes	See Installing Java 1.7 using an archive binary on page 144 or Installing Java 1.7 using an RPM binary on page 145.
If the SAL Gateway user already exists, ensure that the JAVA_HOME variable is updated in the `.bashrc` file of the user after you upgrade the JRE version.	Yes	See Updating the Java environment variable after a JRE upgrade on page 147.
Ensure that the server host name does not resolve to the loopback address, 127.0.0.1. Add the host name and IP address mapping entry at the first line in the `/etc/hosts` file.	Yes	
If you do not want to install the Web License Manager (WebLM) server locally during the SLA Mon server installation, obtain the IP address of the remote WebLM server where you will install the license for the SLA Mon server.	Yes	WebLM is an Avaya licence server used to configure the SLA Mon license. You can either choose to configure the SLA Mon license using the WebLM server locally or using a remote WebLM server. If you choose to install WebLM locally, the system installs WebLM on your local machine along with SLA Mon . If you do not choose to install WebLM locally, then you must provide the IP address of the external WebLM server.
Acquire, maintain, and manage firewalls.	Yes	
Set up an uninterruptible power supply (UPS).	Yes	

Table continues…

Task	Required?	Notes
Ensure that the Domain Name System (DNS) is set up for the proper functioning of Avaya Diagnostic Server on the network.	Yes	
Ensure the security of the platform for Avaya Diagnostic Server.	Yes	You must place some secure mechanisms to prevent attacks on SLA Mon and SLA Mon UI and unauthorized access to SAL Gateway and SLA Mon UI. One of the simple things you can do is to have proper user names and passwords for authorized users.
If you want the audit log entries to be written to an external server, configure syslogd.	Optional	
If you want to restrict remote access to a certain time window, set of people, and set of managed devices, install a Policy Server on a different host.	Optional	For information on the Policy server, see *Secure Access Link Policy Server Installation and Maintenance Guide*.
Configure encryption settings for Apache Tomcat.	Optional	The Avaya Diagnostic Server 2.5 installer is packaged with Apache Tomcat version 6.0.41. By default, Avaya Diagnostic Server is installed with a self-signed certificate. The self-signed certificate is generated using the SHA-2 algorithm and is 256-bit encrypted. You can use a certificate from a certificate authority (CA) and import the certificate to the Avaya Diagnostic Server keystore.
Set up antivirus software if you want such protection for the host server.	Optional	
Enter an appropriate system warning message.	Optional	The `/etc/issue` file holds the default text for the warning. The system administrator can edit this file and enter any appropriate messages for the system users.

Postinstallation customer responsibilities

The customer owns the following postinstallation responsibilities:

- Control and care of the hardware.
- Maintenance of the operating system. Whenever new system updates are available, the customer is responsible to apply the updates that contain bug fixes or resolutions to security issues.

- Maintenance of any third-party software that are not bundled with Avaya Diagnostic Server. Whenever new software updates are available, the customer is responsible to apply the updates that contain bug fixes or resolutions to security issues.

Hardware and software requirements

For a successful installation of Avaya Diagnostic Server, the host server must fulfill the minimum hardware and software requirements.

Hardware requirements

This table provides the minimum and the recommended hardware requirements to install Avaya Diagnostic Server. The requirements vary according to the Avaya Diagnostic Server component that you want to install. Refer to the respective columns accordingly.

Component	SAL Gateway		SLA Mon		SAL Gateway and SLA Mon	
	Minimum	**Recommended**	**Minimum**	**Recommended**	**Minimum**	**Recommended**
Processor	Dual core with minimum 2 GHz clock speed	Quad core with minimum 2 GHz clock speed	Dual core with minimum 2 GHz clock speed	Quad core with minimum 2 GHz clock speed	Dual core with minimum 2 GHz clock speed	Quad core with minimum 2 GHz clock speed
RAM	2 GB	4 GB	4 GB	8 GB	4 GB	8 GB
Hard disk space	If `/opt` and `/var` are in the same partition: • Free space in the partition: 10 GB If `/opt` and `/var` are in separate partitions: • Free space in `/opt`: 10 GB • Free space in `/var`: 80 MB [1]	If `/opt` and `/var` are in the same partition: • Free space in the partition: 40 GB If `/opt` and `/var` are in separate partitions: • Free space in `/opt`: 40 GB • Free space in `/var`: 100 MB	If `/opt` and `/var` are in the same partition: • Free space in the partition: 40 GB If `/opt` and `/var` are in separate partitions: • Free space in `/opt`: 10 GB • Free space in `/var/`	If `/opt` and `/var` are in the same partition: • Free space in the partition: 190 GB If `/opt` and `/var` are in separate partitions: • Free space in `/opt`: 10 GB • Free space in `/var/lib`: 180 GB	If `/opt` and `/var` are in the same partition: • Free space in the partition: 50 GB If `/opt` and `/var` are in separate partitions: • Free space in `/opt`: 20 GB • Free space in `/var/lib`: 30 GB	If `/opt` and `/var` are in the same partition: • Free space in the partition: 230 GB If `/opt` and `/var` are in separate partitions: • Free space in `/opt`: 50 GB • Free space in `/var/`

Table continues…

Component	SAL Gateway		SLA Mon		SAL Gateway and SLA Mon	
	Minimum	Recommended	Minimum	Recommended	Minimum	Recommended
			`lib`: 30 GB [2]			`lib`: 180 GB
Network	100 Mbps Ethernet or NIC		100 Mbps Ethernet or NIC		100 Mbps Ethernet or NIC	
CD-ROM Drive		A CD-ROM drive might be useful for Red Hat installation.				

Software requirements

The following table provides the supported operating system and other software that the host server must have for an installation of Avaya Diagnostic Server.

Component	Supported versions
Operating system	Red Hat Enterprise Linux (RHEL) versions on 32-bit and 64-bit systems: • 5.x • 6.x **Important:** To perform an operating system upgrade on an existing host server, see Instructions for operating system upgrade on page 150.
Java	Oracle JRE 1.7.0_*x*, where x is update 10 or later. **Note:** Do not update to JRE 1.8.0 or later.
Perl	For RHEL 5.x: Version 5.8 For RHEL 6.x: Version 5.10
Web browser	For downloading the software: • Microsoft Internet Explorer 8.0 and later • FireFox 3.x and later with the FireFTP plug-in

Table continues…

[1] If you enable syslog for SAL Gateway, then SAL Gateway writes the logs in `/var/log/SALlogs`. Therefore, you must have the minimum free space in `/var`.

[2] You must have the minimum free space in the `/var/lib` directory because the SLA Mon server stores data in this directory. In addition, never change the `/opt` and the `/var/lib` directory paths in the installation script.

Component	Supported versions
	You require the plug-in only if you download the software from a Linux server or an FTP server. For the RHEL host: • FireFox 3.x or later as the default web browser For opening the web interfaces of Avaya Diagnostic Server components: • For SAL Gateway: Microsoft Internet Explorer 9 and 10 • For SLA Mon: - Microsoft Internet Explorer 9, 10, and 11 - FireFox 33 and 34

Recommended RPMs

For a successful installation of Avaya Diagnostic Server and correct functioning of the Avaya Diagnostic Server components, the RHEL host might require certain RPMs. The default package set that you install with the RHEL operating system might not include all the required RPMs.

The following tables provide the list of RPMs that Avaya recommends for Avaya Diagnostic Server. The lists are supersets of all required RPMs including RPMs that might be required to resolve cycling dependencies for installing and running the SLA Mon server. The following lists of RPMs are not specific to a particular platform or OS version. Use the lists as a reference point when installing Avaya Diagnostic Server.

Note:

You might have to install additional RPMs for the glibc.i686 installation and to resolve dependencies.

Table 1: RPMs common for both SAL Gateway and SLA Mon server

• audit-libs • basesystem • bash • chkconfig • coreutils • cpio • cracklib • cracklib-dicts • cyrus-sasl-lib • db4	• grep • hwdata • initscripts • iproute • iptables • iputils • krb5-libs • libacl • libcap • libgcc • libselinux	• nspr • nss • openldap • openssl • pam • pcre • popt • procps • psmisc • readline • sed

• ethtool • findutils • gawk • glib2 • glibc • glibc-common • glibc.i686 (32 bit) **Note:** Install the glibc i686 RPM only on a *64-bit* RHEL 6.x system.	• libsepol • libstdc++ • libxml2 • libXtst • mingetty • module-init-tools • ncurses • net-tools	• setup • shadow-utils • tar • tzdata • udev • yum • zlib

Table 2: Additional RPMs recommended for SAL Gateway

• anacron • audit-libs-python • authconfig • crontabs • cryptsetup-luks • curl • cyrus-sasl • dbus • dbus-glib • device-mapper • dhclient • dmidecode • dmraid • dos2unix • elfutils-libelf • expat • file • filesystem • gdbm • gnutls • grub • hal	• libgpg-error • libgssapi • libselinux-python • libsysfs • libtermcap • libuser • libvolume_id • libxml2-python • logrotate • lvm2 • m4 • man • mcstrans • mkinitrd • nash • nc • net-snmp • newt • nss_ldap • openssh • openssh-clients • parted • passwd	• pm-utils • policycoreutils • redhat-logos • rhpl • rootfiles • rpm • rpm-libs • rpm-python • selinux-policy • selinux-policy-targeted • setools • slang • sudo • sysklogd • tcpdump • telnet • termcap • traceroute • unzip • usermode • util-linux • which • wireless-tools

• kbd • kpartx • libevent • libgcrypt	• pciutils • openssh-server • perl	• zip

Table 3: Additional RPMs recommended for the SLA Mon server

• binutils • ca-certificates • coreutils-libs • dbus-libs • gamin • gmp • gzip • info • keyutils-libs • libattr	• libblkid • libcom_err • libidn • libnih • libusb • libutempter • libuuid • MAKEDEV • ncurses-base • ncurses-libs	• nss-softokn-freebl • nss-sysinit • nss-util • postgresql • postgresql-libs • postgresql-server • redhat-release-server • sysvinit-tools • upstart • util-linux-ng

Note:

While installing the RPMs, you must ensure that the RPMs match the architecture of the RHEL server, that is, whether the server is a 32-bit or a 64-bit server.

Firewall and ports

For system security, you must enable the iptables firewall software on the system that hosts Avaya Diagnostic Server. The Red Hat Enterprise Linux (RHEL) operating system includes an iptables firewall software. You can enable the firewall to block all inbound traffic, except the traffic that is necessary. After the Avaya Diagnostic Server installation, the server opens only those inbound ports of the host server in the firewall that are necessary for the operations of Avaya Diagnostic Server.

The following table provides a list of required and recommended ports for Avaya Diagnostic Server. Ensure that the required ports are available through the firewall.

Port	Description	Required/Recommended
7443 (TCP/HTTPS)	For SAL Gateway user interface access	Required
4511 (TCP/HTTPS)	For SLA Mon user interface access	Required
162 (UDP)	SNMP trap receiver port	Required

Table continues…

Port	Description	Required/Recommended
161 (UDP)	SNMP GET receiver port	Recommended
22 (TCP)	For remote access through SSH	Recommended
5107 (TCP)	For support of devices that send IP INADS	Recommended
5108 (TCP)	For support of Call Management System that sends IP INADS traps	Recommended
514 (UDP)	For syslog in RHEL 5.x and for rsyslog in RHEL 6.x	Recommended
50009 (UDP)	For the performance monitoring receiver	Recommended
50010 (UDP)	For the packet capture receiver	Recommended
50011 (TCP/UDP)	For the SLA Mon server-to-agent communication	Recommended
52233 (TCP)	For the SLA Mon server licensing	Recommended

Note:

If the required ports are unavailable at the time of Avaya Diagnostic Server installation, the installation fails because the SLA Mon and the SAL Gateway UI services cannot start.

Downloading the Avaya Diagnostic Server installer

Registering for PLDS

Procedure

1. Go to the Avaya Product Licensing and Delivery System (PLDS) website at https://plds.avaya.com.

   The PLDS website redirects you to the Avaya single sign-on (SSO) webpage.
2. Log in to SSO with your SSO ID and password.
3. On the PLDS registration page, register as:
   - An Avaya Partner: Enter the Partner Link ID. To know your Partner Link ID, send an email to prmadmin@avaya.com.
   - A customer: Enter one of the following:
     - Company Sold-To
     - Ship-To number
     - License authorization code (LAC)

4. Click **Submit**.

   Avaya sends the PLDS access confirmation within one business day.

Downloading software from PLDS

About this task

Note:

You can download product software from http://support.avaya.com also.

Procedure

1. Type http://plds.avaya.com in your Web browser to go to the Avaya PLDS website.
2. Enter your Login ID and password to log on to the PLDS website.
3. On the Home page, select **Assets**.
4. Select **View Downloads**.
5. Search for the available downloads by using one of the following:
   - An application type and the version number
   - Download name
6. Click the download icon from the appropriate download.
7. When the system displays the confirmation box, select **Click to download your file now**.
8. If you receive an error message, click the message, install Active X, and continue with the download.
9. When the system displays the security warning, click **Install**.

   When the installation is complete, PLDS displays the downloads again with a check mark next to the downloads that have completed successfully.

Validating the downloaded Avaya Diagnostic Server software

About this task

The installer tar file might get corrupted during the download process because of incomplete download. When you try to unzip a corrupted installer file, you might get errors. Use this procedure to validate that the Avaya Diagnostic Server software download was successful.

Before you begin

Download the `ADS-Installer-2.5.0.0-<xxxx>.tar.gz` file and copy the file to a directory on the target host.

Procedure

1. Log on to the Avaya Diagnostic Server host system as a user with administrator rights.

2. Go to the directory where you have downloaded the installer tarball file, `ADS-Installer-2.5.0.0-<xxxx>.tar.gz`.
3. Run the following command:

   `/usr/bin/md5sum` `ADS-Installer-2.5.0.0-<xxxx>.tar.gz`
4. Check the output.

   For a successful download, the output must match the md5sum that is displayed on the downloads page for Avaya Diagnostic Server on the Avaya support site.
5. If you get a different output for the downloaded software, download the `ADS-Installer-2.5.0.0-<xxxx>.tar.gz` file again and validate the download.

Extracting the Avaya Diagnostic Server software files to a local directory

About this task

After you download the Avaya Diagnostic Server software file from PLDS, you must extract the installer file from the downloaded zip file to a local directory of the Avaya Diagnostic Server host.

Procedure

1. Download the Avaya Diagnostic Server software from PLDS to a local system.

   You can download the installer using the PLDS link.
2. In the home directory of the host server where you want to install Avaya Diagnostic Server, create a new directory.

   Caution:

   You must enter a directory name that contains simple alphanumeric characters. If the directory name contains special characters, such as pound (#), asterisk (*), and dollar ($), the system displays an error when you run the installer.
3. Copy the downloaded `ADS-Installer-2.5.0.0-<xxxx>.tar.gz` file to the new directory.
4. Run the **`tar`** `-xvf ADS-Installer-2.5.0.0-<xxxx>.tar.gz` command.

   The command extracts a directory, `ADS-Installer-2.5.0.0-<xxxx>`, to the directory where you copied the `.tar.gz` file. The new `ADS-Installer-2.5.0.0-<xxxx>` directory contains the Avaya Diagnostic Server installer, `install.sh`, and other related files and folders.

Next steps

Run the installer script with the root user privilege to start the Avaya Diagnostic Server installation.

Related links

Starting the Avaya Diagnostic Server installation in the attended mode on page 43

Registering SAL Gateway

About this task

Registering a product with Avaya is a process that uniquely identifies the product so that Avaya can service the product. When you register a new SAL Gateway, Avaya assigns a Solution Element ID and a Product ID to the SAL Gateway. You require these identifiers when you install SAL Gateway. SAL Gateway becomes operational only when you configure SAL Gateway with the correct identifiers. Through these IDs, Avaya can uniquely identify the SAL Gateway at your location.

Use this procedure to register SAL Gateway and to generate the SAL Gateway identifiers through Global Registration Tool (GRT) without the use of any material codes.

Procedure

1. Open the GRT website at https://support.avaya.com/grt.

   The GRT website redirects you to the Avaya single sign-on (SSO) webpage.

2. Log in using your SSO ID and password.
3. On the GRT home page, click **Create New Registration** > **SAL Migration Only**.
4. In the **Sold To/Functional Location** field, enter the Sold To or customer functional location number that identifies the location where you want to deploy SAL Gateway.
5. On the Site Contact Validation page, complete the required contact information fields.

   Provide valid information so that Avaya can contact you to notify you about the registration status.

6. Click **Next**.

   The SAL Gateway Migration List page lists the SAL Gateway instances available for the Sold To number that you provided.

7. Click **Create New SAL Gateway**.

   GRT starts an automatic end-to-end registration of a new SAL Gateway and performs the install base creation process.

   After the install base creation is complete, GRT automatically proceeds to the first step of the technical onboarding process to generate the Solution Element ID and Product ID of SAL Gateway.

   The SAL Onboarding Summary page displays the Solution Element ID and Product ID generated for the new SAL Gateway. You also receive an email notification with the new IDs.

Next steps

- Complete the SAL Gateway installation process.
- Perform the technical onboarding process for devices that require support through the new SAL Gateway. See *Technical Onboarding Help Document* at https://support.avaya.com/registration.
- Add the devices as managed elements to your SAL Gateway using the SEIDs provided.

Chapter 4: Deploying Avaya Diagnostic Server

Avaya Diagnostic Server installation overview

The Avaya Diagnostic Server installation process includes the installation of the core components, SAL Gateway and the SLA Mon server on a target host. The procedures in this chapter are for a target host that does not have any earlier version of SAL Gateway or Avaya Diagnostic Server installed. This type of installation is called a clean installation.

For information on upgrading from an earlier version of SAL Gateway or Avaya Diagnostic Server, see Chapter 7, Upgrading Avaya Diagnostic Server.

Installation options

You can install one or both components of Avaya Diagnostic Server using the same installer.

You have the following deployment options for the Avaya Diagnostic Server components:

Install both components on the same server as coresident components.	Installing the SLA Mon server and SAL Gatewayon the same server exposes the host server to Avaya Services privileged access, such as shared logins, through the command line interface (CLI) of the operating system. Through the shared logins that include init, inads, and craft, Avaya Services can remotely log in, troubleshoot, and diagnose the SLA Mon server data without customer intervention. The shared logins might include the Linux **sudo** command-tracked privileged access to specific CLI commands to troubleshoot problems.
Install each component on separate servers.	If privileged access to the SAL Gateway server is a security concern, Avaya recommends that you install the SLA Mon server and SAL Gateway on separate servers. This deployment model ensures that SAL Gateway is remotely accessible through 2FA authentication only. For more information, see *Avaya Diagnostic Server Additional Security Configuration Guidance* available at http://support.avaya.com.

Installation methods

You can install Avaya Diagnostic Server using one of the following methods:

Attended installation	The installer runs in an interactive mode and proceeds with the installation according to your responses. To run the installer in this mode, you must log on

	to the RHEL host through Kernel-based Virtual Machine (KVM) or a virtual console.
Unattended installation	The installer performs the installation without any user interaction during the installation. The installer uses an input response file that contains the required user responses. You can run this mode through an SSH session to the RHEL host.

Installation prerequisites

Before you begin the installation of Avaya Diagnostic Server, you must perform the following:

- Ensure that the host server meets all specifications mentioned in Chapter 3, Installation prerequisites.
- Ensure that the JAVA_HOME variable is set on the host computer. Set the variable at the same location as the JRE installation.
- Ensure that you read the End User License Agreement (EULA) for installing and using Avaya Diagnostic Server. The complete EULA text is available in the `README.txt` file of the Avaya Diagnostic Server installer directory, `ADS-Installer-<version_no>-<build_no>`, which you extract from the downloaded package.

  Note:

  The EULA text is also available in the installation directory path `/opt/avaya/ads/LICENSE` in the .txt and .pdf formats as the following:

  - `License.pdf`
  - `Axeda Third Party License.pdf`
  - `README.txt`

Installing Avaya Diagnostic Server in the attended mode

Starting the Avaya Diagnostic Server installation in the attended mode

Before you begin

- Ensure that the host server meets all specifications mentioned in Chapter 3, Installation prerequisites.
- For the SLA Mon server component, if you choose to use a remote WebLM server, ensure that you have the IP address of the license server. You require the IP address to configure the license server during SLA Mon installation.

About this task

Use this procedure to start the Avaya Diagnostic Server installation process on a clean host through the attended mode. You must log on to the RHEL server through KVM or a virtual console to run the installer in this mode.

Procedure

1. Log on to the RHEL host on which you want to install Avaya Diagnostic Server as root through KVM or a virtual console.
2. Change to the directory where you downloaded and extracted the Avaya Diagnostic Server software.
3. Run the following command to start the installation in the attended mode:

   ./install.sh —attended
4. When the CLI-based installer displays the End User License Agreement (EULA) text for Avaya Diagnostic Server, type y to agree to the license, and press **Enter**.

   You must agree to the end user license to continue the installation of Avaya Diagnostic Server. If you type `n`, the installer quits.

   The system displays the results of the prerequisite checks that the installer performs. If the host meets the required prerequisites, the installer prompts you to select the components that you want to install.
5. When the system displays the options to select the components for installation, type one of the following, and press **Enter**:

   - `1`: To install only SAL Gateway.
   - `2`: To install only the SLA Mon server.
   - `3`: To install both components on the server.

   If you choose to install both components, the installer displays a message about the security implication of installing both components on the same server.

   The installer checks the host for hardware requirements according to the selected components. If the server does not meet the minimum requirements, the installer quits the installation. If the server does not meet the recommended requirements, the installer displays a warning message asking you whether to continue with the installation.
6. When the installer displays the security message, perform one of the following:

   - Type `y` to accept and continue with the installation.
   - Type `n` to decline and quit the installation.
7. To continue with the installation if the recommended hardware requirements are not met, type `y`.

Next steps

1. Complete the SAL Gateway installation steps.

2. Complete the SLA Mon server installation steps.

Completing the SAL Gateway installation

Starting the SAL Gateway installation

About this task

On selecting the option to install the SAL Gateway component in the Avaya Diagnostic Server installation console, the system displays the GUI of the SAL Gateway installer. Use this procedure to start the SAL Gateway installation.

Procedure

On the Welcome panel of the GUI-based installer, click **Next**.

The system displays the Packs Selection panel.

Next steps

Select the software packs that you want to install.

Selecting the software packs

Procedure

1. Select the **AgentGateway** check box if the check box is not selected.

   The system displays the size of the pack, the SAL Gateway description, the required space, and the available space.

2. Click **Next**.

   The system displays the Change system configuration files panel.

Next steps

Select the options to change the system configuration files.

Modifying the settings of the system configuration files

For SAL Gateway to function correctly, the system configuration files, including iptables and the syslog configuration file, require some changes. Use this procedure to indicate that you want the installer to make the required changes to the system configuration files.

Procedure

1. Select the **IPTABLE** check box.

   Caution:

   Failure to update iptables renders the SAL Gateway UI inaccessible and prevents SNMP traps from reaching SAL Gateway. If you clear the **IPTABLE** check box, you must update iptables manually.

2. Select the **SYSLOG** check box.

Note:

Syslog is the logging tool for SAL Gateway. If you select the **SYSLOG** check box, the SAL Gateway installer edits the syslog configuration file. If you clear the check box, you must edit the syslog configuration file after the installation. If you fail to edit the file, the SAL Gateway components might not write log messages in syslog after the installation.

3. Click **Next**.

   If you selected the **SYSLOG** check box, the SAL Gateway installer edits the syslog configuration file for the facilities Local0, Local4, and Local5. If these facilities are already configured for some other applications, the installer displays the following warning on the Installation Progress panel:

   ```
   SAL Gateway syslog log files are mixing with the customer syslog log
   files. Do you want to continue?
   ```

   Perform one of the following:

   - Click **No** to roll back the installation.
   - Click **Yes** to continue the installation.

   The system displays the Automatic Software Update Configuration panel.

Next steps

Select the option to activate or deactivate the automatic software update feature.

Setting the automatic software update configuration

About this task

From Avaya Diagnostic Server Release 2.0 onwards, SAL Gateway automatically receives software updates, including major, minor, and service pack releases. If you enable the Automatic Software Update feature, SAL Gateway automatically installs the downloaded software packages after a grace period. If you keep the feature disabled, you must install the downloaded software packages manually. You receive email notifications about download status, installation status, and other events related to the software updates.

Use this procedure to enable or disable the Automatic Software Update feature.

Note:

The Automatic Software Update feature is implemented through SAL Gateway. Therefore, this feature is available on Avaya Diagnostic Server that has both components, SAL Gateway and SLA Mon server, or only SAL Gateway installed. For Avaya Diagnostic Server with only the SLA Mon server, the Automatic Software Update feature is unavailable.

Procedure

1. On the Automatic Software Update Configuration panel, select one of the following:

   - **ON**: To enable the Automatic Software Update feature. If you do not install the downloaded software packages within the grace period set for the packages, the packages are applied to the Avaya Diagnostic Server components automatically.

- **OFF**: To disable the Automatic Software Update feature. You must install the downloaded software packages manually.

Note:

You cannot proceed to the next panel of the installer until you select ON or OFF from the field. You can change this configuration later through the SAL Gateway UI.

2. Click **Next**.

   The system displays the Mail Service Configuration panel.

Next steps

Configure the SMTP details for an email notification service.

Configuring SMTP details for the email notification service

About this task

Use this procedure to configure the Simple Mail Transfer Protocol (SMTP) server details that SAL Gateway uses to send email notifications. Correct SMTP details are necessary for notification about new software updates. On the configured mailbox, you receive email notifications about the download and implementation status of models, certificates, and software updates. You also receive notifications about backup failures.

Procedure

1. On the Mail Service Configuration panel, perform the following:
   a. In the **Host Name/ IP Address** field, enter the host name or the IP address of the SMTP server.
   b. In the **Port** field, enter the port number of the SMTP server.
   c. **(Optional)** If the SMTP server requires authentication, in the **Username** and the **Password** fields, enter the user name and the password for SMTP server authentication.
   d. In the **Administrator's Email Address** field, enter the administrator email address where you want to receive email notifications.
   e. **(Optional)** In the **Secondary Email Address** field, enter a secondary email address for email notifications.
2. Click **Next**.

   The system displays the Auto SEID Generation Option panel.

Next steps

Select the option to provide the Solution Element ID and the Alarm ID of SAL Gateway.

Selecting the option to specify Solution Element ID

About this task

Use this procedure to specify how you want to provide the Solution Element ID and the Alarm ID of SAL Gateway to the SAL Gateway installer.

Procedure

1. On the Auto SEID Generation Option panel, perform one of the following:
   - If you registered SAL Gateway with Avaya and received the Solution Element ID and the Alarm ID, select **Manually provide the Solution Element ID, Alarm ID**.
   - If you are yet to register SAL Gateway with Avaya, select **Auto-Create Solution Element ID, Alarm ID now**.

   Note:

   If you select **Auto-Create Solution Element ID, Alarm ID now**, ensure that you have FireFox 3.x or later as the default web browser on the RHEL host. Other web browsers, especially Konqueror, might not support the Automatic Registration Tool (ART) webpage that the system opens to generate the Solution Element ID.
2. If you select **Manually provide the Solution Element ID, Alarm ID**, click **Next**.

   The system displays the Identify SAL Gateway panel.
3. If you select **Auto-Create Solution Element ID, Alarm ID now**, perform the following:
   a. In the **Customer Functional Location No** field, enter the functional location (FL) number of the customer location where you want to install SAL Gateway.

      The FL number is also known as the Avaya Sold To number.
   b. Click **Next**.

      The system displays the ART Response panel.

      The default web browser opens an Avaya SSO webpage, where you must provide your SSO credentials to generate the Solution Element ID and the alarm ID.

Next steps

Perform one of the following:

- Manually configure the SAL Gateway identification information, including Solution Element ID and Alarm ID.
- Generate the Solution Element ID and the Alarm ID for SAL Gateway automatically.

Configuring the SAL Gateway identification information manually

Before you begin

Register SAL Gateway with Avaya and get the Solution Element ID and the Alarm ID.

About this task

Use this procedure only when you want to provide the SAL Gateway identification information manually.

Procedure

1. On the Identify SAL Gateway panel, complete the following fields for the SAL Gateway server identification:
   - **Solution Element ID**
   - **Alarm/Inventory ID**
   - (Optional) **IP Address**

   Note:

   SAL Gateway starts operations only if you provide the correct values.
2. Click **Next**.

   The system displays the Identify SAL Gateway User panel.

Next steps

Configure the SAL Gateway user and user group.

Identify SAL Gateway field descriptions

Name	Description
Solution Element ID	A unique identifier in the format (nnn)nnn-nnnn, where n is a digit from 0 through 9. Through this ID, Avaya can uniquely identify the particular product. In this case, the product is SAL Gateway. You receive this ID when you register the product with Avaya.
Alarm/Inventory ID	A unique 10-character ID, also known as Product ID, assigned to a product. In this case, the product is SAL Gateway. The alarms that the product generates contain the Alarm ID. Avaya uses the Alarm ID to identify the device that generates the alarm. You receive this ID when you register the product with Avaya.
IP Address	The IP address of the server where you want to install SAL Gateway. This field is optional. SAL Gateway supports both IPv4 and IPv6 addresses as input.

Generating the SEID and the Alarm ID of SAL Gateway automatically

Before you begin

On the Auto SEID Generation Option panel, select **Auto-Create Solution Element ID, Alarm ID now**.

For the customer functional location where you are installing SAL Gateway, ensure that you have an associated SSO login to gain access to Avaya service portals.

About this task

Use this procedure only when you want to generate the SAL Gateway identifiers automatically.

Procedure

1. On the SSO login page, log in using your SSO credentials.

   The system displays the Automatic Registration Tool (ART) webpage with an XML response.

   Note:

   If you cannot connect to the ART webpage, refresh the web browser to retry the connection. If an error occurs in ID generation, you might see the following responses:

   - If the ART database is not running:

     ```
     Error in opening db [unixODBC][FreeTDS][SQL Server]Unable to
     connect: Adaptive Server is unavailable or does not exist
     (SQL-08S01) [err was 1 now 1] [state was 08S01 now 08001]
     [unixODBC][FreeTDS][SQL Server]Unable to connect to data source
     (SQL-08001)
     ```

   - If ART did not generate the Alarm ID:

     ```
     Unique AlarmId failure error
     ```

   Return to the previous panel and enter the FL number again to reload the ART webpage.

2. Copy the complete XML response, and return to the ART Response panel of the installer wizard.
3. In the **ART Response** field , paste the copied XML response.

   Caution:

   While copying and pasting the XML response, ensure the following:

   - Do not miss any XML tags or characters from the response.
   - Do not include any additional characters to the response.

4. Click **Next**.

   If ID generation is successful, the system displays the Generated SEID Details for SAL Gateway panel with the Solution Element ID and the Alarm ID.

   Note:

   If the SSO credentials you used to generate the IDs are not associated with the specified functional location, the system displays the following error message:

   ```
   Your userid does not match with the Functional Location passed.
   ```

   Retry the SEID generation operation, or exit the installation.

5. **(Optional)** In the **IP Address** field, enter the IP address of the SAL Gateway host.
6. Click **Next**.

   The system displays the Identify SAL Gateway User panel.

Next steps

Configure the SAL Gateway user and user group.

Configuring the SAL Gateway user

About this task

Use this procedure to configure the user name and the user group of SAL Gateway. You can accept the default values that the installer provides or change the values.

Procedure

1. On the Identify SAL Gateway User panel, perform the following:
   a. In the **User Name** field, enter a new user name or keep the default user name, `saluser`.

      Note:

      If the user name exists in the system, the user name must have execute permissions to the Bash shell for the SAL Gateway services to run successfully.

   b. In the **User Group** field, enter a new user group name or keep the default user group, `salgroup`.
2. Click **Next**.

   The system displays the Concentrator Core Server Configuration panel.

   The installer uses the values in the Identify SAL Gateway User panel to create a user and a user group. SAL Gateway uses this user name to start the SAL Gateway services. The SAL user owns the SAL Gateway file system.

Next steps

Configure the Secure Access Concentrator Core Server information for communication with SAL Gateway.

Configuring the Concentrator Core Server information

About this task

Use this procedure to configure the Secure Access Concentrator Core Server information, including platform qualifier, host name, and port number, in SAL Gateway. SAL Gateway requires this information to connect to Concentrator Core Server for delivery of alarms and inventory information.

Procedure

1. On the Concentrator Core Server Configuration panel, in the **Platform Qualifier** field, keep the default value, `Enterprise-production`, unless Avaya explicitly instructs you to change the value.

2. In the **Primary destination** field, perform one of the following:
   - If you have a local Concentrator Core Server, enter the host name or the IP address of that server.
   - If you do not have a local Concentrator Core Server, keep the default value, `secure.alarming.avaya.com`, to communicate with Concentrator Core Server located at Avaya.
3. In the **Port** field, perform one of the following:
   - For a local Concentrator Core Server, enter the port number as `8443`.
   - For Concentrator Core Server located at Avaya, keep the default port value `443`.
4. Click **Next**.

   The system displays the Concentrator Remote Server Configuration panel.

   Note:

   If you use the default values, SAL Gateway connects to Concentrator Core Server located at Avaya.

Next steps

Configure the Secure Access Concentrator Remote Server information for communication with SAL Gateway.

Concentrator Core Server Configuration field descriptions

Name	Description
Platform Qualifier	An alphanumeric string to establish a channel for communication between SAL Gateway and Concentrator Core Server. The default platform qualifier is `Enterprise-production`. Do not change the default value unless Avaya explicitly instructs you to.
Primary destination	The fully qualified host name of Concentrator Core Server that SAL Gateway contacts for delivery of alarms and inventory information. The default value is `secure.alarming.avaya.com`, which is the address of Concentrator Core Server located at Avaya. If you have a local Concentrator Core Server, replace the default value with the host name or the IP address of that server. Otherwise, keep the default value to communicate with Concentrator Core Server located at Avaya.

Table continues…

Name	Description
Port	The port number of the primary destination. The default port number is `443`. For Concentrator Core Server located at Avaya, keep the default value. For a local Concentrator Core Server, replace the default value with `8443`.

Configuring the Concentrator Remote Server information

About this task

Use this procedure to configure the Secure Access Concentrator Remote Server information in SAL Gateway. SAL Gateway requires the information to contact Concentrator Remote Server to check for remote access requests and to provide remote access to managed products.

Procedure

1. On the Concentrator Remote Server Configuration panel, in the **Primary destination** field, perform one of the following:
   - To communicate with the Avaya Concentrator Remote Server, keep the default value, `remote.sal.avaya.com`.
   - If you have a local Concentrator Remote Server, enter the host name of that server.
2. In the **Port** field, perform one of the following:
   - For the Avaya Concentrator Remote Server, keep the default value, `443`.
   - For a local Concentrator Remote Server, enter the port number as `8443`.
3. Click **Next**.

   The system displays the Proxy Settings panel.

   If you use the default values, SAL Gateway connects to Concentrator Remote Server located at Avaya.

Next steps

If you use a proxy server for Internet access on the customer network, configure the proxy settings for SAL Gateway.

Concentrator Remote Server Configuration field descriptions

Name	Description
Primary destination	The host name of Concentrator Remote Server that manages the remote access requests to Avaya products through SAL Gateway. The default host name is `remote.sal.avaya.com`.
Port	The port number of the primary destination. The default port number is `443`.

Configuring the proxy settings for SAL Gateway

About this task

If you use a proxy server for Internet access outside the firewall of the customer network, use this procedure to configure the proxy server settings for SAL Gateway. SAL Gateway uses the proxy server to communicate securely with outside servers, including Secure Access Concentrator Core Server and Secure Access Concentrator Remote Server.

Note:

A proxy server is optional and depends on the customer network configuration. This proxy server works the same way that you use a proxy server for Internet browsing. If you have a company proxy server configured in your web browser, you might require to configure the proxy settings for SAL Gateway too.

Procedure

1. On the Proxy Settings panel, select the **Proxy Required** check box.

   The system displays the fields to configure the proxy settings.

2. In the **Type** field, click one of the following proxy server types according to the proxy configuration on the network:

   - **HTTP**: An HTTP proxy server without authentication.
   - **Authenticated HTTP**: An HTTP proxy server with authentication.
   - **SOCKS**: A SOCKS proxy server without authentication.

     Note:

     SAL does not support SOCKS proxies that use authentication.

3. In the **Hostname** field, type the host name or the IP address of the proxy server.
4. In the **Port** field, type the port number of the proxy server.
5. Click **Next**.

   If you select the **Authenticated HTTP** option, the system displays the Proxy Authentication Settings panel.

   Otherwise, the system displays the Model Package Installation panel.

6. **(Optional)** On the Proxy Authentication Settings panel, perform the following to complete the settings of the authenticated HTTP proxy server:

   a. Enter values in the following fields:

      - **User**
      - **Password**

   b. Click **Next**.

      The system displays the Model Package Installation panel.

Next steps

Download and apply the SAL model package using either the online or the offline mode.

Related links

Installing the SAL model package in the online mode on page 55
Installing the SAL model package in the offline mode on page 55

Installing the SAL model package in the online mode

About this task

A model is a collection of rules and configurations that defines how SAL Gateway provides services to a particular set of remotely managed products. During the SAL Gateway installation, you can download and apply the latest model package in two ways: online or offline.

Use this procedure to install the model package in the online mode. In the online mode, the SAL Gateway installer downloads the model package from Secure Access Concentrator Core Server that hosts the model package.

Note:

The installer downloads the models using the Concentrator Core Server URL:

`https://<hostname>:<port>/repository`

where <*hostname*> is the fully qualified host name and <*port*> is the port number of the primary Concentrator Core Server that you configured on the Concentrator Core Server configuration panel.

Procedure

1. On the Model Package Installation panel, select **Download latest models from Avaya or BusinessPartner**.
2. Click **Next**.

   The system displays the Policy Server Configuration panel.

   If the installer cannot connect with Concentrator Core Server, the system displays an online connection failure message.
3. On the message dialog box, perform one of the following:
   - Click **OK** to continue with the model installation in the offline mode.
   - Click **Cancel** to exit the installation.

Next steps

Configure the Secure Access Policy Server information.

Installing the SAL model package in the offline mode

About this task

A model is a collection of rules and configurations that defines how SAL Gateway provides services to a particular set of remotely managed products. During the SAL Gateway installation, you can download and apply the latest model package in two ways: online or offline.

Use this procedure to install the model package in the offline mode.

Note:

The Avaya Diagnostic Server software package contains the latest model package available at the time of the Avaya Diagnostic Server tar file creation. Unless a more recent model package is available online, use this model package to install the SAL models in the offline mode.

You can download the latest model package, which is a zip file, from the Concentrator Core Enterprise Server site:

`https://secure.alarming.avaya.com/repository/`

Procedure

1. On the Model Package Installation panel, select **Install the models from local drive**.
2. Click **Next**.

   The system displays the Model Package Selection panel.
3. In the **Path to Models Package** field, perform one of the following:
   - To use the model package that comes with the installer, accept the default path in the field.
   - To use a model package that you downloaded, click **Browse** to find and select the model package file.

   Note:

   Unless you have a model package that is more recent, accept the default `model.zip` package. The default package is available in the `/Models` subdirectory of the directory that gets created when you extract the tar file.
4. Click **Next**.

   The system displays the Policy Server Configuration panel.

Next steps

Configure the Secure Access Policy Server information.

Configuring the Policy Server information

About this task

If you have Policy Server installed on your network, use this procedure to configure the Policy Server with SAL Gateway. The use of Secure Access Policy Server is optional.

Procedure

1. On the Policy Server Configuration panel, perform the following:
   a. In the **Hostname** field, type the host name or the IP address of Policy Server.

      SAL Gateway takes both IPv4 and IPv6 addresses as input.
   b. In the **Port** field, type the port number that Policy Server uses to communicate with SAL Gateway.

2. Click **Next**.

   The system displays the SNMP SubAgent Configuration panel.

Next steps

Configure the SNMP master agent information for the SNMP subagent that SAL Gateway implements.

Configuring the SNMP master agent information

About this task

Use this procedure to configure the SNMP master agent information to which the SAL Gateway SNMP subagent requires connection.

Procedure

1. On the SNMP SubAgent Configuration panel, perform the following:
   a. In the **Master Agent Hostname** field, type the host name of the SNMP master agent.
   b. In the **Master AgentX Port** field, type the listener port number that the SNMP master agent uses with AgentX. The default port number is `705`.

   Note:

   The SNMP agent coexists with the master and subagents using the Agent Extensibility (AgentX) protocol. Changes in either or both values require a restart of the SAL Gateway SNMP subagent.

2. Click **Next**.

   The system displays the Administration access for Avaya panel.

Next steps

Specify a role for Avaya support personnel. The role defines the level of permissions for Avaya support personnel who might have to access SAL Gateway to provide services.

Assigning a role to Avaya support personnel

About this task

Use this procedure to assign a role to Avaya support personnel. The assigned role defines the access permissions for Avaya support personnel who might want to access the SAL Gateway UI to provide services.

Procedure

1. On the Administration access for Avaya panel, in the **Role** field, select one of the following roles:
   - **Administrator**

     Full permissions to all the SAL Gateway UI pages except the following pages, to which read only permission:

     - Policy Server

- PKI Configuration
- OCSP/CRL Configuration
- Certificate Management

The Administrator role excludes permissions to edit security settings. Only a Security Administrator can change security settings. The Security Administrator role is not available to Avaya support personnel.

- **Browse**

  Read-only access to all the SAL Gateway UI pages.

Note:

If you select **Deny** from the options, Avaya support personnel are denied access to the SAL Gateway UI.

2. Click **Next**.

   The system displays the Pack Installation Progress panel. The bars on the panel display the pack installation progress and the overall SAL Gateway installation progress. During pack installation, the installer copies, parses and executes files. The installer also creates the uninstaller pack and the uninstaller wrapper.

   When all the files are unzipped and installed, the system displays the Installation Summary panel. The panel displays the following information:

   - The installation status to show whether the installation process has completed successfully.
   - The package or packages that have been installed.
   - The version number of the installed SAL Gateway.
   - The location details of the Uninstaller program.

3. Click **Done**.

   The action completes the SAL Gateway installation process. The installer closes the GUI-based wizard and returns you to the CLI-based wizard.

Next steps

Complete the SLA Mon server installation steps.

Completing the SLA Mon server installation

The SLA Mon server installation process follows the installation of the SAL Gateway component of Avaya Diagnostic Server. If you choose not to install the SAL Gateway component, the installer directly starts the SLA Mon server installation after the system validation.

Before you begin

During the SLA Mon Server installation:

- If you choose not to reconfigure the firewall at the time of the SLA Mon server installation, then you must configure the iptables firewall rules for the communication ports used by SLA Mon. See Chapter 5, Post-installation configuration of Avaya Diagnostic Server.
- If you choose not to reconfigure the rsyslog files at the time of the SLA Mon server installation, the you must edit the rsyslog files manually to enable the SLA Mon server logging. See Chapter 5, Post-installation configuration of Avaya Diagnostic Server.

Procedure

1. When the CLI-based installer wizard prompts to import the SLA Mon public key into the RPM database, type `y`, and press **Enter**.

   The system displays a message to install the WebLM license server locally.

2. Perform one of the following:

   - To install the license server locally, type `y`.

     The system installs the WebLM license server locally.
   - To use a remote license server, type `n`, and when the system prompts you for the IP address of the license server, enter the IP address in the following format:

     <server_ip_address>:*<port>*

     Where, the :*<port>* part is optional. If the WebLM server does not use the default port, 52233, specify the port after the IP address in this format.

   The system displays a message to reconfigure the firewall rules for the SLA Mon server.

3. Perform one of the following:

   - To allow the installer script to reconfigure the firewall rules, type `y`.

     The system adds iptables firewall rules for the SLA Mon server.
   - To configure the firewall rules manually later, type `n`.

     The system displays a warning message and displays a message to reconfigure rsyslog.

4. Perform one of the following when the system displays a message to reconfigure rsyslog:

   - To allow the installer to reconfigure the syslog details, type `y`.
   - To configure the syslog details manually later, type `n`.

   The system starts the SLA Mon installation. The installer takes a few minutes to process the files and complete the installation.

Completing the attended installation of Avaya Diagnostic Server

After you complete the installation of the selected components, the Avaya Diagnostic Server installer completes the installation process. The installer displays the status of the processes and

also writes logs. At the end of the installation, the system closes the CLI-based wizard and returns to the command prompt.

Procedure

Check the system output for the Installation Complete message for the selected Avaya Diagnostic Server components to confirm that the installation is successful.

Note:

After the installation, check the logs at `/opt/avaya/ads/logging/ads-<version_no>-install.log` for installation details.

Result

The installer writes an uninstaller script in the `/opt/avaya/ads/uninstaller/` directory. You can use the uninstaller script if you want to uninstall Avaya Diagnostic Server.

Next steps

Complete the required post-installation configurations for each installed component.

Installing Avaya Diagnostic Server in the unattended mode

About this task

You can install Avaya Diagnostic Server by running the installer in the unattended mode remotely through an SSH session. If you do not have access to the console of the RHEL host through KVM or a virtual console, this method is useful.

Before you begin

Update the response file, `ADS_Response.properties`, with the required input responses for the installation properties and the preferences. You must replace the default or representative values in the file with values that suit the installation environment.

The following are some of the properties that you must set:

- For the `ADS_AGREELICENSE` property in the response file, replace the value `n` with `y`.
- For the SAL Gateway component, ensure that you make the following changes in the response file:
  - Replace the value of `AUTOUPGRADE_CUST_SELECT` with `ON` or `OFF`. The `ON` or `OFF` value must be in the uppercase.
  - In the SMTP Configuration fields section, update the SMTP server details with correct and complete values. You must provide values for the `SMTP_HOST`, `SMTP_PORT`, and `SMTP_ADMIN_EMAIL` properties.
  - Choose a mode for model package installation by removing the hash sign (#) before the appropriate lines.
- For the SLA Mon server component, if you want to use a remote WebLM licensing server, update the IP address of the WebLM server in the response file.

Note:

The response file is available in the location where you extracted the Avaya Diagnostic Server software package. The file path is `/<folder_path to the extracted package>/ADS-Installer-<version_no>-<build_no>/ADS_Response.properties`.

For more information about the input response properties in the response file, see ADS_Response.properties file on page 61.

Procedure

1. Log on to the RHEL host on which you want to install Avaya Diagnostic Server as root.
2. Go to the directory where you downloaded and extracted the Avaya Diagnostic Server software package.
3. Run the following command to start the installation in the unattended mode:

   `./install.sh` `-unattended`

   The installer checks the host to verify whether the host meets the installation prerequisites. Then, the installer starts processing the installation files and continues with the installation of Avaya Diagnostic Server according to the inputs that you provided in the response file.

Result

When the installation is complete, the system displays a successful installation message for the components that you selected to install.

Related links

ADS_Response.properties file on page 61

ADS_Response.properties file

The Avaya Diagnostic Server installer uses the `ADS_Response.properties` file as the input response file for an unattended installation or upgrade. In the unattended mode, the installer uses the information in the response file as inputs to complete the process without needing further human intervention.

Before you install Avaya Diagnostic Server in the unattended mode, you must update the response file with values that the installer will require during the installation or upgrade. The installer package of Avaya Diagnostic Server comes with the `ADS_Response.properties` file. You can find this file at the same location where you extracted the installer package.

Caution:

The values in the file are only representative examples and not accurate. You must change the values in this file to values that suit your environment. If you do not enter correct values in the file, an unattended upgrade or installation might result in an unstable system. In addition, you must provide values for the properties that are marked as mandatory. Otherwise, the unattended installation cannot continue.

Important:

You must edit the file using a Linux text editor, such as VI or EMACs, for correct maintenance of the content. Do not edit the file in a Windows text editor.

The following table provides information about the properties that you must set in the response file for an unattended installation:

Information in the file	Description
`#Agree ADS end user license agreement` `ADS_AGREELICENSE=n`	To continue with the installation, change the value to `y`. **Important:** Ensure that you read the End User License Agreement (EULA) for installing and using Avaya Diagnostic Server. The complete EULA text is available in the `README.txt` file in the installer directory, `ADS-Installer-<version_no>-<build_no>`.
`#Following value will tell the installer which component to be installed (1) SAL gateway, 2) SLA Mon server, 3) Both` `ADS_COMPONENT_TO_INSTALL=3`	For a fresh installation of Avaya Diagnostic Server, the installer checks this property. Set the value of `ADS_COMPONENT_TO_INSTALL` to one of the following: • `1`: To install Avaya Diagnostic Server with SAL Gateway only. • `2`: To install Avaya Diagnostic Server with SLA Mon only. • `3`: To install Avaya Diagnostic Server with both components.
If Avaya Diagnostic Server 2.5 is already installed with one component and you want to install the other component, edit the following properties. If you are not installing a new component, keep the default values.	

`#Following properties are for fresh-installation of an individual component when no existing component needs to be upgraded`
 	
`# ADS 2.5 component SAL is already installed do you wish to install SLAMon (y/n)`
`ADS_SLAMON_INSTALL=y`
`# ADS 2.5 component SLAMon is already installed do you wish to install SAL (y/n)`
`ADS_SAL_INSTALL=y`
	Ensure that the value of one of the following properties is `y`:
	• `ADS_SLAMON_INSTALL=y` if SAL Gateway is available and you want to install the SLA Mon server.
	• `ADS_SAL_INSTALL=y` if the SLA Mon server is available and you want to install SAL Gateway.

Update the properties in the following section only if you want to upgrade from SAL 2.0, 2.1, or 2.2 to Avaya Diagnostic Server 2.5. Also, use this section when you upgrade from Avaya Diagnostic Server 1.0 or 2.0 to Avaya Diagnostic Server 2.5. Based on the software version available in your environment, set one of the	

Table continues…

Information in the file	Description
properties in this section. You can leave the rest of the properties in this section with the default values. For a fresh installation, leave these properties with the default values.	

`#Following properties are for upgrade scenarios.`
 	
`# SAL 2.0, 2.1, or 2.2 is installed. Which component to be installed 1) Upgrade SAL 2) Upgrade SAL and install SLAMon.`
`SAL_UPGRADE_TO_ADS=1`
	To upgrade from SAL 2.0, 2.1, or 2.2 to Avaya Diagnostic Server 2.5, set the value of `SAL_UPGRADE_TO_ADS` to one of the following:
	• For SAL upgrade only, the value must be `1`.
	Example: `SAL_UPGRADE_TO_ADS=1`
	• For SAL upgrade and SLA Mon installation, the value must be `2`.
	Example: `SAL_UPGRADE_TO_ADS=2`

`#ADS [1.0/2.0] component SAL is already installed. Which components to be installed 1) Upgrade SAL 2) Upgrade SAL and Install SLAMON` `ADS_SAL_UPGRADE=1`	To upgrade from Avaya Diagnostic Server 1.0 or 2.0 with SAL to 2.5, set the value of `ADS_SAL_UPGRADE` to one of the following: • For SAL upgrade only, the value must be `1`. Example: `ADS_SAL_UPGRADE=1` • For SAL upgrade and SLA Mon installation, the value must be `2`. Example: `ADS_SAL_UPGRADE=2`
`#ADS [1.0/2.0] component SLAMon is already installed. Which components to be installed 1) Upgrade SLAMon 2) Upgrade SLAMon and Install SAL` `ADS_SLAMON_UPGRADE=1`	To upgrade from Avaya Diagnostic Server 1.0 or 2.0 with SLA Mon to 2.5, set the value of `ADS_SLAMON_UPGRADE` to one of the following: • For SLA Mon upgrade only, the value must be `1`. Example: `ADS_SLAMON_UPGRADE=1` • For SLA Mon upgrade and SAL installation, the value must be `2`. Example: `ADS_SLAMON_UPGRADE=2`
`#ADS [1.0/2.0] components SAL and SLAMon are already installed Do you wish to Upgrade SAL and SLAMon. (y/n)` `ADS_SAL_SLAMON_UPGRADE=y`	If you have Avaya Diagnostic Server 1.0 or 2.0 with both components on the host, set the value of `ADS_SAL_SLAMON_UPGRADE` as `y` to upgrade to Avaya Diagnostic Server 2.5. **Note:** If some earlier versions of SAL Gateway and SLA Mon server are installed on the host, set this property as `y` to upgrade both components as part of Avaya

Table continues…

<table>
<tr><th>Information in the file</th><th>Description</th></tr>
<tr><td></td><td>Diagnostic Server 2.5. The installer does not support upgrade of only one component when both components are installed.</td></tr>
<tr><td colspan="2">Set the property in the following section of the file to allow SAL Gateway and the SLA Mon server to reside on the same server. You must set this property for a fresh installation or an upgrade operation that results in both components to be coresident.

Important:

Installing the SLA Mon server and SAL Gateway on the same server exposes the host server to Avaya Services privileged access, such as shared logins, through the CLI of the operating system. Through the shared logins that include init, inads, and craft, Avaya Services can remotely log in, troubleshoot, and diagnose the SLA Mon server data without customer intervention. The shared logins might include the Linux sudo command-tracked privileged access to specific CLI commands to troubleshoot problems. If privileged access to the SAL Gateway host server is a security concern, Avaya recommends that you install the SLA Mon server and SAL Gateway on separate servers. This deployment model ensures that SAL Gateway is remotely accessible through 2FA authentication only. For more information, see Avaya Diagnostic Server Additional Security Configuration Guidance available at http://support.avaya.com.</td></tr>
<tr><td><pre>#Following properties are to allow SAL and SLAMon components to exist on the same server(co-resident)
#(Note : Installing SLAMon and SAL Gateway applications on the same server exposes SAL Gateway to Avaya services privileged access such as shared logins (init, inads and craft) via the Command Line Interface (CLI) of the Operating System. The shared services logins will allow Avaya Services to remotely login, troubleshoot and diagnose data as collected by the SLAMon server without customer intervention and may include Linux "sudo" command tracked privileged access if needed to troubleshoot a problem. If shared logins/ Avaya privileged access to the SAL Gateway server is a security concern then it is highly recommended that you install the SLAMon and SAL Gateway application on separate servers. This deployment model ensures that the SAL Gateway application installed on a separate server is remotely accessible via 2-FA authentication only. For additional information, see the Avaya Diagnostic Server Additional Security Configuration Guidance document available at support.avaya.com.)
AGREE_ADS_COMPONENTS_CORESIDENT=n</pre></td><td>To agree to the security implication of having both components coresident, set the value as <tt>y</tt>. If you keep the value as <tt>n</tt>, the installer quits the installation process.</td></tr>
<tr><td colspan="2">Set the following properties to continue with an upgrade to Avaya Diagnostic Server 2.5 even if the host server does not meet the minimum hardware requirements.

Important:

The option to upgrade without meeting the minimum requirements is provided to facilitate backup of existing system configuration. The Avaya Diagnostic Server services might not function at full capacity on such a server. After you take backup, you must restore the configuration data on another server that meets</td></tr>
</table>

Table continues…

Information in the file	Description
the minimum requirements completely. You cannot install a new component on a server that does not meet the minimum requirements.	
`#ADS [1.0] components SAL and SLAMon are already installed. Do you want to proceed with the upgrade of SLAMon and SAL if minimum hardware checks fail. (y/n)` `ADS_SAL_SLAMON_UPGRADE_PROCEED_ON_HW_CHECKS_FAIL=n`	The installer uses this property when Avaya Diagnostic Server 1.0 is installed with both components. To continue with the upgrade even if the host does not meet one or more minimum hardware requirements, including disk space and memory, set the value as `y`. If you keep the value as `n`, the installer quits the upgrade process when a minimum hardware check fails.
`#ADS [1.0] component SAL is already installed. Do you want to proceed with upgrade of SAL if minimum hardware checks fail. (y/n)` `ADS_SAL_UPGRADE_PROCEED_ON_HW_CHECKS_FAIL=n`	The installer uses this property when Avaya Diagnostic Server 1.0 is installed with the SAL Gateway component. To continue with the upgrade even if the host does not meet one or more minimum hardware requirements for Avaya Diagnostic Server with SAL Gateway, set the value as `y`. If you keep the value as `n`, the installer quits the upgrade process when a minimum hardware check fails.
`#ADS [1.0] component SLAMon is already installed. Do you want to proceed with upgrade of SLAMon if minimum hardware checks fail. (y/n)` `ADS_SLAMON_UPGRADE_PROCEED_ON_HW_CHECKS_FAIL=n`	The installer uses this property when Avaya Diagnostic Server 1.0 is installed with the SLA Mon component. To continue with the upgrade even if the host does not meet one or more minimum hardware requirements for Avaya Diagnostic Server with SLA Mon, set the value as `y`. If you keep the value as `n`, the installer quits the upgrade process when a minimum hardware check fails.
`# SAL 2.0, 2.1, or 2.2 is installed. Do you want to proceed with upgrade of SAL if minimum hardware checks fail. (y/n)` `SAL_UPGRADE_TO_ADS_PROCEED_ON_HW_CHECKS_FAIL=n`	The installer uses this property when SAL Gateway 2.0, 2.1, or 2.2 is installed on the host. To continue with the upgrade even if the host does not meet one or more minimum hardware requirements for Avaya Diagnostic Server with SAL Gateway, set the value as `y`. If you keep the value as `n`, the installer quits the upgrade process when a minimum hardware check fails.
Set the appropriate one of the following properties to continue with the installation of Avaya Diagnostic Server with the chosen components if the RAM size or the hard disk space does not meet the recommended requirement.	

Table continues…

Information in the file	Description
Note: For upgrade scenarios, the installer checks for the recommended hardware requirements only if you are upgrading from a version earlier than Avaya Diagnostic Server 2.0.	
`#Proceed with installation of SLAMon if recommended requirement for RAM is not met (y/n)` `ADS_SLAMON_PROCEED_ON_RAM_CHECK_FAIL=n`	The installer uses this property when you choose to install Avaya Diagnostic Server with SLA Mon only. You can set the property as the following: • `ADS_SLAMON_PROCEED_ON_RAM_CHECK_FAIL=y`: To continue with the installation of SLA Mon if RAM is less than the recommended 8 GB but greater than the minimum requirement of 4 GB. • `ADS_SLAMON_PROCEED_ON_RAM_CHECK_FAIL=n`: To quit the installation if RAM is less than the recommended value.
`#Proceed with installation of SLAMon if recommended requirement for Hard-disk free space is not met (y/n)` `ADS_SLAMON_PROCEED_ON_HD_CHECK_FAIL=n`	The installer uses this property when you choose to install Avaya Diagnostic Server with SLA Mon only. You can set the property as the following: • `ADS_SLAMON_PROCEED_ON_HD_CHECK_FAIL=y`: To continue with the installation of SLA Mon if free disk space is less than the recommended 180 GB but greater than the minimum requirement of 50 GB. • `ADS_SLAMON_PROCEED_ON_HD_CHECK_FAIL=n`: To quit the installation if free disk space is less than the recommended value.
`# Proceed with installation of SAL if recommended requirement for Hard-disk is not met (y/n)` `ADS_SAL_PROCEED_ON_HD_CHECK_FAIL=n`	The installer uses this property when you choose to install Avaya Diagnostic Server with SAL Gateway only. You can set the property as the following: • `ADS_SAL_PROCEED_ON_HD_CHECK_FAIL=y`: To continue with the installation of SAL Gateway if free disk space is less than the recommended 40 GB but greater than the minimum requirement of 10 GB. • `ADS_SAL_PROCEED_ON_HD_CHECK_FAIL=n`: To quit the installation if free disk space is less than the recommended value.

Table continues…

Information in the file	Description
`# Proceed with installation of SAL if recommended requirement for RAM is not met (y/n)` `ADS_SAL_PROCEED_ON_RAM_CHECK_FAIL=n`	The installer uses this property when you choose to install Avaya Diagnostic Server with SAL Gateway only. You can set the property as the following: • `ADS_SAL_PROCEED_ON_RAM_CHECK_FAIL=y`: To continue with the installation of SAL Gateway if RAM is less than the recommended 4 GB but greater than the minimum requirement of 2 GB. • `ADS_SAL_PROCEED_ON_RAM_CHECK_FAIL=n`: To quit the installation if RAM is less than the recommended value.
`# Proceed with installation of SAL and SLAMon if recommended requirement for Hard-disk is not met (y/n)` `ADS_PROCEED_ON_HD_CHECK_FAIL=n`	The installer uses this property when you choose to install Avaya Diagnostic Server with both SAL Gateway and SLA Mon. You can set the property as the following: • `ADS_PROCEED_ON_HD_CHECK_FAIL=y`: To proceed with the installation if free disk space is less than the recommended 230 GB but greater than the minimum requirement of 50 GB. • `ADS_PROCEED_ON_HD_CHECK_FAIL=n`: To quit the installation if free disk space is less than the recommended value.
`# Proceed with installation of SAL and SLAMon if recommended requirement for RAM is not met (y/n)` `ADS_PROCEED_ON_RAM_CHECK_FAIL=n`	The installer uses this property value when you choose to install Avaya Diagnostic Server with both SAL Gateway and SLA Mon. You can set the property as the following: • `ADS_PROCEED_ON_RAM_CHECK_FAIL=y`: To proceed with the installation if RAM is less than the recommended 8 GB but greater than the minimum requirement of 4 GB. • `ADS_PROCEED_ON_RAM_CHECK_FAIL=n`: To quit the installation if RAM is less than the recommended value.
The following are responses that the installer uses while installing the SLA Mon server component. If you choose to install the Avaya Diagnostic Server with SAL Gateway only, keep the default values.	
`#Importing SLAMon public key into RPM database (y/n)` `IMPORTKEY=y`	Keep the default value `y`.

Table continues…

Information in the file	Description

`#Install licensing server (WebLM) locally (y/n)`
`WEBLMLOCAL=n`
 	
`#WebLM server IP address This is mandatory field if you selected WEBLMLOCAL=n`
`WEBLMIP=127.0.0.1`
	Set the value of `WEBLMLOCAL` as one of the following:
	• `y`: To install a WebLM licensing server for SLA Mon on the Avaya Diagnostic Server host as part of the installation.
	• `n`: To use a WebLM server that is already installed on your network. Also replace the dummy value of `WEBLMIP` with the IP address of the installed WebLM server.

`# If following values are true then SLAMon Installer update the IPTABLE and SYSLOG (y/n)`
`IPTABLES=y`
`SYSLOG=y`
	For the SLA Mon features to function correctly, some changes are required in the iptables and syslog configurations. Do one of the following:
	• If you want the installer to make the required changes in the iptables and syslog configurations, set the values of `IPTABLES` and `SYSLOG` as `y`.
	• If you want to configure the syslog and firewall rules later, set the values of the properties as `n`.

The following are responses that the installer uses while installing or upgrading SAL Gateway. If you choose to install Avaya Diagnostic Server with SLA Mon only, keep the default values.	
`# pack name is fixed` `packs=AgentGateway`	The pack name is fixed. Do not change this information.

`#If it is a Services-VM/SP box then this variable should be set to true`
`IS_VSP=false`
 	
`#Specify the platform Type as SERVICES_VM or VAPP if IS_VSP is set to true, default is set to STANDALONE`
`GW_TYPE=STANDALONE`
	If you are installing the Avaya Diagnostic Server software as a standalone server on a RHEL host, keep the value of `IS_VSP` as `false`, and keep `GW_TYPE` as `STANDALONE`.
	If you are packaging Avaya Diagnostic Server for Services-VM or as an OVA, set the value of `IS_VSP` as `true`, and set the value of `GW_TYPE` as `SERVICES_VM` or `VAPP`, accordingly.

`# If following values are true then Gateway Installer update the IPTABLE and SYSLOG`
`# For RHEL 5.x, ensure that the syslogd option in the /etc/sysconfig/syslog file reads as:`
`SYSLOGD_OPTIONS="-r -m 0"`
`# For RHEL 6.x, ensure that the following two lines in the /etc/rsyslog.conf file are uncommented, that is, no # sign remains at the start of the lines:`
`# $ModLoad imudp.so`
`# $UDPServerRun 514`
`IPTABLESelect=true`
`SYSLOGSelect=true`
	Keep the values of `IPTABLESelect` and `SYSLOGSelect` as `true`.
	If the installation fails due to some syslog errors, you can change the value for `SYSLOGSelect` to `false` and reinstall Avaya Diagnostic Server.
	If you set the value for `SYSLOGSelect` to `false`, you must edit the syslog configuration file manually after the installation. If you fail to edit the file, the SAL Gateway components

Table continues…

Information in the file	Description
	might not write log records in syslog after the installation. **Note:** Based on the RHEL version, complete the additional syslog configuration as stated in the section.
`#Automatic Software Update Configuration,To enable the feature provide "ON"/"OFF" mandatory field AUTOUPGRADE_CUST_SELECT=SELECT`	Change the value of `AUTOUPGRADE_CUST_SELECT` to one of the following: • `ON`: To enable the Automatic Software Update feature. Software updates including major, minor and service pack releases are downloaded to SAL Gateway automatically. When you activate Automatic Software Update, the downloaded software packages are installed automatically if you do not install the packages within the grace period set for the packages. • `OFF`: To disable the Automatic Software Update feature. Software packages are still downloaded automatically. However, you must install the downloaded software packages manually. **Note:** The ON or OFF value must be in the upper case. If you keep the value as `SELECT`, the installer quits the installation process.

`#SMTP Configuration fields please provide valid details mandatory fields`
`SMTP_HOST=`
`SMTP_PORT=`
`SMTP_ADMIN_EMAIL=`
`#SMTP Configuration fields please provide valid details optional fields (if value of SMTP_USER_NAME is provided then SMTP_PASSWORD is a mandatory field)`
`SMTP_USER_NAME=`
`SMTP_PASSWORD=`
`SMTP_SECONDARY_EMAIL=`
	Both installation and upgrade of SAL Gateway require valid SMTP details. The following properties are mandatory:
	
	• `SMTP_HOST`: The host name or the IP address of the SMTP server. The installer takes both IPv4 and IPv6 addresses as input.
	
	• `SMTP_PORT`: The port number of the SMTP server.
	
	• `SMTP_ADMIN_EMAIL`: The email address of the administrator to whom email notifications must be sent.
	
	The following SMTP properties are optional:
	
	• `SMTP_USER_NAME`: The name of the user to be authenticated. Enter a value only when

Table continues…

Information in the file	Description
	the SMTP server is configured to authenticate users. • SMTP_PASSWORD: The password of the user. If you provide the value of SMTP_USER_NAME, SMTP_PASSWORDbecomes a mandatory field. • SMTP_SECONDARY_EMAIL: A secondary email address where you want to receive email notifications.

# Agent Gateway Configuration mandatory fields 	
GATEWAY_SOLUTION_ELEMENTID=(000)777-9999
 	
# SPIRIT_ALARMID must be 10 digit number. 	
SPIRIT_ALARMID=1234567890
 	
#Keeping it blank as installer discovers actual IP address automatically.
AGENTGATEWAY_IPADRESS=
	Replace the representative values of GATEWAY_SOLUTION_ELEMENTID and SPIRIT_ALARMID with the actual Solution Element ID and the Alarm or Product ID received from Avaya at SAL Gateway registration.
	For the procedure to obtain these IDs of SAL Gateway, see the procedure in the Registering SAL Gateway section.
	You need not enter a value for AGENTGATEWAY_IPADRESS. The installer automatically discovers the actual IP address of the host server.
	Note:
	You can install SAL Gateway with the default IDs. However, for the SAL Gateway services to start, you must configure the correct Solution Element ID and Product ID after the installation through the SAL Gateway UI.

# Select the USER_ACCOUNT and USER_GROUP of Agent Gateway mandatory fields 	
AGENTGATEWAY_USERNAME=saluser
AGENTGATEWAY_USERGROUP=salgroup
	For the Gateway services to run successfully, the user name provided, if existing, must have the execute permissions to the Bash shell.
	The installer uses these values to create a user and a user group. SAL Gateway uses this user name to start the SAL Gateway services. The SAL user owns the SAL Gateway file system.

Avaya Enterprise Configuration mandatory fields PRIMARY_AVAYA_ENTERPRISE_IDENTIFIER=Enterprise-production PRIMARY_AVAYA_ENTERPRISE_URL=secure.alarming.avaya.com PRIMARY_AVAYA_ENTERPRISE_PORT=443 PRIMARY_AXEDA_ENTERPRISE_URL=remote.sal.avaya.com PRIMARY_AXEDA_ENTERPRISE_PORT=443	Unless explicitly instructed, do not change these default values.

Table continues…

Information in the file	Description

`Customer Proxy Configuration Optional fields`
`ProxySelect=false`
`CUSTOMER_PROXY_TYPE=HTTP`
`CUSTOMER_PROXY_HOSTNAME=`
`CUSTOMER_PROXY_PORT=`
`CUSTOMER_PROXY_USER=`
`CUSTOMER_PROXY_PASSWORD=`
	The use of the customer proxy server is optional and depends on your local configuration.
	You can make the following changes to use a proxy server:
	• Change the value for `ProxySelect` to `true`.
	• According to your requirement, set the value of `CUSTOMER_PROXY_TYPE` to one of the following:
	- `HTTP`: For HTTP proxy without authentication
	- `AuthenticatedHTTP`: For HTTP proxy with authentication
	- `SOCKS`: For SOCKS proxy without authentication
	• For `HOSTNAME`, `PORT`, `USER`, and `PASSWORD`, specify the values according to your proxy server settings.

`# Model Package Installation fields(Online)`
`#MODEL_RADIO_SELECTION=ONLINE`
`#GATEWAY_trustHost=false`
 	
`# Model Package Installation fields(Offline)`
`MODEL_RADIO_SELECTION=OFFLINE`
	For model package installation, you can specify one of the following two modes:
	• ONLINE: The installer communicates with Concentrator Core Server to download and install the latest model package available. To choose the ONLINE mode, you must remove the hash (#) sign before the two properties that follow the line `Model Package Installation fields(Online)` and comment out the property that follow the line `# Model Package Installation fields(Offline)`
	For example:
	`# Model Package Installation fields(Online)`
	`MODEL_RADIO_SELECTION=ONLINE`
	`GATEWAY_trustHost=false`
	`# Model Package Installation fields(Offline)`
	`#MODEL_RADIO_SELECTION=OFFLINE`
	• OFFLINE: The installer retrieves the model package from the location specified by the `MODELS_INSTALL_PATH` attribute in the file. Ensure that the first two properties in this

Table continues…

Information in the file	Description
	section are commented out but `MODEL_RADIO_SELECTION=OFFLINE` is not commented out. **Note:** The ONLINE and OFFLINE values must be in upper case.
`#Any local Path to Models package` `MODELS_INSTALL_PATH=./../models/models.zip`	For the OFFLINE mode of model package installation, the installer uses this path to the model package that comes with the installer. Do not change this path unless you have a model package that is later than the one with the installer. You must download the model package from the global URL of the Enterprise server, for example, https://secure.alarming.avaya.com/repository/. If you download a later package, replace the package that came with the installer with the latest package. You can locate the default package in the `models` subdirectory in the `ADS-Installer-<version_no>-<build_no>` directory that was extracted from the tar file. For example, `/tmp/ADS-Installer-2.5.0.0-103/models`.

`# Policy Server Configuration Optional fields`
`POLICY_SERVER_HOSTNAME=`
`POLICY_SERVER_PORT=`
	To use a policy server, you must enter the host name and port number of the policy server in the appropriate fields. If you do not have a policy server, you can leave the values blank.

`# SNMP SubAgent Configuration Optional fields`
`SNMP_SERVER_HOSTNAME=127.0.0.1`
`SNMP_SERVER_PORT=705`
	The SNMP subagent requires the host name or the IP address and the port number of the SNMP master agent to register with the master agent. You can configure these values after the installation through the SAL Gateway UI.

`# Assign Role to Avaya Technician mandatory field` `AVAYA_TECH_ASSIGNED_ROLE=Administrator`	This response is to define the access permission of Avaya support personnel to the SAL Gateway UI. You can set one of the following values: • `Administrator`: Full permissions to all the UI pages, except a few. Administrator have read-only access to Policy Server, PKI Configuration, OCSP/CRL Configuration, and Certificate Management pages. • `Browse`: Ready-only access to the UI pages.

Table continues…

Information in the file	Description
`# Language selection code mandatory field localeISO3=eng`	English is the language that the installer supports. Do not change the default value.

Note:

When you install Avaya Diagnostic Server in the unattended mode, and your devices and the host computer on which you want to install Avaya Diagnostic Server are configured with IPv6 settings, replace the default IPv4 values with IPv6 values in the response file.

Related links

Installing Avaya Diagnostic Server in the unattended mode on page 60

Chapter 5: Post-installation configuration of Avaya Diagnostic Server

Post-installation configuration for SAL Gateway

Updating iptables

About this task

If you did not select the option to configure iptable rules during the SAL Gateway installation, use this procedure to update the iptables after the installation. For SAL Gateway to function properly, you must update the iptable rules.

Procedure

1. Log on to the SAL Gateway host as the root user.
2. Update the iptables with the following commands:

   ```
   /sbin/iptables -I INPUT -i lo -j ACCEPT
   /sbin/iptables -I INPUT -p tcp -m tcp --dport 5108 -j ACCEPT
   /sbin/iptables -I INPUT -p tcp -m tcp --dport 5107 -j ACCEPT
   /sbin/iptables -I INPUT -p udp -m udp --dport 162 -j ACCEPT
   /sbin/iptables -I INPUT -p tcp -m tcp --dport 7443 -j ACCEPT
   /sbin/iptables -I INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
   ```

3. Run the following command to save the iptables configuration:

   ```
   /sbin/service iptables save
   ```

4. Run the following command to restart the iptables:

   ```
   /sbin/service iptables restart
   ```

5. Run the following commands for IPv6 tables:

   ```
   /sbin/ip6tables -I INPUT -i lo -j ACCEPT
   sbin/ip6tables -I INPUT -p tcp -m tcp --dport 5108 -j ACCEPT
   ```

```
/sbin/ip6tables -I INPUT -p tcp -m tcp --dport 5107 -j ACCEPT
/sbin/ip6tables -I INPUT -p udp -m udp --dport 162 -j ACCEPT
/sbin/ip6tables -I INPUT -p tcp -m tcp --dport 7443 -j ACCEPT
/sbin/ip6tables -I INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
```

6. Run the following command to save the iptables configuration:

   ```
   /sbin/service ip6tables save
   ```

7. Run the following command to restart the iptables:

   ```
   /sbin/service ip6tables restart
   ```

Setting up additional firewall rules for remote administration of SAL Gateway

SAL Gateway requires additional firewall rules for its remote administration. These rules are not required for the proper functioning of SAL Gateway, but are necessary for remote access and troubleshooting.

Procedure

1. Log on to the SAL Gateway host as the root or SAL user.
2. For remote administration of SAL Gateway, run the following commands:

   ```
   /sbin/iptables -I INPUT -p icmp -m icmp --icmp-type any -j ACCEPT
   /sbin/iptables -I INPUT -p tcp -m tcp --dport 22 -j ACCEPT
   ```

3. Run the following command to save the iptables configuration:

   ```
   /sbin/service iptables save
   ```

4. Run the following command to restart the iptables service:

   ```
   /sbin/service iptables restart
   ```

5. For remote administration of SAL Gateway with IPv6 rules, run the following commands:

   ```
   /sbin/ip6tables -I INPUT -p ipv6-icmp -j ACCEPT
   /sbin/ip6tables -I INPUT -p tcp -m tcp --dport 22 -j ACCEPT
   ```

6. Run the following command to save the ip6tables configuration:

   ```
   /sbin/service ip6tables save
   ```

7. Run the following command to restart the ip6tables service:

   ```
   /sbin/service ip6tables restart
   ```

Editing RHEL syslog file

Editing the syslog configuration file for RHEL 5.x

About this task

On an RHEL 5.x system, the installer edits the `/etc/syslog.conf` file to store the log messages of SAL Gateway in the appropriate files. Syslog stores log data in a file based on the facility and priority of the data. The `syslog.conf` file stores the facility and priority information as facility.priority. The SAL Gateway components use the following three facilities to write logs:

- Local0
- Local4
- Local5

The installer performs the required syslog configuration for SAL Gateway. If you did not select the **SYSLOG** check box on the Change system configuration files panel during the installation, you must edit the syslog configuration file manually. Use this procedure to ensure that the log messages from the SAL Gateway components are stored in the appropriate log files.

Procedure

1. Log on to the SAL Gateway host as the root user.
2. Open the `/etc/syslog.conf` file, and verify whether the file contains the following entries:

```
local4.*        /var/log/SALLogs/audit.log
local5.*        /var/log/SALLogs/messages.log
local0.*        /var/log/SALLogs/remoteAccess.log
```

3. If the syslog configuration file does not contain the mentioned lines, add the lines to the file.
4. To enable remote agent logging on the local server, ensure that the syslogd option in the `/etc/sysconfig/syslog` file reads as:

   ```
   SYSLOGD_OPTIONS="-r -m 0"
   ```

5. Run the following command to restart the syslog service and to make the changes effective:

   ```
   service syslog restart
   ```

Editing the syslog configuration file for RHEL 6.x

About this task

On an RHEL 6.x system, the SAL Gateway edits the `/etc/rsyslog.conf` file to store the log messages from the SAL Gateway components in the appropriate files. If you did not select the **SYSLOG** check box on the Change system configuration files panel during the installation, you must edit the `/etc/rsyslog.conf` file manually.

Use this procedure to ensure that the log messages from the SAL Gateway components are stored in the appropriate log files.

Procedure

1. Log on to the SAL Gateway host as the root user.

2. Open the `/etc/rsyslog.conf` file, and verify whether the file contains the following entries:

```
local4.*        /var/log/SALLogs/audit.log
local5.*        /var/log/SALLogs/messages.log
local0.*        /var/log/SALLogs/remoteAccess.log
```

3. If the syslog configuration file does not contain the mentioned lines, add the lines to the file.
4. To enable remote agent logging on the local server, ensure that the following two lines in the `/etc/rsyslog.conf` file are uncommented, that is, no # sign remains at the start of the lines:

```
$ModLoad imudp.so
$UDPServerRun 514
```

5. Run `service rsyslog restart` to restart the rsyslog service and make the changes effective.

Post-installation configuration for the SLA Mon server

User configuration for 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 the 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 the 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 the `eqmAdmin` group is optional. The installer creates the `eqmAdmin` group during the SLA Mon server installation. Create the `eqmAdmin` group only if the installer does not create the user group.
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.

SSL protocol configuration for 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. Open the `/opt/avaya/slamon/tomcat/conf/server.xml` file, and edit the connector for SLA Mon, as shown in 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"
   SSLEnabled="true"
   clientAuth="want"
   sslProtocol="TLSv1"
   keyAlias="slamon"
   keystorePass="avaya123"
   keystoreFile="/opt/avaya/slamon/misc/slamon-ui-keystore.jks"
   truststorePass="avaya123"
   truststoreFile="/opt/avaya/slamon/misc/slamon-ui-truststore.jks"
   sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2"
   ciphers="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_AES_128_CBC_
   SHA,TLS_RSA_WITH_AES_128_CBC_SHA,SSL_RSA_WITH_3DES_EDE_CBC_SHA,SSL_DHE_DSS_WITH_3DE
   S_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 need not 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 <certificate_validity_in_days> -keystore slamon-ui-keystore.jks -storepass <keystore_password>
   ```

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

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

Note:

Keep the -validity option in a similar time range as the SLA Mon license, so that the root CA certificate also expires at similar time. The typical SLA Mon license expires in 3 years.

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

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

   Note:

   The CSR file `slamon.csr` in the command is different from the CSR that you generate for a certificate for the server-agent communication.

6. Run the following command to import the certificate chain signed by a signing authority from a well-known CA, such as VeriSign® or Symantec, or your in-house CA in response to the CSR. You can also import a self-signed certificate.

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

   Note:

   Ensure that the *<keystore_password>* values you provide for `keypass` and `storepass` are the same.

7. Edit the `/opt/avaya/slamon/tomcat/conf/server.xml` file, and change `keystorePass="avaya123"` to the password that you used to generate the key pair.

   Note:

   In the server.xml file, `avaya123` is the default value for `keystorePass`. If the keystore password was updated earlier, the value might be different than `avaya123`. Replace the value with the password 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

After you receive a signed certificate chain from the CA, you must import the certificate chain 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 SLA Mon server host as root, and run the following command to stop the SLA Mon web service:

   service slamonweb stop

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

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

3. Run the following command:

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

   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. Replace <*keystore_password*> with the password for the SLA Mon UI keystore.

4. Run the following command to restart the web service:

   service slamonweb start

Certificate management for communication between the server and an agent

For any communication between the SLA Mon server and the agent that resides in Avaya products, including endpoints, Media Gateways, and switches, you must import a certificate to the server keystore and the agent truststore. For more details about managing certificates, see Chapter 6, Managing certificates for the communication between the server and agent, in *Administering Avaya Diagnostic Server with SLA Mon*™.

Editing syslog for SLA Mon

Editing the syslog configuration file for RHEL 5.x

About this task

On an RHEL 5.x system, the installer edits the `/etc/syslog.conf` file to store log messages of the SLA Mon server in the appropriate files. Syslog stores log data in a file based on the facility and priority of the data. The `syslog.conf` file stores the facility and priority information as facility.priority. The SLA Mon components use two facilities to write logs:

- local2
- local3

Note:

If some other applications are using the facilities, local2 and local3, the system combines the other application logs with the SLA Mon server logs.

The installer performs the required syslog configuration for SLA Mon at the time of installation. If you decided not to configure the syslog service at the time of the installation, you must edit the syslog configuration file manually. Use this procedure to edit the syslog file and to ensure that the log messages from the SLA Mon server are stored in the appropriate log files.

Procedure

1. On the SLA Mon host, open the `/etc/syslog.conf` file, and verify whether the file contains the following entries:

```
local2.* /var/log/slamon/eqmaudit.log
local3.* /var/log/slamon/eqmoperational.log
```

2. If the syslog configuration file does not contain the mentioned lines, add the lines to the file.
3. To enable remote logging, ensure that the syslogd option in the `/etc/sysconfig/syslog` file reads as the following:

```
SYSLOGD_OPTIONS="-r -m 0"
```

4. Run the following command to restart the syslog service and to make the changes effective:

```
service syslog restart
```

Editing the syslog configuration file for RHEL 6.x

About this task

On an RHEL 6.x system, the SLA Mon server edits the `/etc/rsyslog.conf` file to store the log messages from the SLA Mon components in the appropriate files.

If you decided not to configure the rsyslog files at the time of the SLA Mon server installation, you must edit the `/etc/rsyslog.conf` file manually.

Use this procedure to ensure that the log messages from the SLA Mon components are stored in the appropriate log files.

Procedure

1. On the SLA Mon host, open the `/etc/rsyslog.conf` file, and verify whether the file contains the following entries:

```
local2.* /var/log/slamon/eqmaudit.log
local3.* /var/log/slamon/eqmoperational.log
```

Note:

If some other applications are already using the facilities local2 and local3, the system might mix logs from other applications with the SLA Mon server logs.

2. If the syslog configuration file does not contain the mentioned lines, add the lines to the file.

3. To enable remote logging, ensure that the following two lines in the `/etc/rsyslog.conf` file are uncommented, that is, no hash sign (#) remains at the start of the lines:

   ```
   $ModLoad imudp.so
   $UDPServerRun 514
   ```

4. Run the following command to restart the rsyslog service and make the changes effective:

   `service rsyslog restart`

Updating iptables for SLA Mon

About this task

If you did not choose to configure the firewall during the SLA Mon server installation, you must configure the firewall manually. Use this procedure to configure the iptables rules for the communication ports used by the SLA Mon server.

Procedure

1. Log on to the Avaya Diagnostic Server with administrative privileges.
2. Run the following commands to update the iptables for the SLA Mon server:

   `/sbin/iptables -I INPUT -p udp --dport 50011 -j ACCEPT`

   `/sbin/iptables -I INPUT -p tcp --dport 50011 -j ACCEPT`

   `/sbin/iptables -I OUTPUT -p udp --dport 50011 -j ACCEPT`

   `/sbin/iptables -I INPUT -p udp --dport 50010 -j ACCEPT`

   `/sbin/iptables -I OUTPUT -p udp --dport 50010 -j ACCEPT`

   `/sbin/iptables -I INPUT -p udp --dport 50009 -j ACCEPT`

   `/sbin/iptables -I OUTPUT -p udp --dport 50009 -j ACCEPT`

   `/sbin/iptables -A INPUT -p tcp -m tcp --dport 4511 -j ACCEPT`

3. **(Optional)** If you installed WebLM locally during the SLA Mon server installation, run the following command to open the port to communicate with the WebLM server from outside:

   `/sbin/iptables -A INPUT -p tcp -m tcp --dport 52233 -j ACCEPT`

4. Run the following command to save the iptables configuration:

   `/sbin/service iptables save`

5. Run the following command to restart the iptables service:

   `/sbin/service iptables restart`

   Note:

   Do not use system-config-securitylevel-tui to update the iptables rules.

Registering the SLA Mon and WebLM servers with SAL

Registering a product with Avaya and SAL is a process that uniquely identifies the product so that Avaya can service the product remotely. To provide service and support to registered customers, Avaya assigns a Solution Element ID and a Product ID to the product. This data is critical for the correct execution of various Avaya business functions and tools.

About this task

You can register a device with SAL Gateway for remote support through Global Registration Tool (GRT). During the technical onboarding part of the registration process through GRT, a Solution Element ID is generated automatically for the device. If alarm transfer from the device is possible, a Product ID is also generated.

Before you begin

Ensure that you know the Solution Element ID of the SAL Gateway through which you want to provide remote access to the devices. If your SAL Gateway is unavailable for selection during device registration, you can add the new SAL Gateway using the Solution Element ID as part of the process.

Procedure

Through GRT, perform the technical onboarding process for each device.

For more information, see *Technical Onboarding Help Document* at https://support.avaya.com/registration.

Next steps

Add the devices to SAL Gateway as managed elements using the Solution Element IDs.

Adding the SLA Mon and WebLM servers as managed elements to SAL Gateway

About this task

SAL Gateway can provide remote access and alarm transfer facilities to devices that are added as managed elements to SAL Gateway. SAL Gateway controls remote access connections to managed elements and verifies certificates for authentication.

Before you begin

- Ensure that you have an authorized user ID to log on to the SAL Gateway web interface.
- Ensure that you have registered your device with Avaya and received the Solution Element ID and Product ID numbers of the device from Avaya.

Procedure

1. Open the SAL Gateway web interface using the following URL:

   `https://[host name or IP address of SAL Gateway]:7443`

The system displays the login page.

2. Enter the authorized user ID and password to log in.
3. In the navigation pane of the SAL Gateway user interface, click **Secure Access Link Gateway** > **Managed Elements**.
4. On the Managed Element page, click **Add New**.

   The system displays the Managed Element Configuration page.
5. In the **Solution Element ID** field, type the Solution Element ID of the device that you want to add as a managed element.

   The format of the ID is (NNN)NNN-NNNN, where N is a digit from 0 to 9.

   Note:

   The details of devices that you register using GRT for support through SAL become available to SAL Gateways present in the network. When you enter a Solution Element ID for which device information is available to SAL Gateway, SAL Gateway automatically populates additional fields, such as Product ID and SAL model.
6. In the **Product ID** field, type the product ID or the alarm ID of the device.

   If SAL Gateway automatically populates this field after you provide the Solution Element ID, the field becomes read only.

   Caution:

   Exercise caution when you enter the product ID of a device. If the product ID of the device differs from the one you entered on the SAL Gateway UI, the auto-onboarding process resets the product ID of the device to match the product ID provided on the SAL Gateway UI. For some products, the product ID reset process restarts the services on the device and results in service interruptions on the devices during auto-onboarding.
7. Perform the following to select a model for the product:
   a. In the **Model** field, click the model that is applicable to the product.

      Note:

      If the SLA Mon or the WebLM model is not available in the **Model** field, see SLA Mon and WebLM models are not present when adding as managed elements to SAL Gateway on page 139.

      If SAL Gateway automatically populates the **Model** and the **Product** fields after you provide the Solution Element ID, the fields become read only.

      The system displays the **Product** field in accordance with the selected model.
   b. In the **Product** field, click an appropriate option from the list of supported product versions.
   c. **(Optional)** To view the applicable products under a model, select the model, and click **Show model applicability**.
8. In the **Host Name** field, type the host name of the managed device.

9. In the **IP Address** field, type the IP address of the managed device. SAL Gateway takes both IPv4 and IPv6 addresses as input.
10. If you want to use a Network Interface Unit (NIU) port for remote access, select the **NIU** check box and select a value from the list box. The value must be in the range of 0 to 9.
11. Select the **Provide remote access to this device** check box if you want to provide the ability to connect to the managed device remotely.
12. Select the **Transport alarms from this device** check box if you want SAL Gateway to receive alarms from this device.

    If the model you select does not support alarming, the **Transport alarms from this device** check box is unavailable on the user interface.
13. Click **Add**.

Next steps

For the configuration changes to take effect, restart the SAL Gateway services. You can perform this task on the Apply Configuration Changes page.

Important:

Restarting the SAL Gateway services terminates all established connections and might result in SNMP traps being missed. To minimize disruption of services, apply configuration changes only after you complete all configurations on SAL Gateway.

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

Note:

In Avaya Diagnostic Server 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 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

About this task

Use this procedure to install the SLA Mon server license 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.

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.

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. However, in WebLM OVA, the value provided is a hashed value of the MAC address and the IP address of the WebLM server.
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 is 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 on the SLA Mon server

About this task

Use this procedure to change the WebLM server IP address configured on the SLA Mon server. If you enter a wrong WebLM server IP address when installing the SLA Mon component or want to point to a new WebLM server, you can use this procedure to replace the current WebLM server address with the new one.

Procedure

1. Log on to the Avaya Diagnostic Server host as a user with administrative privileges.
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:

   service slamonsrvr restart

   Note:

   After you start the slamonsrvr service, wait for maximum 3 minutes to start the slamonweb service. The waiting time can be less depending on the number of agents the server discovers after you start the service.

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

   service slamonweb restart

   The system updates the WebLM server IP address on the SLA Mon server.

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. Do one of the following:
   - Run the following command to change the WebLM server address:

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

   - Run the following command to change the WebLM server address and port:

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

Where, <*WebLM IP address*> is the IP address of the new WebLM server and <*port*> is the new port you want to use for accessing the 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 Step 5 of the procedure, Changing the WebLM server address.

Managing the authentication file

Access Security Gateway and the authentication file

Access Security Gateway (ASG) ensures that Avaya Services have privileged access to a customer device in a secure manner. ASG uses a challenge and response protocol to validate the user and to reduce unauthorized access. An ASG user uses a predetermined user ID to provide service at the customer site. ASG challenges this user ID, and the user must provide a proper response to log in successfully. The ASG user can use the response to a challenge only one time.

Authentication is successful only when the product and ASG communicate with a compatible key. ASG creates customer-specific ASG keys that are stored in an authentication file. With ASG keys, Avaya Services can securely access the customer system.

The SLA Mon server component of Avaya Diagnostic Server supports privileged access by Avaya Services to the host server through ASG. A default authentication file is installed with the SLA Mon server component. The default authentication file has an authentication file ID (AFID) of 7100000015. You must replace the default file with a unique authentication file for your site to allow Avaya Services and BusinessPartners to access your system.

Note:

You can create unique authentication files through Authentication File System (AFS) at http://rfa.avaya.com/. AFS is available only to Avaya Services personnel and Avaya BusinessPartners. If you are a customer in need of an authentication file, contact Avaya or your authorized BusinessPartner.

Salient points of Avaya Services privileged access to the SLA Mon server

- Avaya Services privileged access opens the host server to shared logins through the CLI of the operating system. Through the shared logins, including init, inads, and craft, Avaya Services personnel can remotely log in, troubleshoot, and diagnose the SLA Mon server data without customer intervention. The shared logins include the Linux **sudo** command-tracked privileged access to run specific commands to troubleshoot a problem.
- ASG users can perform the following:
  - Run operations, such as start, stop, restart, and status check, on the SLA Mon services. For example:

    ```
    service slamonsrvr status
    service slamondb restart
    service slamonweb stop
    ```
  - Install an authentication file through the **asgloadauth** script. For example:

    ```
    asgloadauth /tmp/<authfile_name>
    ```
- ASG users can log in to the SLA Mon CLI session by directly running the **slamoncli** command. In a CLI session, the user can use the `/tmp` folder to save and upload a file.

Important:

Installing the SLA Mon server and SAL Gateway on the same server exposes the SAL Gateway host server to Avaya Services privileged access. If privileged access to the SAL Gateway server is a security concern, Avaya recommends that you install the SLA Mon server and SAL Gateway on separate servers. By deploying SAL Gateway on a separate server, you can ensure that SAL Gateway is remotely accessible through the 2FA authentication only.

Installing an authentication file

Before you begin

Create and download the authentication file from AFS.

Note:

If you are a customer in need of an authentication file, contact Avaya or your authorized BusinessPartner.

About this task

Use this procedure to install an ASG authentication file for the SLA Mon server.

Procedure

1. Log on to the Avaya Diagnostic Server host as root or using an ASG shared login, such as init, inads, or craft.
2. Copy the authentication file to the `/tmp` directory on the host.

   If you are copying the file from a remote system, you can use the following:

   - From a Linux remote system: Use the **scp** command to copy the file to the host.

- From a Windows remote system: Use WinSCP or a similar file transfer utility to copy the file to the host.

3. Run the **asgloadauth** script as the following:

   asgloadauth /tmp/*<auth_filename>*

   Where *<auth_filename>* is the name of the authentication file to be loaded.

   The system uploads the specified authentication file and validates the file. If the file is valid, the system installs the authentication file.

Chapter 6: Verifying the Avaya Diagnostic Server implementation

Verification of the SAL Gateway implementation

You can run a number of tests to verify whether the SAL Gateway installation is successful. The verification is to ensure that the SAL Gateway services, including SAL Watchdog, alarming, remote access, and the SAL Gateway UI, are running properly.

Testing the SAL Watchdog service

About this task

The SAL Watchdog service routinely tests the operational state of all SAL Gateway components and restarts the components in case of any abnormal shutdowns. Use this procedure to verify that the Watchdog service is running properly.

Procedure

1. Log on to the host server as root.
2. Run the following command, and check the outcome of the command:

   ```
   service salWatchdog status
   ```

3. If the service is not running, run the following command to start the service:

   ```
   service salWatchdog start
   ```

4. Check the status again to verify that the service is running.

Testing the alarming service of SAL Gateway

About this task

Use this procedure to verify that the alarm transfer service of SAL Gateway is running properly. Through this service, SAL Gateway forwards alarms from Avaya devices to NMS, Avaya, or a certified partner to monitor the alarm activities better.

Procedure

1. Log on to the host server as root.

2. Run the following command, and check the outcome of the command:

   service spiritAgent status

3. If the service is not running, run the following command to start the service:

   service spiritAgent start

4. Check the status again to verify that the service is running.

Testing the remote access service of SAL Gateway

About this task

Use the following procedure to test whether the remote access service of SAL Gateway is running properly.

Procedure

1. Log on to the host server as root.
2. Run the following command, and check the outcome of the command:

   service axedaAgent status

3. If the service is not running, run the following command to start the service:

   service axedaAgent start

4. Check the status again to verify that the service is running properly.

Testing the SAL Gateway UI

About this task

You can administer the SAL Gateway configurations through the web interface for the remote connectivity and alarm transfer facilities. Use this procedure to ensure that the SAL Gateway web interface is available.

Procedure

1. From another terminal on the network where SAL Gateway is deployed, open a web browser.
2. In the address bar, type the following URL:

   `https://<IP address of the Avaya Diagnostic Server host>:7443`

   You can replace the host IP with the DNS host name if the host server is registered under DNS.

   The browser displays the SAL Gateway login page.

3. **(Optional)** If the SAL Gateway login page does not open, perform the following:
   a. Log on to the Avaya Diagnostic Server host as admin, and switch to the root user.
   b. Run the following command to check the status of the gatewayUI service:

      service gatewayUI status
   c. If the service is not running, run the following command to start the service:

      service gatewaUI start
   d. Check the status again to verify that the service is running properly.

Verification of the SLA Mon implementation

You can run a number of tests to verify that the implementation of the SLA Mon component of Avaya Diagnostic Server is successful. The verification includes ensuring that the SLA Mon server service, database service, and web interface service are running correctly.

Note:

The SLA Mon server component of Avaya Diagnostic Server is licensed. After you deploy the Avaya Diagnostic Server virtual appliance, you get a 30-days trial period to use the SLA Mon server. You must get a valid license to use the SLA Mon server before the trial period is over. For more information about managing the SLA Mon server license, see *Deploying Avaya Diagnostic Server.*

Testing the slamonsrvr service

About this task

Use this procedure to confirm whether the SLA Mon server service is running.

Procedure

1. Log on to the Avaya Diagnostic Server host as root.
2. Run the following command, and check the outcome of the command:

   service slamonsrvr status

   Expected output sample:

   `SLAMon Server Running (<Process ID>)`
3. If the service is not running, run the following command to start the service:

   service slamonsrvr start

Testing the slamonweb service

About this task

Use this procedure to confirm whether the web interface service of SLA Mon is running.

Procedure

1. Log on to the Avaya Diagnostic Server host as root.
2. Run the following command, and check the outcome of the command:

   service slamonweb status

   Expected output sample:

   `Avaya Diagnostic Server Slamon web 2.5 is running (<process id>)`
3. If the service is not running, run the following command to start the service:

   service slamonweb start

Testing the slamondb service

About this task

Use this procedure to confirm whether the database service of the SLA Mon server is running.

Procedure

1. Log on to the Avaya Diagnostic Server host as root.
2. Run the following command, and check the outcome of the command:

   service slamondb status

   Expected output sample:

   ```
   postmaster (pid 21287 21286 21285 21284 21282 21280 15031 15027
   10402 10387 10370) is running
   ```
3. If the service is not running, run the following command to start the service:

   service slamondb start

Chapter 7: Upgrading Avaya Diagnostic Server

Upgrade paths to Avaya Diagnostic Server 2.5

The Avaya Diagnostic Server 2.5 installer supports a direct upgrade capability from Avaya Diagnostic Server 1.0 and 2.0, and some earlier releases of SAL Gateway. For SAL Gateway releases that do not support a direct upgrade, you must upgrade to a later release of SAL Gateway that supports direct upgrade by using one of the following upgrade paths:

Product release	Upgrade path
SAL Gateway 1.5	Upgrade to SAL Gateway 2.1 before upgrading to Avaya Diagnostic Server Release 2.5.
SAL Gateway 1.8	Upgrade to SAL Gateway 2.1 before upgrading to Avaya Diagnostic Server Release 2.5.
SAL Gateway 2.0	Supports direct upgrade to Avaya Diagnostic Server Release 2.5.
SAL Gateway 2.1	Supports direct upgrade to Avaya Diagnostic Server Release 2.5.
SAL Gateway 2.2	Supports direct upgrade to Avaya Diagnostic Server Release 2.5.
SAL Gateway 2.2 virtual appliance	Upgrade to Avaya Diagnostic Server 2.0 virtual appliance, and then perform in-place upgrade to Avaya Diagnostic Server 2.5. **Note:** When upgrading to Avaya Diagnostic Server 2.0 virtual appliance, ensure that on the ADS Components page, **SAL Gateway** or **Both** is selected for installation. For more information about upgrading from SAL Gateway 2.2 virtual appliance to Avaya Diagnostic Server 2.0 virtual appliance, see *Deploying Avaya Diagnostic Server 2.0 using VMware® in the Virtualized Environment*.
Avaya Diagnostic Server 1.0	Supports direct upgrade to Avaya Diagnostic Server Release 2.5.
Avaya Diagnostic Server 2.0	Supports direct upgrade to Avaya Diagnostic Server Release 2.5.
Avaya Diagnostic Server 2.0 virtual appliance	Supports direct upgrade to Avaya Diagnostic Server Release 2.5. **Note:** You can upgrade Avaya Diagnostic Server 2.0 virtual appliance to Avaya Diagnostic Server 2.5 using only the unattended mode of upgrade. The steps to upgrade the virtual appliance are similar to

Table continues…

Product release	Upgrade path
	the steps in a standalone software-only upgrade of Avaya Diagnostic Server.

Note:

If Avaya Diagnostic Server 2.0 is installed with SAL Gateway, you can upgrade to Avaya Diagnostic Server 2.5 through the automatic software update feature in SAL Gateway. After the Avaya Diagnostic Server 2.5 installer becomes available, SAL Gateway automatically downloads the installer from Avaya. If the automatic software update feature is enabled, you can wait for the system to automatically install the software update. The system automatically installs the software update after the grace period, which is defined in the package, is over. Otherwise, you can apply the downloaded Avaya Diagnostic Server 2.5 package manually.

Minimum hardware requirements for upgrade

The minimum hardware requirements to upgrade to Avaya Diagnostic Server 2.5 are the same as the requirements for a clean installation of Avaya Diagnostic Server 2.5. For information about the hardware requirements, see Chapter 3, Installation prerequisites.

You can upgrade to Avaya Diagnostic Server 2.5 even without the minimum hardware requirements. However, the host must meet a bare-minimum disk space requirement as mentioned in the following table.

Important:

You cannot install a new component during such an upgrade. Avaya provides you this option so that you can upgrade from an earlier version of SAL Gateway or Avaya Diagnostic Server to the latest version. You can then use the backup and restore facility of Avaya Diagnostic Server to migrate to another server that meets the minimum requirements completely. If you do not migrate, you might not be able to use all features of Avaya Diagnostic Server.

Only SAL Gateway	1024 MB of free disk space
Only SLA Mon server	2048 MB of free disk space • 1024 MB in `/opt` and 1024 MB in `/var/lib/` if both directories are mounted on different file systems.
Cohosted components	3072 MB of free disk space • 2048 MB in `/opt` and 1024 MB in `/var/lib/` if both directories are mounted on different file systems.

Checklist for upgrading from SAL Gateway Release 1.5 or 1.8

The following checklist provides the high-level steps to upgrade from SAL Gateway Release 1.5 or 1.8 to Avaya Diagnostic Server Release 2.5.

No.	Task	Description	Notes	✔
1	Ensure that you have root privileges to the host server and that you log in as the root user to perform the upgrade operations.		Do *not* log in as saluser or use the `su` command to switch the user from saluser to root for an upgrade operation. Upgrade attempts through both login methods result in upgrade failure because the installer tries to kill any active processes owned by saluser.	
2	Ensure that the SAL Gateway host meets the minimum hardware requirements, such as RAM and disk space, for Avaya Diagnostic Server 2.5.	See Hardware and software requirements on page 33.	You can continue to upgrade to Avaya Diagnostic Server 2.5 even without the minimum hardware requirements. However, the host must meet a minimum disk space requirement. See Minimum hardware requirements for upgrade on page 99. You cannot install a new component during such an upgrade. After the upgrade, you must use the backup and restore facility of Avaya Diagnostic Server to migrate to another server that meets the minimum requirements completely. If you do not migrate, you might not be able to use all features of Avaya Diagnostic Server.	
3	Install JRE 1.6.	See Installing Java 1.7 using an archive binary on page 144.	**Caution:** Do not uninstall the earlier versions of JRE until you successfully upgrade to Avaya Diagnostic Server 2.5. Some other software on the server might also use the existing JRE	

Table continues…

No.	Task	Description	Notes	✔
			version. Install the new JRE version at a different location.	
4	Update the JAVA_HOME environment variable to point to JRE 1.6, and export JAVA_HOME in the `/root/.bashrc` file. Also, update the `.bashrc` file of the SAL Gateway user, saluser, to point to JRE 1.6.	See Updating the Java environment variable after a JRE upgrade on page 147.	**Caution:** Perform this step only when you are ready to upgrade to SAL Gateway Release 2.1 immediately. If you plan to upgrade the system at some future time, do not perform this step.	
5	From PLDS, download the SAL Gateway 2.1 software that you require for the interim upgrade, and extract the files to a local directory on the host server.	See Downloading software from PLDS on page 39.		
6	Upgrade to SAL Gateway 2.1.	See *Secure Access Link 2.1 Gateway Implementation Guide* on the Avaya Support website at http://support.avaya.com/.		
7	Validate that the upgrade operation is successful.	Log on to the web interface of the SAL Gateway component to check whether the configuration information persists after the upgrade. In addition, see Chapter 6, Verifying the Avaya Diagnostic Server implementation.		
8	Complete the steps to upgrade to Avaya Diagnostic Server 2.5.	See Checklist for upgrading from SAL Gateway 2.0 or later and Avaya Diagnostic Server 1.0 or 2.0 on page 102.		

Checklist for upgrading from SAL Gateway 2.0 or later and Avaya Diagnostic Server 1.0 or 2.0

The following checklist provides the high-level steps to upgrade from SAL Gateway Release 2.0, 2.1, or 2.2, and Avaya Diagnostic Server Release 1.0 or 2.0 to Avaya Diagnostic Server Release 2.5.

No.	Task	Description	Notes	✔
1	Ensure that you have root privileges to the host server and that you log in as the root user to perform the upgrade operations.		Do *not* log in as saluser or use the `su` command to switch the user from saluser to root for an upgrade operation. Upgrade attempts through both login methods result in upgrade failure because the installer tries to kill any active processes owned by saluser.	
2	Ensure that the host meets the minimum hardware requirements, such as RAM and disk space, for Avaya Diagnostic Server 2.5.	See Hardware and software requirements on page 33.	You can continue to upgrade to Avaya Diagnostic Server 2.5 even without the minimum hardware requirements. However, the host must meet a minimum disk space requirement. See Minimum hardware requirements for upgrade on page 99. You cannot install a new component during such an upgrade. After the upgrade, you must use the backup and restore facility of Avaya Diagnostic Server to migrate to another server that meets the minimum requirements completely. If you do not migrate, you might not be able to use all features of Avaya Diagnostic Server.	
3	Install Oracle JRE 1.7.	See Installing Java 1.7 using an archive binary on page 144.	**Caution:** Do not uninstall the earlier versions of JRE until you successfully upgrade to Avaya Diagnostic Server 2.5. Some other software on the server might also	

Table continues…

No.	Task	Description	Notes	✔
			use the existing JRE version. Install the new JRE version at a different location.	
4	Update the JAVA_HOME environment variable to point to JRE 1.7, and export JAVA_HOME in the `/root/.bashrc` file. Also, update the `.bashrc` file of the SAL Gateway user, saluser, to point to JRE 1.7.	See Updating the Java environment variable after a JRE upgrade on page 147.	**Caution:** Perform this step only when you are ready to upgrade to Avaya Diagnostic Server Release 2.5 immediately. If you plan to upgrade the system at some future time, do not perform this step.	
5	Download the Avaya Diagnostic Server 2.5 software package from PLDS, and extract the files to a local directory on the host server.	See Downloading software from PLDS on page 39 and Extracting the Avaya Diagnostic Server software files to a local directory on page 40.		
6	Copy and extract the downloaded `ADS-Installer-2.5.0.0-<xxxx>.tar.gz` file to a local directory on the host server.	See Extracting the Avaya Diagnostic Server software files to a local directory on page 40.		
7	Upgrade to Avaya Diagnostic Server 2.5.	See Upgrading Avaya Diagnostic Server in the attended mode on page 104 or Upgrading Avaya Diagnostic Server in the unattended mode on page 108.		
8	Validate that the upgrade operation is successful.	Log on to the web interfaces of the components to check whether the configuration information persists after the upgrade. In addition, see Chapter 6, Verifying the Avaya Diagnostic Server implementation.		

Upgrading Avaya Diagnostic Server in the attended mode

About this task

Use this procedure to upgrade to Avaya Diagnostic Server Release 2.5 in the attended mode from SAL Gateway Release 2.x or Avaya Diagnostic Server Release 1.0 or 2.0. You must log on to the RHEL server through KVM or a virtual console to run the installer in the attended mode.

Before you begin

- Copy and unzip the downloaded Avaya Diagnostic Server software file, `ADS-Installer-<version_no>-<build_no>.tar.gz`, to a directory on the host server.
- Install JRE 1.7. Set the JAVA_HOME environment variable to point to JRE 1.7 in the `/root/.bashrc` file. Set the variable also in the `.bashrc` file of the user who owns the file system and the services associated with SAL Gateway. The default user is `saluser`.
- Ensure that the host server meets all other system requirements mentioned in Chapter 3, Installation prerequisites.
- Ensure that the SAL Gateway data on the Managed Element Configuration page is in accordance with the data on the Gateway Configuration page. Take this precaution to avoid any error on the Gateway Configuration page after the upgrade.

Procedure

1. Log on to the host server through KVM or a virtual console as root.

   Note:

   Do *not* log in as saluser or use the **su** command to switch the user from saluser to root for an upgrade operation. Upgrade attempts through both login methods result in upgrade failure because the installer tries to kill any active processes owned by saluser.

2. Go to the directory where you downloaded and extracted the Avaya Diagnostic Server software package.
3. From the command line, run the following command:

   ./install.sh `-attended`

   The system starts the installation in the attended mode.

4. Read the End User License Agreement text for Avaya Diagnostic Server, type `y` to agree to the license, and press **Enter**.

   If you type `n`, the installer quits the process.

   The installer checks the host to verify whether the host meets the prerequisites. The installer also checks for any earlier version of SAL Gateway or Avaya Diagnostic Server on the host server. If the installer detects an earlier software version that supports a direct upgrade, the installer displays the upgrade options according to the available software version.

5. When the installer prompts you to select an upgrade option, perform one of the following according to your current environment:

Note:

You can continue to upgrade to Avaya Diagnostic Server 2.5 even without the minimum hardware requirements. However, the host must meet the minimum disk space requirement. You cannot install a new component during such an upgrade. After the upgrade, you must use the backup and restore facility of Avaya Diagnostic Server to migrate to another server that meets the minimum requirements completely. If you do not migrate, you might not be able to use all features of Avaya Diagnostic Server.

- If you are upgrading from SAL Gateway 2.x, type one of the following options:
  - `1`: To upgrade to Avaya Diagnostic Server 2.5 with only the SAL Gateway component.
  - `2`: To upgrade to Avaya Diagnostic Server 2.5 with SAL Gateway and to install the SLA Mon component.
- If Avaya Diagnostic Server 1.0 or later is available with the SAL Gateway component, type one of the following options:
  - `1`: To upgrade to Avaya Diagnostic Server 2.5 with only the SAL Gateway component.
  - `2`: To upgrade to Avaya Diagnostic Server 2.5 with SAL Gateway and to install the SLA Mon component.
- If Avaya Diagnostic Server 1.0 or later is available with the SLA Mon component, type one of the following options:
  - `1`: To upgrade to Avaya Diagnostic Server 2.5 with only the SLA Mon component.
  - `2`: To upgrade to Avaya Diagnostic Server 2.5 with SLA Mon and to install the SAL Gateway components.
- If Avaya Diagnostic Server 1.0 or later is available with both components, type `y` when the installer prompts you to upgrade to Avaya Diagnostic Server 2.5 with both components.
- If Avaya Diagnostic Server 2.5 is available with one component, and you want to install the second component, type `y` when the installer prompts you to install the second component.

According to the upgrade option you provide, the installer checks the host to verify whether the host meets the prerequisites for the upgrade. If the host meets the prerequisites, the installer continues with the upgrade process of the Avaya Diagnostic Server components.

Note:

The installer checks whether the recommended hardware requirements are met only if you are upgrading from a version earlier than Avaya Diagnostic Server 2.0. The installer prompts you to enter `y` to continue with the upgrade.

The upgrade option might cause both components to reside on the same server. In such cases, the installer displays a message about the security implication of having both components on the same server. To continue with the upgrade process, you must accept the security implication. Else, quit the upgrade process.

Next steps

Complete the SAL Gateway upgrade and then complete the SLA Mon server upgrade.

If you upgrade from a software version without the SAL Gateway or the SLA Mon component and choose to install the missing component, complete the installation of the missing component. See Chapter 4, Deploying Avaya Diagnostic Server.

Related links

Completing the SAL Gateway upgrade on page 106
Completing the SLA Mon server upgrade on page 107
Completing the SLA Mon server installation on page 58

Completing the SAL Gateway upgrade

About this task

After you select to upgrade the SAL Gateway component in the Avaya Diagnostic Server installation console, the installer starts the GUI-based wizard for SAL Gateway. Use this procedure to complete the SAL Gateway upgrade steps.

Note:

You can upgrade the redundant SAL Gateways one by one without affecting the redundancy configuration. After both SAL Gateways upgrade to the latest version, the redundancy feature works as expected.

During the time frame when you upgrade one SAL Gateway, the managed device synchronization between the two SAL Gateways might not happen. However, alarm transfer, remote access, and other functionalities remain available through the second SAL Gateway that participates in redundancy.

Procedure

1. On the Welcome panel, click **Next**.
2. On the Packs selection panel, select the component for installation, and click **Next**.

   If you are upgrading from Avaya Diagnostic Server 2.0, the system displays the Pack Installation Progress panel. Continue from Step 5.

   If you are upgrading from Avaya Diagnostic Server 1.0 or SAL Gateway 2.x, the system displays the Automatic Software Update Configuration panel. Continue from Step 3.
3. On the Automatic Software Update Configuration panel, select one of the following two options, and click **Next**:
   - ON: To enable the Automatic Software Update feature. If you do not install the downloaded software packages within the grace period set for the packages, the packages are installed automatically.
   - OFF: To disable the Automatic Software Update feature. You must install the downloaded software packages manually.

Note:

When you upgrade from Avaya Diagnostic Server 2.0 to 2.5, the system does not display the Automatic Software Update Configuration panel and the subsequent Mail Service Configuration panel.

The system displays the Mail Service Configuration panel. If the current SAL Gateway was configured to send email notifications to your system administrator, the panel populates the fields with the existing configuration details.

4. If the SMTP server details on the Mail Service Configuration panel are incomplete, complete the fields, and click **Next**.

   The installer takes a few minutes to complete the backup of the earlier version of the software and starts the upgrade. The installer copies all files on to the target path after the backup process.

   Note:

   If the upgrade process fails for some reason, the installer automatically rolls back to the state before the upgrade.

5. Click **Done**.

   The installer completes the upgrade process and returns you to the CLI-based wizard.

   According to the upgrade option you selected, the installer displays the message to upgrade or install the SLA Mon server component.

Next steps

Complete the SLA Mon upgrade or installation steps.

Completing the SLA Mon server upgrade

The SLA Mon server upgrade process follows the upgrade process of the SAL Gateway component of Avaya Diagnostic Server.

Procedure

When the CLI-based installation wizard displays the message to continue with the upgrade of the SLA Mon server, type `y`, and press **Enter**.

The system starts the SLA Mon upgrade. The installer takes a few minutes to process the files and complete the upgrade process.

When the upgrade operation completes successfully, the system displays a completion message. The installer starts the SAL Gateway and the SLA Mon services.

Next steps

Verify that the upgrade operation is successful.

Note:

Check the logs at `/opt/avaya/ads/logging/ads-install.log` for upgrade details.

Important:

The upgrade process retains the existing certificate that the earlier release of the SLA Mon server used for the server-agent communication. If the existing certificate is the Avaya demo certificate, Avaya recommends you to replace the demo certificate with a custom certificate as a security best practice. For more information, see Chapter 6, Managing certificates for the communication between the server and the agent certificates in *Administering Avaya Diagnostic Server SLA Mon*.

Related links

Verifying the upgrade operation on page 109

Upgrading Avaya Diagnostic Server in the unattended mode

About this task

You can upgrade Avaya Diagnostic Server in the unattended mode. If you do not have access to the console of the RHEL host through KVM or virtual console to run the installer in the GUI mode, you can run the installer in the unattended mode remotely through a SSH session.

Before you begin

Ensure that you have updated the response file, `ADS_Response.properties`, with the following information:

- For the `ADS_AGREELICENSE` property, replace the value `n` with `y`.
- According to the existing software version, set the appropriate property from the upgrade scenarios section in the file with the required value for the upgrade preference.
- To upgrade from SAL Gateway 2.x or from Avaya Diagnostic Server 1.0 with the SAL Gateway component to Avaya Diagnostic Server 2.5, make the following changes in the file:
  - Replace the value of `AUTOUPGRADE_CUST_SELECT` with `ON` or `OFF`.
  - In the SMTP configuration fields section, if required, update the SMTP server details with correct and complete values. You must provide values for the `SMTP_HOST`, `SMTP_PORT`, and `SMTP_ADMIN_EMAIL` properties.

  Note:

  To upgrade from Avaya Diagnostic Server 2.0 to 2.5, you need not change the properties related to automatic software upgrade and SMTP configuration in the file.

The response file is available in the location where you extracted the Avaya Diagnostic Server software package. The file path is `/<folder_path to the extracted package>/ADS-Installer-<version_no>-<build_no>/ADS_Response.properties`. For more information, see ADS_Response.properties file on page 61.

Procedure

1. Log on to the RHEL host as root.

   Note:

   Do *not* log in as saluser or use the **su** command to switch the user from saluser to root for an upgrade operation. Upgrade attempts through both login methods result in upgrade failure because the installer tries to kill any active processes owned by saluser.

2. Change to the directory where you downloaded and extracted the Avaya Diagnostic Server software package.
3. Run the following command to start the upgrade process in the unattended mode:

   ./install.sh –unattended

   The installer checks the host to verify whether the host meets the prerequisites. The installer also checks for the availability of any earlier version of SAL Gateway or Avaya Diagnostic Server. After the checks are complete, the installer starts processing the installation files and proceeds with the upgrade of Avaya Diagnostic Server according to the inputs you provided in the response file.

Result

When the upgrade completes successfully, the system displays a successful completion message. The installer starts the services for the components.

Related links

ADS_Response.properties file on page 61
Verifying the upgrade operation on page 109

Verifying the upgrade operation

Procedure

1. For the SAL Gateway component, ensure that the SAL Gateway services, including SAL Watchdog, alarm transfer, remote access, and SAL Gateway UI, are running correctly.

   For more information, see Chapter 6, Verifying the Avaya Diagnostic Server implementation.

2. For the SLA Mon component, ensure that the SLA Mon services, including slamonsrvr, slamonweb, and slamondb, are running correctly.

   For more information, see Chapter 6, Verifying the Avaya Diagnostic Server implementation.

3. Log on to the web interfaces of the components to check whether the configuration information persist after the upgrade.
4. If a test pattern was running on the SLA Mon server before the upgrade operation, stop and start the test pattern after the upgrade operation.

Note:

After upgrade, you might observe reduced number of network performance tests on the SLA Mon web interface. The reason might be that some agents did not respond to the SLA Mon server after the restart of the slamonsrvr service. For more information, see Reduced number of network performance tests after upgrade on page 138.

Chapter 8: Backing up and restoring Avaya Diagnostic Server

Backing up Avaya Diagnostic Server

About this task

Use this procedure to back up the configuration data of all installed components of Avaya Diagnostic Server.

From Avaya Diagnostic Server 2.5 onwards, you can also back up the network monitoring data as part of the SLA Mon server backup. You can back up the network test results on the server only if the server has sufficient disk space. Otherwise, you must mount a USB or a network drive to take the backup.

Important:

The backup process in Avaya Diagnostic Server does not save the WebLM server license or the password. You must reinstall the WebLM server license after a restore operation.

Procedure

1. Log on to the RHEL host of Avaya Diagnostic Server as root.
2. If the folder where you want to save the backup file does not exist, create the folder on the host server or the mounted USB or network drive.
3. Navigate to the `/opt/avaya/ads/backuprestore` directory:

   `cd` `/opt/avaya/ads/backuprestore`
4. Run the following command to start the backup process:

   `./backup_restore.sh` `backup /<backup_folder_path>`

   Where *<backup_folder_path>* is the absolute path to the backup folder that you created. The script does not support a relative path.

   The system takes a backup of the configuration data of all installed components of Avaya Diagnostic Server.

   If the SLA Mon server component is present, the utility checks whether the target location has sufficient free space to store the network monitoring data. If sufficient free space is available, you get the option to back up the network monitoring data. Otherwise, you get the option to back up only the configuration data. The system displays the available free space and the approximate space required for backing up the network monitoring data.

The system saves the backup archive file, `ADS_<version_no>_backup.tar`, at the specified location.

5. **(Optional)** If the system provides the option to back up the network monitoring data, do one of the following:
   - Press **y** to back up the network monitoring data.
   - Press **n** to back up only the configuration data of the SLA Mon server.

   Depending on the size of the data to be backed up, the process takes some time to complete. For example, backup of 100 GB of network monitoring data might take approximately 2 hours.

   Note:

   If you back up data on a mounted FAT file system drive, you might see the following error for a few files:

   ```
   failed to preserve ownership for "*****" : Operation not permitted
   ```

   The error does not affect the backup and restore functionalities. You can ignore such messages. During the restore process, the system restores the files with the right permissions.

Restoring Avaya Diagnostic Server

About this task

Use this procedure to restore the backed up data, including configuration and network monitoring, of Avaya Diagnostic Server. The restore process is independent of the deployment environment. You can restore data on the same Avaya Diagnostic Server or on another Avaya Diagnostic Server that is installed on a different server.

From Avaya Diagnostic Server 2.5 onwards, you can choose to back up and restore the network monitoring data of the SLA Monserver component. The restore process provides the option to restore the network monitoring data only if the target server has sufficient disk space. Otherwise, you get the option to restore only the configuration data.

Before you begin

Take the following points into account while you prepare the target server for restoring Avaya Diagnostic Server:

- The Avaya Diagnostic Server version on the source and the target server must be the same.
- The restore process overwrites the existing data, including the configuration and the network monitoring data, on the target system. To avoid data loss, Avaya recommends that you perform the restore operation on a clean system.
- To avoid changing the IP address configuration after a restore operation, install the target server with the existing IP address on a private network. After you complete the restore

operation and take the old server offline, you can make the new server available on the public network.

- The restore process is a service impacting process, and all services of the Avaya Diagnostic Server components remain unavailable during the restore process. The services become available after the restore process completes successfully. To minimize disruption of services, choose a time for the restore operation when the impact of a system downtime is the least.

Procedure

1. Log on as root to the RHEL host on which you want to restore Avaya Diagnostic Server.
2. If the backup file is not on the local host or any of the mounted drives, copy the file to a local folder on the host.

   Note:

   You can restore data directly from a mounted USB or network drive.
3. Change the working directory to `/opt/avaya/ads/backuprestore`:

   `cd` `/opt/avaya/ads/backuprestore`
4. Run the following command to start the restore process:

   `./backup_restore.sh` `restore /<backup_folder_path>`

   Where *<backup_folder_path>* is the absolute path of the folder where the `ADS_<version_no>_backup.tar` file is located. The script does not support relative path.

   The system checks for the installed components and the component data available in the backup archive. Accordingly, the system stops the services of the components that are installed, and restores the configuration data of the components from the `ADS_<version_no>_backup.tar` file. After the restore process is complete for a component, the script restarts the services.

   If the SLA Mon server is present on the target server and the network monitoring data is present in the backup archive, the script checks the available disk space on the server. If the target server has sufficient disk space, you get the option to restore the network monitoring data. Otherwise, you get the option to restore only the configuration data. The system displays the available free space and the approximate space required for restoring the backed up network monitoring data.
5. **(Optional)** If the system provides the option to restore the network monitoring data, do one of the following:

   - Press **y** to restore the network monitoring data.
   - Press **n** to restore only the configuration data of the SLA Mon server.

   Depending on the size of the data to be restored, the process takes some time to complete. For example, restore of 100 GB of network monitoring data might take approximately 4 hours.

Next steps

1. Reinstall the WebLM server license for the SLA Mon server because the backup process in Avaya Diagnostic Server does not save the WebLM server license or the password.

2. If you restored data on a different server and the MAC address has changed, get a new license, and install the license. The earlier license is no longer valid.
3. After installing the license, restart the slamonsrvr service and then the slamonweb service.
4. If you restored data on a different server and the server IP address is different from the existing server, perform the following:
   a. Change the SAL Gateway IP address configuration.
   b. After updating the SAL Gateway IP address, perform onboarding of the managed devices again.

      For more information about changing the SAL Gateway IP address configuration and onboarding devices, see *Administering Avaya Diagnostic Server SAL Gateway*.
   c. Rediscover SLA Mon agents.

Note:

To avoid changing the IP address configuration, install the target server with the existing IP address on a private network.

Related links

Installing the SLA Mon server license on WebLM on page 88

Migration of Avaya Diagnostic Server from one server to another server

Using the backup and restore facility of Avaya Diagnostic Server, you can migrate Avaya Diagnostic Server from one host server to another server. You might want to migrate Avaya Diagnostic Server from an existing server to another server in the following scenarios:

- You want to upgrade from an earlier version of SAL Gateway or Avaya Diagnostic Server to the latest Avaya Diagnostic Server release. But the current hardware specifications do not meet the minimum requirements.
- The current hardware specifications support the remote access and the alarm transfer features. But, to use the network monitoring feature of Avaya Diagnostic Server, you require a host with higher hardware specifications.

The full backup and restore facility of the configuration data is available from Avaya Diagnostic Server 2.0 onwards only. Also, Avaya Diagnostic Server 2.5 and later support backup and restore of network monitoring data from the SLA Mon server. Therefore, you must upgrade any earlier version of Avaya Diagnostic Server or SAL Gateway to Avaya Diagnostic Server 2.0 or later before you can migrate to another server.

Migration checklist

The following checklist provides the high-level steps to migrate Avaya Diagnostic Server from one server to another server:

No.	Task	Description	✔
1	Ensure that you have upgraded to Avaya Diagnostic Server 2.0 or later on the current host server.	The full backup and restore facility that you require to migrate from one server to another is available from Avaya Diagnostic Server 2.0 onwards only.	
2	Take the full backup of Avaya Diagnostic Server, and save the backup archive file to a remote location.	See Backing up Avaya Diagnostic Server on page 111.	
3	Perform a clean installation of Avaya Diagnostic Server on the new host server that is on a private network.	Install the same version of Avaya Diagnostic Server as the version installed on the source server. See Chapter 4, Deploying Avaya Diagnostic Server. **Important:** Maintain the new server on a private network until you complete the migration steps.	
4	Restore the configuration data of the backed up Avaya Diagnostic Server on the new host server.	See Restoring Avaya Diagnostic Server on page 112. **Important:** Do not make the new server available on the public network yet.	
5	Validate that the restoration of data is successful on the new server.		
6	Take the old server offline, or at least stop all services related to Avaya Diagnostic Server on the server.		
7	Bring the new server online. That is, make the server available on the public network.	**Important:** Do not keep both servers functional simultaneously as that results in running two SAL Gateways with the same SEID or UUID. Running two SAL Gateways simultaneously with the same UUID leads to erroneous alarm transfer and remote access handling.	

Chapter 9: Uninstalling Avaya Diagnostic Server

Avaya Diagnostic Server uninstallation overview

This chapter describes the procedures to uninstall Avaya Diagnostic Server, and the components. You can choose to uninstall only one component, SAL Gateway or the SLA Mon server, or remove Avaya Diagnostic Server completely from the server.

During the installation of Avaya Diagnostic Server, the installer creates an **uninstall.sh** script inside the installation directory, `/opt/avaya/ads/uninstaller/`. You can run the script in one of the following two modes to uninstall Avaya Diagnostic Server.

- Unattended: You can run this mode through an SSH session to the RHEL host.
- Attended: You must log on to the RHEL server through KVM or virtual console to run the uninstaller in this mode.

Uninstalling Avaya Diagnostic Server in the attended mode

About this task

Use the following interactive procedure to uninstall Avaya Diagnostic Server from the RHEL server through KVM or virtual console.

Procedure

1. Log on to the system on which Avaya Diagnostic Server is installed.
2. From the GUI, use root permissions and open a new shell prompt on the GUI.
3. Change the directory to `/opt/avaya/ads/uninstaller`, and run the following command:

   ./uninstall.sh `-attended`

   The system displays a message to back up Avaya Diagnostic Server.
4. Perform one of the following:
   - To take a backup, type `y` and press **Enter**.

- To continue without taking a backup, press **Enter**.

If you choose to back up Avaya Diagnostic Server, the system prompts you to enter the path where you want to save the backup archive. Else, the system prompts you to select the components you want to uninstall.

5. **(Optional)** When the system prompts, type the path where you want to save the backup archive.
6. If Avaya Diagnostic Server is installed with both components, type one of the following options to specify what you want to uninstall:
   - `1`: To uninstall only SAL Gateway.
   - `2`: To uninstall only SLA Mon.
   - `3`: To uninstall Avaya Diagnostic Server with both components.
7. If Avaya Diagnostic Server has only one component, when the system displays a message to uninstall the component, type `y` to uninstall that component.

Next steps

Complete the steps to uninstall SAL Gateway.

Complete the steps to uninstall the SLA Mon server.

Related links

Completing the SAL Gateway uninstallation on page 117
Completing the SLA Mon server uninstallation on page 118

Completing the SAL Gateway uninstallation

About this task

Complete the steps in this procedure to uninstall the SAL Gateway component of Avaya Diagnostic Server.

Procedure

1. On the Uninstaller wizard panel, click **Next** to continue with the SAL Gateway uninstallation.

   The system displays the Uninstall options panel.

2. Click **Next**.

   The system displays the Select Installed Packs panel.

3. Select the pack or packs for uninstallation, and click **Next**.

   The system displays the Uninstallation progress panel with bars that indicate the progress of the uninstall process.

Caution:

Do not use the **Quit** option when the uninstall process is in progress. This action might corrupt some files and make your system unstable. If you accidentally click **Quit**, the system displays a dialog box to confirm the action. If you click **Yes**, the uninstallation process is stopped and the file system might get corrupted. You might then have to manually clean up the disk and stop the services.

4. After the uninstaller completes executing the files, click **Next**.

   The system displays the Uninstallation summary panel. This panel displays the pack, SAL Gateway, which has been uninstalled successfully.

5. Click **Done**.

   The system completes the SAL Gateway uninstallation process and returns you to the CLI-based wizard.

   If you selected to uninstall the SLA Mon server component, the system starts the SLA Mon server uninstallation process.

Next steps

Complete the steps to uninstall the SLA Mon server.

Related links

Uninstalling Avaya Diagnostic Server in the attended mode on page 116

Completing the SLA Mon server uninstallation

The SLA Mon uninstallation process starts after the SAL Gateway uninstallation process is complete.

About this task

Complete the steps in this procedure to uninstall the SLA Mon server.

Procedure

1. When the system displays the message to continue with the uninstallation of the SLA Mon server, type `y`.

   The system starts the uninstallation process.

   The system displays a message for removing PostgreSQL server.

   PostgreSQL is the database and supported libraries. You choose to either remove or retain PostgreSQL.

2. When the system prompts you to uninstall the PostgreSQL database and libraries, type `y` or `n` as appropriate, and press **Enter**.

Important:

Before you choose to remove PostgreSQL, ensure that no other applications are using the PostgreSQL database or libraries.

The system starts uninstalling the SLA Mon server.

After the uninstallation process is complete, the system displays an `Uninstall Complete` message and returns you to the command line.

Related links

Uninstalling Avaya Diagnostic Server in the attended mode on page 116

Uninstalling Avaya Diagnostic Server in the unattended mode

Before you begin

Ensure that you have updated the uninstaller response file, `/opt/avaya/ads/uninstaller/ADS_Uninstall_Response.properties`, with the required input responses for the uninstallation preferences. Read the instructions in the file carefully while providing the inputs. The uninstaller script uses the information you provide in the response file to run the uninstallation process.

About this task

If you do not have access to the console of the RHEL host through KVM or virtual console to run the Avaya Diagnostic Server uninstaller in the GUI mode, use this procedure to run the uninstaller in the unattended mode remotely through a SSH session.

Procedure

1. Log on to the RHEL host on which you installed Avaya Diagnostic Server as root.
2. Change to the `/opt/avaya/ads/uninstaller` directory.
3. Run the following command:

   `./uninstall.sh` `-unattended`

   The uninstaller checks the response file and proceeds with the uninstallation process of Avaya Diagnostic Server according to the inputs you provided in the response file.

   After the uninstallation process is complete, the system displays an `Uninstall Complete` message and returns you to the command line.

Chapter 10: Installing and configuring Net-SNMP on RHEL 5.x and 6.x

SNMP capability in SAL Gateway

SAL Gateway uses the SNMP capability to communicate information to network management applications such as NetView Management Console (NMC) or Network Management System (NMS). SAL Gateway can use SNMP traps to communicate product status, performance metrics, alarm states, and inventory information to the network management applications.

SNMP, a network management protocol in the TCP/IP protocol suite, uses a simple request and response protocol to communicate management information. A set of managed objects called SNMP Management Information Bases (MIB) defines this information. SNMP can alternatively generate traps that asynchronously report significant events to clients.

SAL Gateway defines its own application-specific MIB that contains the definition of managed objects that SAL Gateway wants to be exposed to a network management tool, such as NMS or NMC. The MIB also defines the traps SAL Gateway sends.

Implementing the SNMP capability for SAL Gateway requires implementing an SNMP master agent on SAL Gateway. The master agent, a prerequisite for the SAL Gateway installation, can be any standard SNMP agent that supports the following:

- All MIB modules that the SNMP standards require
- The AgentX protocol

The SAL Gateway administrator configures the SNMP master agent. The procedures described in this chapter pertain to the implementation of Net-SNMP as the master agent on RHEL 5.x and 6.x.

Net-SNMP

Net-SNMP is the preferred implementation for an SNMP master agent, because Net-SNMP is:

- A standard, widely accepted SNMP agent.
- Supported on most of the Operating System (OS) platforms.
- An SNMP agent that supports:
  - Most of the MIB modules that ECG Internal Standards mandate.

- The AgentX protocol and SNMP v3.

- The default SNMP agent in many operating systems, including Red Hat Enterprise Linux (RHEL).
- Easy to install and configure.

Installing Net-SNMP

Use this procedure to install and configure the Net-SNMP master agent on RHEL 5.x or 6.x.

Before you begin

Before installing Net-SNMP, ensure that you have the following:

- A Linux system to install Net-SNMP.
- Net-SNMP RPMs for the installed Linux flavor.
- Sufficient knowledge of RPM installation.
- Valid IPv6 configuration on the target machine to run the SNMP master agent in the IPv6 environment.

Procedure

1. Log on to the Linux machine using an SSH client.
2. Open a terminal on the Linux machine.
3. If you logged in as a non-root user, run the **sudo su –** command to change your login to root.
4. Install the following Net-SNMP RPMs:
   - net-snmp
   - net-snmp-utils

   Note:

   Use the RPMs provided on the RHEL installation CD or DVD. You might also need to install additional RPMs to satisfy OS dependencies.
5. Run the **rpm** command and specify the path of the Net-SNMP RPMs as the following:

   ```
   rpm -iv net-snmp-5.3.2.2-5.el5.i386.rpm net-snmp-utils-*.rpm
   ```

   System output :

   ```
   warning: net-snmp-5.3.2.2-5.el5.i386.rpm: Header V3 DSA signature:
   NOKEY, key ID 37017186
   Preparing packages for installation...
   net-snmp-5.3.2.2-5.el5
   net-snmp-utils-5.3.2.2-5
   ```
6. Set the PATH environment variable, and if `/usr/bin` is missing, run the following command to add this path to the PATH environment variable:

```
export PATH=$PATH:/usr/bin
```

SNMP master agent configuration

The correct configuration of the SNMP master agent in `snmpd.conf`, the SNMP agent configuration file, is critical for two reasons:

- The master agent registers the SAL SNMP subagent.
- The customer NMSs query the master agent for managed objects.

The configuration of the SNMP master agent involves two tasks:

- Configuring the master agent for the AgentX communication with the subagent over TCP on port 705.
- Configuring the master agent for the SNMP v2c or v3 protocol.

  If you configure the master agent for SNMP v3, you must define an SNMP v3 user.

Note:

After you complete the master agent configuration, you must restart the SNMP master agent and SAL SNMP subagent services.

Related links

Configuring the master agent to communicate with the subagent on page 122
Configuring the master agent for SNMP v2c on page 124
Configuring the master agent for SNMP v3 on page 124
Defining an SNMP v3 user on page 125

Configuring the master agent to communicate with the subagent

About this task

After you install the SNMP master agent, you must configure the master agent to enable AgentX communication with the SAL SNMP subagent. Use this procedure to configure the master agent to communicate with the subagent over TCP on port 705.

Note:

SAL Gateway does not mandate the use of the standard port 705 for subagent and master agent communication. You can configure a port other than 705 in SAL Gateway for the SNMP subagent and configure that port in the master agent instead of port 705. However, port 705 is the standard port for the master agent and subagent communication (AgentX).

Procedure

1. If Net-SNMP is already installed and running, run the following command to stop the snmpd service:

service snmpd stop

If the snmpd service was running, the system displays the following output:

```
Stopping snmpd: [OK]
```

If the service was not running, the system displays the `Failed` status. Ignore this status and proceed to the next step.

2. Check whether port 705 is in use by running the following command:

   netstat -na --proto=inet,inet6 | grep 705

   If the port is in use, the system displays the following output:

   ```
   tcp 0 0 127.0.0.1:705 0.0.0.0:* LISTEN
   ```

3. If port 705 is in use, do one of the following to free the port:
   - Assign a different free port to the process that is using port 705.
   - Stop the process that is using port 705.
4. Rename the `/etc/snmp/snmpd.conf` file, if exists, to `/etc/snmp/snmpd.conf.bak`.
5. Create a new and empty `/etc/snmp/snmpd.conf` file.

   You can use the following command to create the file:

   touch `/etc/snmp/snmpd.conf`
6. Open the newly created file using the vi text editor.
7. Do one of the following:
   - For IPv4, enter the following lines at the top of the file:

     ```
     master agentx
     agentXSocket tcp:localhost:705
     ```

   - For IPv6, enter the following lines at the top of the file:

     ```
     master agentx
     agentXSocket tcp6:[<IPv6 address>]:705
     ```

8. (For IPv6 only) Add the following line at the top of the file:

   ```
   agentaddress udp:161,tcp:161,udp6:161,tcp6:161
   ```

   This addition configures the master agent to accept both UDP and TCP requests over IPv4 and IPv6.
9. Save the `/etc/snmp/snmpd.conf` file and exit the editor.

Next steps

After you configure the SNMP master agent to communicate with the subagent, configure the master agent for SNMP v2c or v3.

Related links

SNMP master agent configuration on page 122
Configuring the master agent for SNMP v2c on page 124

Configuring the master agent for SNMP v3 on page 124

Configuring the master agent for SNMP v2c

About this task

Use this procedure to configure the SNMP master agent for SNMP v2c.

Procedure

1. Open the `/etc/snmp/snmpd.conf` file in a text editor.
2. Add the following line to the file:

```
rocommunity <community-string> default .1.3.6.1.4.1.6889.2.41.1.1
```

Note:

Do not use common or decipherable values, such as `public`, as a community string. With `default`, you enable all the IP addresses to query the master agent.

3. Save the `/etc/snmp/snmpd.conf` file and exit the editor.

Next steps

You might need to configure iptables on the Linux host to open the required SNMP ports.

After you complete the master agent configuration, restart the SNMP master agent and SAL SNMP subagent services.

Related links

SNMP master agent configuration on page 122

Configuring the master agent for SNMP v3

About this task

Use this procedure to configure the SNMP master agent for SNMP v3.

Procedure

1. Open the `/etc/snmp/snmpd.conf` file in a text editor.
2. Add the following line to the file:

```
rwuser <v3-user> <securityLevel> .1.3.6.1.4.1.6889.2.41.1.1
```

In the line, replace *<securityLevel>* with the appropriate security level for SNMP v3. The NMS administrator decides the security level. The following table contains the security levels available for SNMP v3:

Security level	Description
noAuthNoPriv	No authorization and no encryption (Privacy)
authNoPriv	Authorization but no encryption (Privacy)
authPriv	Authorization and encryption (Privacy)

Note:

If the value for `<securityLevel>` is unknown, set the value as `authPriv`.

3. Save the `/etc/snmp/snmpd.conf` file and exit the editor.

Next steps

After you configure the SNMP master agent for SNMP v3, create an SNMP v3 user.

You might need to configure iptables on the Linux host to open the required SNMP ports.

After you complete the master agent configuration, restart the SNMP master agent and SAL SNMP subagent services.

Related links

SNMP master agent configuration on page 122
Defining an SNMP v3 user on page 125

Defining an SNMP v3 user

About this task

If you configured the SNMP master agent for SNMP v3, use this procedure to define an SNMP v3 user.

Procedure

1. Depending on the version of the operating system on the host computer, locate and open one of the following files in a text editor:
   - For RHEL 5.x: `/var/net-snmp/snmpd.conf`
   - For RHEL 6.x: `/var/lib/net-snmp/snmpd.conf`

   If no such file already exists, create the file.
2. Add the following line at the end of the file:

```
createUser <v3-user> MD5 <auth-pass> AES <priv-pass>
```

   Where, replace the following variables with the actual values for the protocols. Choose the values after a consultation with your network administrator.

   <v3–user> The v3 user name. The user name must be identical with the user name that you specified in the access control directive, `rwuser`, in the `/etc/`

`snmp/snmpd.conf` file during the master agent configuration for SNMP v3.

<auth-pass>	Password to be used with the MD5 authentication protocol.
<priv-pass>	Password to be used with the Advanced Encryption Standard (AES) privacy protocol.

Note:

The `createUser` directive creates an SNMP v3 user `<v3-user>`. This user uses MD5 and the password `<auth-pass>` for authentication, and AES and password `<priv-pass>` for encryption or privacy.

3. Save the file and exit the text editor.

Related links

SNMP master agent configuration on page 122

Firewall (iptables) configuration

You must ensure that the firewall rules on the Linux system, on which you installed the SNMP master agent, do not block the standard SNMP port and the AgentX port. You might need to configure iptables on the Linux host to open the required ports.

The following procedures describe the steps to configure iptables on an RHEL 5.x or 6.x system. There might be variations in configuring iptables on other Linux flavors. Consult the firewall user guide for your OS if the configuration is different for other firewall applications. Even on an RHEL system, the steps described in the following procedures might not be the only way to configure iptables to open ports.

Related links

Configuring the firewall for IPv4 on page 126
Configuring the firewall for IPv6 on page 127

Configuring the firewall for IPv4

About this task

You can use this procedure to configure the firewall or iptables on an RHEL 5.x or 6.x system with IPv4 settings to open ports that are required for SNMP communication.

Procedure

1. Log on to the system as root.

2. Run the following command to check if the firewall is enabled and running:

   ```
   service iptables status
   ```

   If the firewall is stopped or disabled, the system displays one of the following outputs:

   - `Firewall is stopped`
   - `Table: filterChain INPUT (policy ACCEPT) num target prot opt source destination Chain FORWARD (policy ACCEPT) num target prot opt source destination Chain OUTPUT (policy ACCEPT) num target prot opt source destination`

   If the firewall is disabled, skip the rest of the steps, and carry out the procedure to disable SELinux. Otherwise, continue to the next step.

3. From the output generated in step 2, validate if the SNMP standard port 161 is open. Check if the output resembles the following example:

   ```
   ...
   ACCEPT udp -- 0.0.0.0/0 0.0.0.0/0 udp dpt:161
   ...
   ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:161
   ...
   ```

   If the output matches the sample, the ports are already open. Carry out the procedure to disable SELinux. Otherwise, continue to the next step.

4. If port 161 is closed, run the following commands to open port 161:

   ```
   iptables -I INPUT 1 -p udp -m udp --dport 161 -j ACCEPT
   ```

   ```
   iptables -I INPUT 1 -p tcp -m tcp --dport 161 -j ACCEPT
   ```

5. **(Optional)** Depending on the network setup of the customer, you might require to open the AgentX port on the system. Open the port by running the following command:

   ```
   iptables -I INPUT 2 -p tcp -m tcp --dport <agentX_port> -j ACCEPT
   ```

6. Run the following command to save the iptables configuration:

   ```
   service iptables save
   ```

7. Run the following command to restart the iptables:

   ```
   service iptables restart
   ```

Related links

Firewall (iptables) configuration on page 126
Disabling SELinux for the master agent on page 129

Configuring the firewall for IPv6

About this task

You can use this procedure to configure the firewall or iptables on an RHEL 5.x or 6.x system with IPv6 settings to open ports that are required for SNMP communication.

Procedure

1. Log on to the system as root.
2. Run the following command to check if the firewall is enabled and running:

   ```
   service ip6tables status
   ```

   If the firewall is stopped or disabled, the system displays one of the following outputs:

   - `Firewall is stopped`
   - `Table: filterChain INPUT (policy ACCEPT) num target prot opt source destination Chain FORWARD (policy ACCEPT) num target prot opt source destination Chain OUTPUT (policy ACCEPT) num target prot opt source destination`

   If the firewall is disabled, skip the rest of the steps, and carry out the procedure to disable SELinux. Otherwise, continue to the next step.
3. From the output generated in step 2, validate if the SNMP standard port 161 is open. Check if the output resembles the following example:

   ```
   ...
   ACCEPT    udp  --  ::/0       ::/0         udp dpt:161
   ...
   ACCEPT    tcp  --  ::/0       ::/0         tcp dpt:161
   ...
   ```

   If the output matches the sample, the ports are already open. Carry out the procedure to disable SELinux. Otherwise, continue to the next step.
4. If port 161 is closed, run the following commands to open port 161:

   ```
   ip6tables -I INPUT 1 -p udp -m udp --dport 161 -j ACCEPT
   ```

   ```
   ip6tables -I INPUT 1 -p tcp -m tcp --dport 161 -j ACCEPT
   ```
5. **(Optional)** Depending on the network setup of the customer, you might require to open the AgentX port on the system. Open the port by running the following command:

   ```
   ip6tables -I INPUT 2 -p tcp -m tcp --dport <agentX_port> -j ACCEPT
   ```
6. Run the following command to save the iptables configuration:

   ```
   service ip6tables save
   ```
7. Run the following command to restart the iptables:

   ```
   service ip6tables restart
   ```

Related links

Firewall (iptables) configuration on page 126
Disabling SELinux for the master agent on page 129

Disabling SELinux for the master agent

About this task

If SELinux is enabled and in the enforcing mode, you must configure SELinux to disable the SELinux protection for the SNMP master agent.

Procedure

On the Linux system where you installed the SNMP master agent, ensure that SELinux is disabled. If SELinux is enabled and in the *Enforcing* mode, disable SELinux.

For more information, see Disabling SELinux protection on page 149. For other techniques to configure and disable SELinux, see the SELinux documentation for your operating system.

Starting the SNMP master agent service

About this task

Use this procedure to start the SNMP master agent service after you complete the master agent configuration.

Procedure

1. Log in as root to the system where you installed the SNMP master agent.
2. Run the following command to start the snmpd service:

   `service snmpd start`

   You must get the following output:

   ```
   Starting snmpd: [OK]
   ```

   Note:

   The snmpd service must start with an `OK` message.
3. Run the following command to ensure that the master agent service snmpd starts when the system boots:

   `chkconfig snmpd on`
4. Run the following command to verify that the **`chkconfig`** command was successful:

   `chkconfig snmpd --list`

   You must get the following output:

   ```
   snmpd 0:off 1:off 2:on 3:on 4:on 5:on 6:off
   ```

   Note:

   The last line in the output indicates *on* for 2, 3, 4, and 5.

Next steps

Restart the SAL SNMP subagent service.

Starting the SNMP subagent service

About this task

Use this procedure to restart the SAL SNMP subagent service after you complete the SNMP master agent configuration. On the SAL Gateway host, run the following command to restart the subagent service:

```
service snmpAgent start
```

Procedure

1. Log in as root to the SAL Gateway host.
2. Run the following command to restart the subagent service:

   `service snmpAgent start`

Verifying the SNMP master agent setup

Before you begin

Install an MIB browser of your choice on a system on the network other than the one on which the SNMP master agent is running.

About this task

You can use an MIB browser of your choice to verify whether the SNMP master agent is set up correctly.

Procedure

1. On the remote system, start the MIB browser and provide the following values to the parameters to set the SNMP target entity for SNMP v3:

Parameter	Value
Security Name	The user name, *<v3-user>*, defined for SNMP v3.
Security Level	The security level specified while configuring the master agent for SNMP v3. See Configuring the master agent for SNMP v3 on page 124.
Authorization Protocol	MD5

Table continues…

Parameter	Value
Authorization Password	The authorization password, *<auth-pass>*, set while defining the SNMP v3 user.
Privacy Protocol	AES
Privacy Password	The privacy password, *<priv-pass>*, set while defining the SNMP v3 user.

2. Load MIB-II, RFC 1213 - http://tools.ietf.org/html/rfc1213.
3. Run a GET query for the following standard SNMP Object IDs (OIDs) and verify whether you get the expected output:

OID	Attribute	Expected outcome
.1.3.6.1.2.1.1.1	sysDescr	System description
.1.3.6.1.2.1.1.3	sysUpTime	System up time
.1.3.6.1.2.1.1.5	sysName	System (machine) name

If you get the expected output for the GET queries, you have set up the SNMP master agent successfully.

Chapter 11: Troubleshooting

Avaya Diagnostic Server installation fails due to missing dependent RPMs

Problem

When installing Avaya Diagnostic Server, you might get an error if the dependent RPMs are not installed on the server. If you do not install the required RPMs on the RHEL server before running the installer, the Avaya Diagnostic Server installation fails.

Resolution

You can either search the Web and download the missing RPMs or install the missing RPMs using the Yum installer.

Use the following procedure to install the missing RPMs using the Yum installer.

Note:

- Yum is a command line tool that uses an Internet connection to install and manage RPMs. Ensure that you have access to the Internet from your server for completing this task.
- If your server does not have access to the Internet, you can point to a local repository file under `/etc/yum.repos.d/` folder.

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

   `cat /etc/redhat-release`

   The system displays the RHEL version details on the server.
3. Create the local repository file `/etc/yum.repos.d/file.repo`, and add following lines:

   ```
   [RH-Server-Local]
   name= RHEL Server Local Repository
   baseurl=<baseurl>
   gpgkey=<gpgkey>
   enabled=1
   ```

   Where, depending on your RHEL version:

   - Replace the `<baseurl>` with the file path to the Yum repository. If you are using the local repository on the server, provide the file path of the repository. If you want to install the RPMs online and have a RHEL subscription, provide the respective URL.
   - Replace the <gpgkey> with a local or Web URL accordingly.

4. Run the following command to find the packages that are installed or available for installation:

   yum list

5. Run the following Yum command to install a package or RPMs:

   yum install *<package name>*

   Make sure that *<package name>* is correct and valid.

“Unsupported Operating System, List of supported Operating System RHEL 5.X (32 & 64 bit)” message while installing SAL

Problem

During the installation of SAL Gateway, you get the error messages such as “Unsupported Operating System, List of supported Operating System RHEL 5.X (32 & 64 bit)”.

Resolution

If you are running the Avaya Diagnostic Server installer on RHEL 6.4, ensure that the following preinstallation steps are performed:

Preinstallation steps

- Run the `ls -l /etc/*-release` command. If the output indicates other files apart from `redhat-release` and `system-release`, move the other files to a temporary folder.

  For example:

  The `ls -l /etc/*-release` command generates the following output:

```
[root@linpubc056 ~]# ls -l  /etc/*-release
-rw-r--r--. 1 root root 148 Jul 17 20:19 /etc/lsb-release
-rw-r--r--. 1 root root  55 Jan 29 21:18 /etc/redhat-release
lrwxrwxrwx. 1 root root  14 Jul 17 20:16 /etc/system-release -> redhat-release
[root@linpubc056 ~]#
```

- Move `/etc/lsb-release` to a temporary location using the following command:

  `mv /etc/lsb-release /tmp/`

Postinstallation steps

Note:

Carry out the postinstallation steps only if the preinstallation steps detected additional files.

- Move back the files from the temporary location, `/tmp`, to the original folder, `/etc/`.

  Based on the earlier example, the commands include the following:

  - Run the `mv /tmp/lsb-release /etc/` command to move the file back to the original folder.

- Run the `chmod 644 /etc/lsb-release` command to make sure the same permissions exist after moving the file to the original folder.

System mitigation after an unsuccessful installation or upgrade of Avaya Diagnostic Server

When an installation or an upgrade operation of Avaya Diagnostic Server ends abruptly, you might have to perform some mitigation steps to recover the state before the operation. This section covers the cleanup and restoration procedures for each Avaya Diagnostic Server component if an installation or upgrade operation ends abruptly.

Note:

When the Avaya Diagnostic Server installer performs an installation or an upgrade operation on all components, the first component to get installed or upgraded is SAL Gateway. Therefore, if the operation on SAL Gateway ends abruptly, the installer does not perform any operation on the SLA Mon server. In such cases, perform the restore steps for only SAL Gateway.

System cleanup required as the installation of Avaya Diagnostic Server ends abruptly

When an installation of Avaya Diagnostic Server ends abruptly, you must perform some cleanup operations to ensure that no residual files from the attempt remain on the system. By cleaning up the system, you can ensure that any future installation does not fail because of residual or corrupted files of an earlier installation attempt.

Cleaning up SAL Gateway files

About this task

If an installation of the SAL Gateway component fails, use this procedure to clean up the system before you try to install the component again.

Procedure

1. **(Optional)** If the SLA Mon server is installed on the host server, uninstall the SLA Mon server.
2. On the host server, stop all SAL Gateway services that are in the running state.

   For example, run the following commands to stop the services:

   ```
   service salWatchdog stop
   service spiritAgent stop
   service gatewayUI stop
   ```

service axedaAgent stop

3. Open a new Linux shell on the host server, and navigate to the `/opt/avaya/` directory.
4. Run the following command to clean up the files in the folder:

   rm `-fr SAL`

   Caution:

   Do not run this command for a failed upgrade. Use this command for a failed installation only. For information on system restoration in case of a failed upgrade, see the troubleshooting section, System restoration required as Avaya Diagnostic Server upgrade ends abruptly.

5. Run the following command to remove the `/etc/avaya-base.loc` file, if present:

   rm `-fr /etc/avaya-base.loc`

   Caution:

   Do not run this command for a failed upgrade. Use this command for a failed installation only. For information on system restoration in case of a failed upgrade, see the troubleshooting section, System restoration required as Avaya Diagnostic Server upgrade ends abruptly.

6. In the `/etc/init.d` folder, remove the shortcuts, spiritAgent, snmpAgent, salWatchdog, gatewayUI, and axedaAgent, if present.
7. Reinstall the SAL Gateway and the SLA Mon server components using the Avaya Diagnostic Server installer.

Cleaning up SLA Mon files

About this task

If an installation of the SLA Mon server component fails, use this procedure to clean up the system before you try to install the component again.

The Avaya Diagnostic Server installer performs the SLA Mon installation using Red Hat Package Manager (RPM). Therefore, you must clean up the SLA Mon packages from the RPM repository on the host if an installation fails.

Procedure

1. On the host server, stop any SLA Mon services that are running.

   For example, run the following commands to stop the services:

   service slamonweb stop

   service slamonsrvr stop

   service slamondb stop

2. From the command line on the host server, run the following command:

   rpm `-qa '*salmon*'`

If any SLA Mon packages are installed on the host, the command output displays the packages. Note the package names to remove the packages from the system.

3. Use the following command to remove the SLA Mon packages:

   yum erase *<package name>*

   If any error occurs while running this command, use the `–skip-broken` flag with the command.

4. Navigate to the `/opt/avaya/` directory, and delete the `slamon` folder, if the folder exists.
5. Run the following commands to delete any remaining services from the installation attempt:

   /sbin/chkconfig `--del slamonsrvr`

   /sbin/chkconfig `--del slamonweb`

   /sbin/chkconfig `--del slamondb`

   Ignore any errors that you might see when you try to delete the services. The errors might occur because the services were not copied during the installation.

6. Run the following command to delete any remaining log files from the installation attempt:

   rm `–fr /var/log/slamon*`

System restoration required as Avaya Diagnostic Server upgrade ends abruptly

When an upgrade operation of an Avaya Diagnostic Server component ends abruptly, you might have to perform some operations to restore the system to the state before the upgrade. You must perform the restore operation for each component of Avaya Diagnostic Server, SAL Gateway or the SLA Mon server for which the upgrade operation fails.

Restoring SAL Gateway if the upgrade operation fails

About this task

If an upgrade operation of SAL Gateway fails due to some reason, the Avaya Diagnostic Server installer quits the process and rolls back to the state before the upgrade. If the installer does not automatically roll back to the earlier version of SAL Gateway, use this procedure to restore the earlier state.

Procedure

1. On the host server, open a Linux shell, and navigate to the `/<SAL install path>/upgradeScripts/` directory.
2. Copy the `gw-restoreScript.sh` script from the directory to a temporary directory outside the `/<SAL install path>` directory.
3. Navigate to the temporary directory where you copied the script.
4. Run the following command to assign executable permissions to the file:

```
/bin/chmod 700 gw-restoreScript.sh
```

5. Run the following command:

   ```
   /bin/sh gw-restoreScript.sh
   ```

   The script restores the earlier version of SAL Gateway.

Next steps

Verify the status of all SAL Gateway services. Open the SAL Gateway UI on a web browser to verify whether the UI is functioning correctly.

Note:

If the `/<install path>/upgradeScripts/gwrestoreScript.sh` script is not available on the host server, you cannot restore to the earlier version of SAL Gateway. You must clean up the host and reinstall SAL Gateway using the Avaya Diagnostic Server installer.

Related links

Cleaning up SAL Gateway files on page 134

Restoring SLA Mon if the upgrade operation fails

About this task

If the upgrade operation of the SLA Mon server ends abruptly, use this procedure to restore to the state before the upgrade.

Before performing the upgrade operation on the component, the Avaya Diagnostic Server installer takes a backup of the existing version of the components. This procedure provides the steps to restore the SLA Mon server from the backup, which the installer saves in the `/tmp/backup/slamon` folder.

If the backup folder, `/tmp/backup/slamon`, is not present on the host server, the following are the two possible scenarios:

- The abrupt termination of the upgrade operation did not affect the system. Restart the SLA Mon services to restore the earlier state of the SLA Mon server.
- The abrupt termination of the upgrade operation occurred during the RPM package upgrade and the RPM repository is corrupted. You cannot recover the earlier state. You must perform a complete clean up of the SLA Mon files and reinstall the SLA Mon server component. For more information, see the procedure about cleaning up the SLA Mon files.

Procedure

1. Open a Linux shell on the host server, and check whether the `/tmp/backup/slamon` folder is present on the server.

   If the folder is present, continue with the following steps.

2. Check if any SLA Mon services are running, and stop those services.

   For example, run the following commands to stop the services:

   ```
   service slamonweb stop
   ```

   ```
   service slamonsrvr stop
   ```

```
service slamondb stop
```

3. Perform the following to delete any remaining SLA Mon files or folders from the upgrade attempt:
   a. Navigate to the `/opt/avaya/` folder.
   b. Run the following command:

      ```
      rm -fr slamon
      ```

4. Run the following command to copy the content of the backup folder to the `/opt/avaya/` folder and to maintain the permissions:

   ```
   cp -rp /tmp/backup/slamon/** /opt/avaya/
   ```

   This command restores the earlier version of the SLA Mon server on the host.

5. Run the following commands to start the SLA Mon services.

   Keep a gap of at least 10 seconds between the execution of each command.

   ```
   service slamondb start
   service slamonsrvr start
   service slamonweb start
   ```

Reduced number of network performance tests after upgrade

Condition

After an Avaya Diagnostic Server upgrade, you might observe reduced number of network performance tests on the SLA Mon web interface.

Cause

Some agents do not respond to the SLA Mon server at the restart of the slamonsrvr service after the upgrade operation.

Solution

1. If a default test pattern is in use on the SLA Mon server, perform the following:
   a. On the SLA Mon web interface, navigate to the **TEST ADMINISTRATION** > **TEST EXECUTION** page, and stop and restart the default test pattern.
   b. Through the server CLI, restart the slamonsrvr service followed by the slamonweb service.

      ```
      service slamonsrvr restart
      ```

Note:

After you start the slamonsrvr service, wait for maximum 3 minutes to start the slamonweb service. The waiting time can be less depending on the number of agents that the server discovers.

```
service slamonweb restart
```

2. If a custom test pattern is in use, the test pattern automatically recovers from this situation if the agents are active.

SLA Mon and WebLM models are not present when adding as managed elements to SAL Gateway

Problem

The SLA Mon and WebLM models are not present in the **Model** drop-down list when adding SLA Mon and WebLM servers as managed elements to SAL Gateway. The issue indicates that SAL Gateway is not updated with the latest models published by Avaya.

Resolution

The Model Distribution feature of SAL Gateway ensures that SAL managed devices are associated with the latest model definitions. To apply the latest SLA Mon and WebLM models, make sure that the **Attempt to apply latest model immediately** check box under **Model Distribution Preferences** is always selected.

License installation failure on the WebLM server

Avaya Diagnostic Server comes with a WebLM server, which you can choose to install and use for Avaya Diagnostic Server licensing. License installation attempt on this local WebLM server might sometime throw an error message similar to the following:

```
An error occurred while performing license installation checks. Please ensure that the following steps were performed before deploying WebLM server and attempting to install a license file: 1. Check whether "C:\temp" folder (for a Windows system) or "/var/tmp" folder (for a Unix system) exists and that it has "write" permissions. 2. Ensure that there are no multiple instances of WebLM server running on the same system with a license file for the same product installed.
```

This error might occur due to multiple reasons. This section covers a number of reasons that might result in license installation issue on a WebLM server that is hosted by a Linux system. The section also provides the steps that you can take to resolve such issues.

License installation fails because of the presence of files from an earlier license installation

The error might occur if you run the Avaya Diagnostic Server installer more than once on the server and licensed the instances of Avaya Diagnostic Server. A license installation attempt for a new instance might fail if the `.##<HOSTNAME>SLAMon.l` file is left in the `/var/tmp` directory of the host server from a previous installation. The leftover file from an earlier installation has user ID and group ID instead of the actual user name and group name. This issue occurs as the user and group that owned the file got deleted during the uninstallation of the previous instance of Avaya Diagnostic Server.

Note:

The <HOSTNAME> variable that is part of the file name mentioned earlier depicts the actual host name of the server.

Resolution

Procedure

1. Log on to the Linux shell of the host server as root.
2. Navigate to the to `/var/tmp` directory:

   cd `/var/tmp`
3. List the directory content to check whether the hidden file, `.##<HOSTNAME>SLAMon.l`, is present in the directory:

   ls `-la`

   The command displays the content of the directory including any hidden files and directories.

   Note down the actual file name. For example, if the server host name is MyHost, then you might see the `.##MyHostSLAMon.l` file.
4. Delete the file you found in Step 3.

   rm `.##MyHostSLAMon.l`
5. Return to the WebLM interface and try to reinstall the license file.

License installation fails because of incorrect or insufficient entry in the hosts file

WebLM is unable to resolve the host name due to incorrect or insufficient entry in the `/etc/hosts` file. WebLM displays the error message as mentioned earlier.

Resolution

Procedure

Make an entry to the `/etc/hosts` file or configure DNS correctly to ensure that the host name is resolvable and reachable.

Resetting or restoring the password of the cohosted WebLM server

On the first login to the WebLM server, the system prompts you to change the default password. If you forget the password of the WebLM server that was installed locally with the SLA Mon server, you can reset the password back to the default one. Later, if required, you can also restore the password you set for the WebLM server.

Solution

1. Log on to the Avaya Diagnostic Server host as root.
2. Run the following command to reset the password to the default password:

   ```
   /usr/local/bin/weblm_password reset
   ```
3. Run the following command to restore the password that you set for the WebLM server:

   ```
   /usr/local/bin/weblm_password restore
   ```

Permission denied error when ASG users run SLA Mon services operations as `/sbin/service`

When you, as an ASG user, issue commands to perform operations, such as start, stop, restart, and status, on SLA Mon services as the following, you get a permission denied message:

`/sbin/service` `slamonsrvr status`

`/sbin/service` `slamonweb start`

`/sbin/service` `slamonsrvr stop`

Resolution

Procedure

As an ASG user, you must run the commands as one of the following:

- **`service`** *`<service_name> <operation>`*

For example:

service slamonsrvr status

- **sudo /sbin/service** *<service_name> <operation>*

  For example:

  sudo /sbin/service slamonsrvr status

Scheduled tasks on Avaya Diagnostic Server not functioning correctly after the system time is changed

Resolution

Procedure

Each time you reset the system time, restart the SLA Mon services:

service slamonsrvr restart

service slamonweb restart

service slamondb restart

Chapter 12: Service pack installation

Service pack installation

The service pack releases of Avaya Diagnostic Server are applied automatically if you activated the automatic software update feature in Avaya Diagnostic Server. Otherwise, you can apply the service packs manually by following the instructions in the release notes or the email notifications that you receive about software updates. You must keep the following points in mind about service pack implementation:

- When a service pack is installed, manually or automatically, the service pack applies only to the installed components of Avaya Diagnostic Server. If you install a new component of Avaya Diagnostic Server after a service pack implementation, the service pack does not apply to the new component.
- You can run the installer of a base Avaya Diagnostic Server version to install a new component after a service pack implementation. For example, if you already applied service pack 2.0.1.0, you can still run the Avaya Diagnostic Server 2.0 installer to install the new component.

  Note:

  To get the latest fixes and enhancements, apply the latest service pack after installing the base version of an Avaya Diagnostic Server component.
- You can rerun the installer of a service pack that you applied on Avaya Diagnostic Server to apply the same to a newly installed Avaya Diagnostic Server component.

  Note:

  For information about installing a service pack, see the release notes and the email notifications about software updates. You can find the downloaded software packages in the `/opt/avaya/ads/Upgrade/packages` folder of the host server.

Appendix A: Installing Java Runtime Environment

Installing Java 1.7 using an archive binary

Before you install Avaya Diagnostic Server, you must install JRE 1.7 on the RHEL host server. RHEL comes with a version of Java that might not be compatible with Avaya Diagnostic Server.

About this task

Use this procedure to install JRE 1.7 using an archive binary file, `.tar.gz`. This procedure is useful when you want to maintain multiple versions of JRE simultaneously.

This procedure considers that the target server is a 64-bit RHEL and uses the file `jre-7u<version>-linux-x64.tar.gz`. For a 32-bit RHEL server, download the binary archive file, `jre-7u<version>-linux-i586.tar.gz`, and use the file in the steps in the following procedure.

Procedure

1. On the RHEL server, enter the following URL in the web browser:

   `http://www.oracle.com/technetwork/java/javase/downloads/jre7-downloads-1880261.html`

   Note:

   If you do not find the JRE 1.7 downloads at the mentioned URL, download JRE 1.7 from the Oracle Archive at http://www.oracle.com/technetwork/java/javase/archive-139210.html.

2. On the Java SE Runtime Environment 7 Downloads page, select **Accept License Agreement**.
3. From the list of files, download the appropriate `.tar.gz` file for your Linux system.

   For example, for a 64-bit server, download `jre-7u<version>-linux-x64.tar.gz`.
4. Open a terminal on the RHEL server and log in as an administrator user.
5. From the directory where you downloaded the `.tar.gz` archive binary, copy the file to the location where you want to install the JRE.
6. Change directory to the location where you copied the archive binary.
7. Run the following command to unpack the tarball and install the JRE:

```
tar –zxvf jre-7u<version>-linux-x64.tar.gz
```

The system installs the JRE files in the `jre1.7.0_<version>` directory in the current directory.

8. After the successful installation of the JRE, perform the following to update the environment variables:
   a. Open the `/root/.bashrc` file in a text editor.
   b. In the file, search for the `JAVA_HOME` variable and update the JRE installation path, as the following:

      ```
      JAVA_HOME=/<java_install_path>/jre1.7.0_<version>
      ```

   c. Add the following lines in the file:

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

      export JAVA_HOME PATH
      ```

   d. Save and close the file.

Installing Java 1.7 using an RPM binary

About this task

Use this procedure to install JRE 1.7 using an RPM binary file, `.rpm`. In this procedure, you must uninstall any earlier installations of the JRE packages. If you must maintain multiple versions of JRE simultaneously, use the archive binary file (.tar.gz) for JRE installation.

This procedure considers that the target server is a 64-bit RHEL and uses the file `jre-7u<version>-linux-x64.rpm`. For a 32-bit RHEL server, download the RPM binary file, `jre-7u<version>-linux-i586.rpm`, and use the file in the steps in the following procedure.

Procedure

1. On the RHEL server, enter the following URL in your web browser:

   ```
   http://www.oracle.com/technetwork/java/javase/downloads/jre7-downloads-1880261.html
   ```

   Note:

   If you do not find the JRE 1.7 downloads at the mentioned URL, download JRE 1.7 from the Oracle Archive at http://www.oracle.com/technetwork/java/javase/archive-139210.html.

2. On the Java SE Runtime Environment 7 Downloads page, select **Accept License Agreement**.

   You must accept the license agreement to download the file.

3. From the list of files, download the appropriate `.rpm` file for your Linux system.

For example, for a 64-bit server, download `jre-7u<version>-linux-x64.rpm`.

4. Open a terminal on the RHEL server and log in as root.
5. Run the following command to uninstall any earlier installations of the JRE packages:

   rpm `-e <package name>`
6. Change directory to the location where you downloaded the `.rpm` file.
7. Run the following command to install the JRE package:

   rpm `-ivh jre-7u<version>-linux-x64.rpm`

   The JRE installation is complete.
8. Delete the `.rpm` file if you want to save disk space.
9. Exit the root shell. You need not reboot the server.
10. After the successful installation of the JRE, perform the following to update the environment variables:
    a. Open the `/root/.bashrc` file in a text editor.
    b. In the file, search for the `JAVA_HOME` variable and update the JRE installation path, as the following:

       `JAVA_HOME=/<java_install_path>/jre1.7.0_<version>`
    c. Add the following lines in the file:

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

       export JAVA_HOME PATH
       ```
    d. Save and close the file.

Verifying the Java version

About this task

You can test the Java installation by verifying the installed Java version.

Procedure

Start a new shell prompt on the Linux system and enter the following command:

`java -version`

Result

The system displays the version of Java.

Example

```
java version "1.7.0_51" Java(TM) SE Runtime Environment (build 1.7.0_51-
b11) Java HotSpot(TM) Client VM (build 20.4-b02, mixed mode, sharing)
```

Updating the Java environment variable after a JRE upgrade

About this task

If you upgrade the version of JRE on the host server of Avaya Diagnostic Server, you must update the JAVA_HOME environment variable in the `.bashrc` file of the root user and the user who owns the file system and the services associated with SAL Gateway.

Use this procedure to update the JAVA_HOME variable for the root user and the SAL Gateway user whenever you install an updated version of Java on the host server.

Note:

This procedure considers the SAL Gateway user as saluser, the default user name that SAL Gateway installer accepts. If you are using a different user name for SAL Gateway, replace saluser with that user name in the procedure.

Procedure

1. Perform the following to update the Java environment variable for the SAL Gateway user:
   a. Open the `/home/saluser/.bashrc` file in a text editor.
   b. Insert `export JAVA_HOME = <location of the installed JRE>` in the file.

      For example, insert `export JAVA_HOME =/usr/java7/jre1.7.0_51` if `/usr/java7/jre1.7.0_51` is the location of the installed JRE.
   c. Save and close the `/home/saluser/.bashrc` file.
2. Perform the following to update the Java environment variable for root:
   a. Open the `/root/.bashrc` file in a text editor.
   b. In the file, search for the `JAVA_HOME` variable and update the JRE installation path, as the following:

      `JAVA_HOME=/usr/java7/jre1.7.0_51`
   c. Add the following lines in the file:

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

      export JAVA_HOME PATH
      ```
   d. Save and close the file.

Next steps

Restart the services of each Avaya Diagnostic Server component.

Installing JCE Unlimited Strength Jurisdiction Policy Files

About this task

Use this procedure to install Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files on the Avaya Diagnostic Server host. The JCE policy files that are bundled with JRE 1.7 support maximum 128-bit cryptographic strength. To support cryptographic strengths greater than 128 bit, download JCE Unlimited Strength Jurisdiction Policy Files from the Oracle site and install the files in the JRE location.

Note:

If you use SNMP v3 for SAL Gateway and set the authentication protocol as AES 192 or AES 256, you must update JCE with Unlimited Strength Jurisdiction Policy Files.

Procedure

1. On the host server, open the Oracle Java SE Downloads page, http://www.oracle.com/technetwork/java/javase/downloads/index.html.
2. From the Additional Resources section, download Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files for the installed JRE version.
3. Unzip the downloaded zip file to a directory.
4. From the directory, copy the following `.jar` files to `$JAVA_HOME/jre/lib/security`:
   - `local_policy.jar`
   - `US_export_policy.jar`

   Note:

   These files already exist in the path. Therefore, you must replace the existing files.

Next steps

Restart the services of each Avaya Diagnostic Server component.

Appendix B: Disabling the SELinux protection

About this task

Use this procedure to disable the SELinux protection on a Linux system. For other methods to configure and disable SELinux, see the SELinux documentation for your Linux operating system.

Procedure

1. Log in as root to the Linux host.
2. Run the following command to check if SELinux is enabled and in the *Enforcing* mode:

   `getenforce`

   If the output is `Enforcing`, continue to the next step.
3. Open the `/etc/selinux/config` file in a text editor, and change the following line:

   `SELINUX=enforcing`

   To:

   `SELINUX=disabled`

   Important:

   Verify that the syntax in the file exactly matches the entry as shown here.
4. Save the file and exit the text editor.
5. Reboot the system.

   The SELinux protection is disabled.

Appendix C: Instructions for operating system upgrade

Perform the following steps for operating system upgrade on an existing server.

1. If the host has any earlier version of SAL Gateway or Avaya Diagnostic Server, upgrade to Avaya Diagnostic Server 2.0 or later.

   Note:

   The full backup and restore facility of configuration data is available from Avaya Diagnostic Server 2.0 onwards only. If you want to back up network monitoring test results, upgrade to Avaya Diagnostic Server 2.5 or later.

2. Take a full backup of Avaya Diagnostic Server.
3. Install the new operating system according to the installation instructions provided in the installation documentation for the specific RHEL version on the Red Hat site.
4. On the upgraded server, install the same version of Avaya Diagnostic Server that you backed up.
5. Restore the backed up data to the new Avaya Diagnostic Server.
6. If required, correct the IP address from the SAL Gateway UI after the restore operation.

   The restore operation restores the original SAL Gateway IP address.

   Do not reregister SAL Gateway and managed devices. The restore operation restores the registration information. Also during the installation of Avaya Diagnostic Server, you can provide the original SEID and product ID of SAL Gateway.

7. SAL Gateway displays the onboarding status of managed devices according to the configuration data at the time of backup. If the post restore IP address of SAL Gateway is different from the IP address at the time of backup, perform the following:

   a. Off board the devices that have the status as onboarded.

   b. Onboard the devices again.

   This manual task is associated with the post restore change of IP address.

8. If the IP address of the host has changed, run a rediscovery of the SLA Mon agents.
9. If required, perform any OS-related configuration or hardening according to the instructions provided in the current document and the *Avaya Diagnostic Server Additional Security*

Configuration Guidance document available on the Avaya Support website, http://support.avaya.com.

Appendix D: Commands to check disk partitioning on the operating system

The Avaya Diagnostic Server installer requires a certain amount of disk space in `/var` and `/opt` based on the components that you select to install. You can use the following commands to check whether hard disk partitioning exists on the system and whether `/var` and `/opt` are in the same or separate partitions.

Commands to check disk partitioning

You can run the following two commands and compare the command outputs to evaluate disk partitioning and available disk space for each file systems:

- **df** `--block-size=G`

  The command displays the disk space allocated and the available disk space for the respective file systems as well as the mount details. The displayed space details are in GB.

- **df** `-P` *<directory>*

  For example: **df** `-P /opt`

  The command displays the file system that the `/opt` directory is part of.

You can run the following two commands and compare the outputs to check whether `/opt` and `/var` are in the same or different partitions.

- **df** `-h /opt`
- **df** `-h /var`

Commands to resize a partition

You can use the following series of commands to resize a partition.

Note:

For more information, see the partition guide for the operating system distribution.

Warning:

Do not attempt to resize a partition on a device that is in use. Before resizing a partition, boot in the rescue mode or unmount any partitions on the device and turn off any swap space on the device.

1. **parted** /dev/sda

   Where, /dev/sda is the device on which you want to resize the partition.

2. **print**

3. Run the **resize** command followed by the minor number for the partition to be resized, the starting place in megabytes, and the end place in megabytes.

   For example:

   resize 3 1024 2048

Appendix E: Configuring TLS1.2 on the SLA Mon Server

About this task

Use this procedure to set the SLA Mon server to use only TLS1.2 for the communication between the SLA Mon server and the agent. On the SLA Mon server, you can enable or disable the TLS versions to list the supported versions using the configuration file.

Procedure

1. Log on to the SLA Mon Server as a root user.
2. Run the following command to open the `agentcom-slamon.conf` file:

   `vi` `/opt/avaya/slamon/bundleconf/agentcom-slamon.conf`
3. Locate the entry *keyServer.protocols* in the file.
4. Remove the hash (#) character in front of the entry to uncomment the line.
5. Change the entry to use TLS1.2 version only.

   keyServer.protocols=TLSv1.2
6. Save and close the configuration file.
7. Run the following command to restart the slamonsrvr service:

   `service slamonsrvr restart`

   Note:

   After you restart the slamonsrvr service, you must wait for maximum three minutes to start the slamonweb service. The waiting time can be less depending on the number of agents the server discovers.
8. Run the following command to restart the slamonweb service:

   `service slamonweb restart`

   After you configure TLSv1.2 on the SLA Mon server, the server uses TLSv1.2 only to communicate with the SLA Mon agents.

Note:

The configuration file can be changed to provide a list of protocols separated by comma as follows: `keyServer.protocols=TLSv1.1,TLSv1.2`. Also, the SLA Mon server and the agent uses the common version of the protocols that both can handle. Thus, if the SLA Mon Server is configured to use TLSv1.1 and TLSv1.2 and the agent is configured to use TLSv1.2, then they will use only TLSv1.2, and vice versa. If the agent does not support any of the configured protocols, the communication between the server and the agent is not supported

Appendix F: Configuring the SLA Mon Server UI timeout settings

About this task

Use this procedure to configure the SLA Mon Server UI session timeout settings. The default session timeout is set as 10 minutes.

Procedure

1. Log on to the SLA Mon Server as a root user.
2. Run the following command to open the `web.xml` file:

   ```
   vi /opt/avaya/slamon/tomcat/webapps/slamon/WEB-INF/web.xml
   ```

3. Locate the entry *<session-timeout>10</session-timeout>* in the file.
4. Change the number of minutes in the entry as required.
5. Save and close the configuration file.
6. Run the following command to restart the slamonweb service:

   ```
   service slamonweb restart
   ```

   The UI session will remain active for the configured number of minutes.

Glossary

AgentX	Agent Extensibility Protocol
Alarm	An Avaya-specific XML message wrapper around a trap.
Alarm ID	A 10-digit numeric field where the first two digits indicate the product family and the remaining numbers are a sequential assignment created by ART. For example, 1012345678. The Product ID and Alarm ID are exactly the same number.
Authentication	The process of proving the identity of a particular user.
Authorization	The process of permitting a user to access a particular resource.
Avaya Aura® Communication Manager	A key component of Avaya Aura®. It delivers rich voice and video capabilities and provides a resilient, distributed network for media gateways and analog, digital, and IP-based communication devices. It includes advanced mobility features, built-in conference calling, contact center applications and E911 capabilities.
Avaya Diagnostic Server	Avaya Diagnostic Server is an Avaya application suite to provide secure remote access and advanced diagnostics services on the customer network. The terms Avaya Diagnostic Server and Diagnostic Server are used interchangeably.
Call Management System	An application that enables customers to monitor and manage telemarketing centers by generating reports on the status of agents, splits, trunks, trunk groups, vectors, and VDNs. Call Management System (CMS) enables customers to partially administer the Automatic Call Distribution (ACD) feature.
Command Line Interface	A text-based interface for configuring, monitoring, or operating an element. Command Line Interface (CLI) is often supported over RS-232, telnet, or SSH transport.
Credential	ASG key, password, or SNMP community string.
Credential Package	Package containing ASG keys and Passwords from Avaya back-office.

Demilitarized Zone (DMZ)	In computer networking, DMZ is a firewall configuration for securing local area networks (LANs).
Domain Name System (DNS)	A hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. A DNS resolves queries for domain names into IP addresses for the purpose of locating computer services and devices worldwide.
eToken	A USB-based FIPS-140 certified smart card which stores a user's certificates and corresponding private keys. The private keys of the X.509 certificates on the eToken are usually protected by a pass phrase.
Global Access Server (GAS)	The GAS server is specifically designed to enhance the performance of remote access and allow separation of remote access from file transfers (session separation). The user's browser and the Agent for the target device are automatically directed to the nearest Global Access Server with available capacity.
Graphical User Interface (GUI)	A type of user interface which allows people to interact with a computer and computer-controlled devices, which employ graphical icons, visual indicator or special graphical elements along with text or labels to represent the information and actions available to a user.
Internet Engineering Task Force	A technical working body of the Internet Activities Board. Internet Engineering Task Force (IETF) develops new TCP/IP standards for the Internet.
Lightweight Directory Access Protocol	A data store used to store user information such as name, location, password, group permissions, and pseudo permissions.
Managed Element	A managed element is a host, device, or software that is managed through some interface.
Product ID	A 10-digit numeric field where the first two digits indicate the product family and the remaining numbers are a sequential assignment created by ART. For example, 1012345678. The Product ID and Alarm ID are exactly the same number.
Public Key Infrastructure (PKI)	An authentication scheme that uses exchange of certificates which are usually stored on a fob. The certificates use asymmetric public key algorithms to avoid sending shared secrets such as passwords over the network. Certificates are usually generated and signed by a certificate authority (CA) such as VeriSign. CAs and the signing certificates have expiry dates, and all can be revoked. Authentication with certificates requires verification that the certificate is valid, that the client sending the certificate possesses the private key for the certificate, that the certificate is signed by a trusted certificate authority, that the certificate and its signers have not expired and that the certificate and signers have not been

	revoked. Checking a certificate for revocation requires looking up the certificate in a Certificate Revocation List (CRL) or querying an Online Certificate Status Protocol (OCSP) service.
Secure Socket Layer (SSL)	A protocol developed by Netscape to secure communications on the Transport layer. SSL uses both symmetric and public-key encryption methods.
Solution Element ID (SE ID)	The unique identifier for a device-registered instance of a Solution Element Code. This is the target platform which is being remotely serviced or accessed by this solution. Solution Elements are uniquely identified by an ID commonly known as Solution Element ID or SEID in the format (NNN)NNN-NNNN where N is a digit from 0 to 9. Example: Solution Element ID (000)123-5678 with solution element code S8710.
Transport Layer Security (TLS)	A protocol based on SSL 3.0, approved by IETF.

Index

E

F

H

I

J

L

M

N

O

P

R

S

T

U

V

W