Deploying Avaya Diagnostic Server

Release 4.1
Issue 1
November 2022

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

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. 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 set of Designated Processors that hosts (physically or virtually) 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: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. 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.

Cluster License (CL). End User may install and use each copy or an Instance of the Software only up to the number of Clusters as indicated on the order with a default of one (1) Cluster if not stated. “Cluster” means a group of Servers and other resources that act as a single system.

Enterprise License (EN). End User may install and use each copy or an Instance of the Software only for enterprise-wide use of an unlimited number of Instances of the Software as indicated on the order or as authorized by Avaya in writing.

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 EQUIYIPMENT (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.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Contents

Chapter 1: Introduction

Purpose

The document contains installation, initial configuration, and basic maintenance checklists and procedures for Avaya Diagnostic Server.

This document is intended for people who install, configure, and maintain Avaya Diagnostic Server at a customer site.

Change history

Issue	Date	Summary of changes
Release 4.0, Issue 1	January 2022	The first issue of the document in this release. Updated the following topics: • Supported operating system and Java versions for upgrade on page 110 • Software requirements on page 31 • SAL Gateway on page 14 • Migrating Avaya Diagnostic Server data in the unattended mode on page 128 • Installing and enabling iptables on RHEL 7.x and 8.x on page 39 • Backing up Avaya Diagnostic Server data using a migration utility on page 126 • Upgrading Avaya Diagnostic Server in the unattended mode on page 114 • Upgrade paths to Avaya Diagnostic Server 4.1 on page 108 • Testing SAL Gateway Managed Services on page 104 • Editing the syslog configuration file for SAL Gateway on page 85 • Upgrading Avaya Diagnostic Server in the attended mode on page 111 • Updating the Java environment variable after a JRE upgrade on page 161 • Cleaning up SAL Gateway files on page 147 • Firewall (iptables) configuration on page 140 • Starting the SNMP subagent service on page 144 • Starting the SNMP master agent service on page 143 • Configuring the firewall for IPv6 on page 142 • Configuring the firewall for IPv4 on page 140 • Defining an SNMP v3 user on page 139 • Configuring the master agent to communicate with the subagent on page 136 • SNMP capability in SAL Gateway on page 134 • Support for Enhanced Access Security Gateway on page 102 • Changing the WebLM server address on the SLA Mon server on page 100

Table continues…

Issue	Date	Summary of changes
		• Updating iptables for SLA Mon on page 94 • Configuring the local syslog server for SLA Mon on page 94 • Editing the syslog configuration file for SLA Mon on page 93 • Adding an SSL/TLS certificate to the truststore of the SLA Mon server user interface on page 92 • Replacing the SSL/TLS certificate of the SLA Mon server user interface on page 90 • Updating iptables for SAL Gateway on page 83 • Setting up additional firewall rules for remote administration of SAL Gateway on page 84 • ADS_Response.properties file on page 66 • Migration checklist on page 123 • Migration of Avaya Diagnostic Server on page 123 • Testing the slamondb service on page 107 • Migrating Avaya Diagnostic Server data in the attended mode on page 127 • Uninstalling Avaya Diagnostic Server in the attended mode on page 130

Table continues…

Issue	Date	Summary of changes
Release 4.1, Issue 1	November 2022	The first issue of the document in this release. Updated the following topics: • Supported operating system and Java versions for upgrade on page 110 • Software requirements on page 31 • ADS_Response.properties file on page 66 • Uploading the SAL Policy Manager certificate to SAL Gateway on page 86 • Minimum hardware requirements for upgrade on page 110 • Checklist for upgrading from Avaya Diagnostic Server 4.0 to 4.1 on page 108 • Upgrading Avaya Diagnostic Server in the unattended mode on page 114 • Upgrading Avaya Diagnostic Server in the attended mode on page 111 • Completing the SAL Gateway upgrade on page 113 • Avaya Diagnostic Server installation overview on page 48 • Upgrade paths to Avaya Diagnostic Server 4.1 on page 108 • Supported operating system and Java versions for upgrade on page 110

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. • Secure remote connection to third party devices that are managed by SAL Gateway • Centralization of remote inventory management, logging, and authorization. • The latest SAL enhancements enables a secure, bi-directional communication between customer devices and Avaya Private Cloud Service (APCS) tools.
Alarm transport	SAL Gateway	• Aggregation and secure transport of alarms from Avaya products and third party devices that are managed by SAL Gateway to Avaya. • Alarm logging and filtering.
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.

Table continues…

Feature	Avaya Diagnostic Server component	Description
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. • 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 Service 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 HTTPS communication. Therefore, SAL minimizes network impact.

SAL uses CA certificate-based authentication for remote access requests. You can intelligently establish access policies using an optional SAL Policy Manager.

Avaya Diagnostic Server has introduced Flex support for cloud based Avaya products. Flex platform assists in uniform installation and standardizes the product packaging for all the types of deployment.

The flex supported products are:

- Cluster Control Manager
- Common Service Platform
- Avaya Analytics

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 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.

Table continues…

Feature	Description
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:

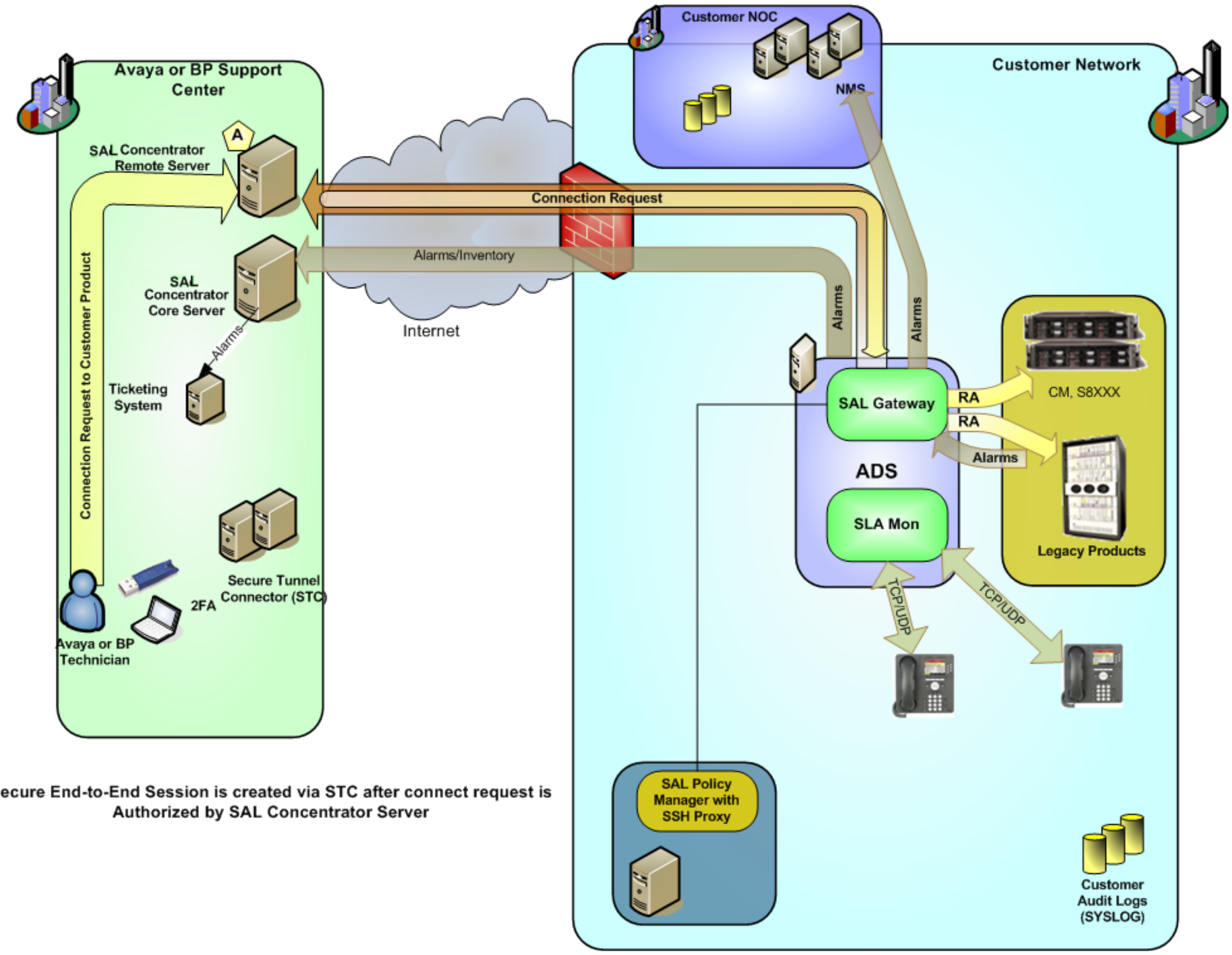
Customer NOC
NMS
Customer Network
Avaya or BP Support Center
A
SAL Concentrator Remote Server
Connection Request
Alarms/Inventory
SAL Concentrator Core Server
Internet
Alarms
Alarms
Alarms
Connection Request to Customer Product
Ticketing System
SAL Gateway
RA
RA
CM, S8XXX
Alarms
ADS
SLA Mon
Legacy Products
Secure Tunnel Connector (STC)
2FA
Avaya or BP Technician
TCP/UDP
TCP/UDP
Secure End-to-End Session is created via STC after connect request is Authorized by SAL Concentrator Server
SAL Policy Manager with SSH Proxy
Customer Audit Logs (SYSLOG)

Figure 1: Avaya Diagnostic Server architecture

Capacity of Avaya Diagnostic Server

The following table provides the maximum capacity of Avaya Diagnostic Server 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	• 1000 managed elements • 100 simultaneous remote sessions	• 150 bidirectional links for data, voice, and video together • 3000 registered agents • 3 simultaneous packet capture sessions • 3 simultaneous phone remote control sessions	• 1000 managed elements • 100 simultaneous remote sessions • 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	• 1000 managed elements • 100 simultaneous remote sessions	• 250 bidirectional links for data, voice, and video together • 5000 registered agents • 3 simultaneous packet capture sessions • 5 simultaneous phone remote control sessions	• 1000 managed elements • 100 simultaneous remote sessions • 200 bidirectional links for data, voice, and video together • 4000 registered agents • 3 simultaneous packet capture sessions • 5 simultaneous phone remote control sessions
Standalone server: 8-GB RAM and quad core processor with 2.2 GHz speed	• 1000 managed elements • 100 simultaneous remote sessions	• 100000 registered Remote worker agents • 3 simultaneous packet capture sessions • 5 simultaneous phone remote control sessions	• 1000 managed elements • 100 simultaneous remote sessions • 8000 registered Remote Worker agents • 3 simultaneous packet capture sessions • 5 simultaneous phone remote control sessions

Table continues…

Hardware specification	Maximum load		
	SAL Gateway only	**SLA Mon only**	**Cohosted components**
Standalone server: 16-GB RAM and 8 core processor with 2.2 GHz speed	• 1000 managed elements • 100 simultaneous remote sessions	• 100000 registered Remote worker agents • 3 simultaneous packet capture sessions • 5 simultaneous phone remote control sessions • 250 bidirectional links for data, voice, and video together • 5000 registered Enterprise agents	• 1000 managed elements • 100 simultaneous remote sessions • 8000 registered Remote Worker agents • 3 simultaneous packet capture sessions • 5 simultaneous phone remote control sessions • 200 bidirectional links for data, voice, and video together • 4000 registered enterprise agents

Chapter 3: Planning and initial setup

Planning and site preparation checklist

Use this checklist to prepare the host server before installing and configuring Avaya Diagnostic Server.

#	Task	Description	Notes	✔

1	Ensure that the host server on which you want to install Avaya Diagnostic Server meets the minimum hardware requirements.	See Hardware requirements on page 30.	Use the following command to check the partitioning in the file system and available disk space:
			`df -h`
			Use the following command to check the total RAM size:
			`cat /proc/meminfo`	

2	Ensure that the operating system of the host server is a supported version of Red Hat Enterprise Linux (RHEL).	See Software requirements on page 31. Ensure that the ISO or DVD that you use to install the RHEL version is downloaded or issued from Red Hat, Inc. only. 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/.	Use the following command to check the RHEL version: `cat /etc/redhat-release`	
3	Ensure that you have root privileges to the host server and that you log in as the root user to install Avaya Diagnostic Server.			

Table continues…

#	Task	Description	Notes	✔
4	Ensure that the Bash shell, `/bin/bash`, exists on the host computer.			
5	Ensure that the SAL Gateway user, if it 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*.	

6	Ensure that OpenJDK Java Runtime Environment (JRE) 1.8 is installed on the server.	For a clean installation, you can remove any earlier JRE version, and install OpenJDK.
		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.
			RHEL 7.x comes with OpenJDK as part of the suite.
			Use the following command to check the installed Java version:
			`java -version`
			Use the following command to install OpenJDK on RHEL 8.x:
			`sudo yum install java-1.0.8-openjdk`
			Reference:
			https://access.redhat.com/documentation/en-us/openjdk/8/html-single/installing_and_using_openjdk_8_for_rhel/index	

Table continues…

#	Task	Description	Notes	✔
7	Ensure that the JAVA_HOME and PATH environment variables are set correctly to point to the location of the installed JRE 1.8.	Export the JAVA_HOME environment variable in the following files: `/root/.bash_profile` or `/root/.bashrc` See Updating the Java environment variable after a JRE upgrade on page 161.	RHEL 7.x and 8.x comes with OpenJDK as part of the suite. Therefore, the host might have multiple Java versions. You must ensure that `/etc/alternatives` is updated to use the correct JRE version supported by Avaya Diagnostic Server.	
8	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 161.	The default SAL Gateway user is *saluser*.	
9	Ensure that the host computer meets all other software requirements for Avaya Diagnostic Server.	See Software requirements on page 31.		
10	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.		
11	Ensure that the RHEL host is configured to use a valid DNS server that resolves external host names.			
12	(Optional) If you are installing SAL Gateway on a separate server and the managed devices are configured with IPv6 settings, configure the host for IPv6.	SAL Gateway supports both IPv4 and IPv6, However, the SLA Mon server works only on IPv4. If you plan to install Avaya Diagnostic Server with SLA Mon server or with both components as co-hosted, configure the host for IPv4 only. Do not configure the host for IPv6.		

Table continues…

#	Task	Description	Notes	✔
13	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/. For the Avaya Diagnostic Server virtual appliance deployment, follow the timekeeping best practices that are recommended for the virtualized environment.	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 files from multiple servers. For more information about NTP, see http://www.ntp.org or http://www.ntp.org/ntpfaq/NTP-a-faq.htm.	
14	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 3.2.x or later.	For Yum upgrade, run the following command: `yum update yum`	
15	Ensure that the Yum repository is configured correctly on the host.	For RHEL 7.x see https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/system_administrators_guide/ch-yum#sec-Configuring_Yum_and_Yum_Repositories. For RHEL 8.x see https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/configuring_basic_system_settings/managing-software-packages_configuring-basic-system-settings		

Table continues…

#	Task	Description	Notes	✔
16	Ensure that the minimum set of RPMs required for the installation and correct functioning of Avaya Diagnostic Server are installed on the RHEL host.	See RPMs for Avaya Diagnostic Server on page 32. If the default package set that comes with RHEL does not include the required RPMs, install the RPMs before installing Avaya Diagnostic Server. **Note:** While installing the RPMs, ensure that the RPMs match the architecture of the server, that is, 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 12, Troubleshooting.	
17	Ensure that the iptables service is installed on the host server and is enabled.	Run the following commands start the iptables service: RHEL 7.x and 8.x: `systemctl start iptables` In RHEL 7.x and 8.x, ensure that the firewall service is disabled and the iptables service is installed and enabled. See Installing and enabling iptables on RHEL 7.x and 8.x on page 39.	Run the following commands to check the status and ensure that the iptables service is enabled: RHEL 7.x and 8.x: `systemctl status iptables` When the service is enabled, the iptables rules are displayed in the output.	
18	Ensure that any firewall between the browser of the administrator and Avaya Diagnostic Server do not block ports 7443 and 4511.			
19	Ensure that the `/etc/hosts` and `/etc/sysconfig/network` files have host name entries that match the values that the system displays when you run the **`hostname`** command.			

Table continues…

#	Task	Description	Notes	✔
20	Ensure that the server host name does not resolve to the loopback address, 127.0.0.1.	In the `/etc/hosts` file, add the host name to IP address mapping entry as the first line of the file. Ensure that there are no other entries or commented lines apart from the host name. Make the entry as the following: `<ip_address> <hostname>` ✱ **Note:** For Amazon Web Services server, provide the internal IP address as *<ip_address>*		

21	To enable remote agent logging on the local RHEL host server, 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:
	`$ModLoad imudp`
	`$UDPServerRun 514`
		After making this change, you must restart the rsyslog service to make the changes effective.
		For more information about editing the rsyslog file, see Editing the syslog configuration file for SAL Gateway on page 85.
			To restart the service:
			In RHEL 7.x and 8.x:
			`systemctl restart rsyslog`	

22	To generate Solution Element ID for SAL Gateway automatically during installation, ensure that the host server has Mozilla FireFox 34.x or later as the default web browser.	The GUI-based installer opens the Global Registration Tool (GRT) website on the default browser for SAL Gateway registration. Other web browsers available with RHEL might not support the GRT website.	To obtain the Solution Element ID and Product ID prior to the SAL Gateway installation, See *Technical Onboarding Help Document* at https://support.avaya.com/registration.	

23	For remote connectivity using OpenSSL, ensure that the host has OpenSSL and Apache Portable Runtime (APR) RPMs installed.	See OpenSSL support for SAL remote connectivity on page 39.	To check the current versions of OpenSSL and APR, run the following commands:
			`rpm -q openssl`
			`rpm -q apr`	

Table continues…

#	Task	Description	Notes	✔

24	Ensure that OpenSSL version 1.0.1e or later is available on the host.	SLA Mon 3.0 employs Enhanced Access Security Gateway (EASG) authentication, which is a certificate-based version of the dynamic authentication method used in previous releases of SLA Mon. With EASG, Avaya support tools and personnel can authenticate with SLA Mon to respond to service requests.
		To enable EASG, the host server must have OpenSSL version 1.0.1e or later.
			To identify the current OpenSSL version, run the command:
			`rpm -q openssl`
			You can upgrade OpenSSL using a Red Hat subscription. Use the following command to upgrade to the latest OpenSSL version:
			`yum upgrade openssl`	

25	Ensure that Security-Enhanced Linux (SELinux) is disabled on the Avaya Diagnostic Server host.	See Disabling the SELinux protection on page 40.	SAL Gateway and SLA Mon might not function properly if SELinux on the host server is enabled and in the enforcing mode.	
26	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.	
27	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**.	
28	Download the Avaya Diagnostic Server software from Product Licensing and Delivery System (PLDS).	See Downloading software from PLDS on page 42.		

Table continues…

#	Task	Description	Notes	✔
29	Copy and extract the downloaded `ADS-Installer-<version_no>-<build_no>.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 44.		
30	**(Optional)** Obtain the SAL Gateway identifying numbers, Solution Element ID and Product ID, from Avaya.	Obtaining the IDs in advance is not mandatory. Additional options are: • 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 user interface. To obtain these numbers in advance, See *Technical Onboarding Help Document* at https://support.avaya.com/registration.	If you use the default IDs to install SAL Gateway, you must 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.	
31	Obtain the addresses of SAL Core Server and SAL Remote Server, and ensure that you have network access to these addresses.	During the SAL Gateway installation, you must ensure that the installer is using the following fully qualified domain names (FQDN) and port numbers to configure the communication paths of SAL Gateway with Avaya: • SAL Core Server: *secure.alarming.avaya.com* and port 443 • SAL Remote Server: *remote.sal.avaya.com* and port 443 Configure the firewall and outbound proxies on your network to allow access to these FQDNs.		

Table continues…

#	Task	Description	Notes	✔
32	Ensure that you have network access to Secure Tunnel Connectors (STCs).	You need not administer STCs 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 the STC host names.	For the list of SAL FQDNs or IP addresses that SAL Gateway needs to communicate with, see *Avaya Diagnostic Server Port Matrix*.	

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 SAL Gateway registration 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 SAL Gateway registration 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:				

Table continues…

Field	Description	Required to proceed	Value provided by	Value
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	
(Optional) To configure a proxy server for Internet access on the customer network:				
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 SAL Policy Manager with SSH Proxy:				
Host name	The fully qualified domain name (FQDN) of the host server where SAL Policy Manager with SSH Proxy is installed.	Optional	Customer	
port	The port number that SAL Policy Manager uses for incoming communications from SAL Gateway.	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	
Encryption method	The method of encryption for SMTP server. The options are: • None • STARTTLS • SSL/TLS	Yes	Customer	
Administrator email address	The email address of the administrator to whom email notifications must be sent.	Yes	Customer	

Table continues…

Field	Description	Required to proceed	Value provided by	Value
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 the SLA 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	

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	4 GB	6 GB	4 GB	8 GB	6 GB	8 GB
Hard disk space	• Free space in `/opt/avaya`: 10 GB • Free space in `/var`: 80 MB [1]	• Free space in `/opt/avaya`: 40 GB • Free space in `/var`: 100 MB	• Free space in `/opt/avaya`: 10 GB • Free space in `/var/lib`: 30 GB [2] • Free space in `/var/log`: 1 GB	• Free space in `/opt/avaya`: 10 GB • Free space in `/var/lib`: 175 GB • Free space in `/var/log`: 5 GB	• Free space in `/opt/avaya`: 20 GB • Free space in `/var`: 80 MB • Free space in `/var/lib`: 30 GB • Free space in `/var/log`: 1 GB	• Free space in `/opt/avaya`: 50 GB • Free space in `/var`: 100 MB • Free space in `/var/lib`: 175 GB • Free space in `/var/log`: 5 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 a fresh installation of Avaya Diagnostic Server:

[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 Monserver stores data in this directory. In addition, never change the `/opt` and the `/var/lib` directory paths in the installation script.

Component	Supported versions
Operating system	• Red Hat Enterprise Linux (RHEL): - 7.x - 8.x
Java	• OpenJDK 8.0
Perl	Version 5.10 or later
OpenSSL	Version 1.0.1e or later
OpenSSH	Version 7.0 or later
Web browser	Google Chrome

RPMs for Avaya Diagnostic Server

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 are required and recommended for Avaya Diagnostic Server.

Required RPMs for installation and operation of Avaya Diagnostic Server

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

Package	Required on RHEL 7.x	Required on RHEL 8.x
bash	Yes	Yes
chkconfig	Yes	Yes
coreutils	Yes	Yes
findutils	Yes	Yes
gawk	Yes	Yes
grep	Yes	Yes
iproute	Yes	Yes
iptables	Yes	Yes
iptables-services	Yes	Yes
iputils	Yes	Yes
lsof	Yes	Yes
openssl	Yes	Yes
pam	Yes	Yes
passwd	Yes	Yes

Table continues…

Package	Required on RHEL 7.x	Required on RHEL 8.x
procps	No	No
procps-ng	Yes	Yes
rpm	Yes	Yes
rpm-libs	Yes	Yes
sed	Yes	Yes
setup	Yes	Yes
shadow-utils	Yes	Yes
sudo	Yes	Yes
tar	Yes	Yes
tcpdump	Yes	Yes
unzip	Yes	Yes
yum	Yes	Yes
zip	Yes	Yes

Table 2: Additional RPMs required for SAL Gateway

Package	Required on RHEL 7.x	Required on RHEL 8.x
cronie	Yes	Yes
cronie-anacron	Yes	Yes
crontabs	Yes	Yes
curl	Yes	Yes
dos2unix	Yes	Yes
gnutls	Yes	Yes
net-snmp	Yes	Yes
openssh	Yes	Yes
openssh-clients	Yes	Yes
openssh-server	Yes	Yes
perl	Yes	Yes
util-linux	Yes	Yes
which	Yes	Yes
libnsl	No	Yes
compat-openssl	Yes	Yes

Table 3: Additional RPMs required for the SLA Mon server

Package	Required on RHEL 7.x	Required on RHEL 8.x
coreutils-libs	No	No

Table continues…

Package	Required on RHEL 7.x	Required on RHEL 8.x
gzip	Yes	Yes
postgresql	Yes	Yes
postgresql-libs	Yes	Yes
postgresql-server	Yes	Yes

Note:

This is not an exhaustive list. You might have to install additional packages for resolving operating system dependencies and for operating and debugging purposes.

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.

Recommended RPMs for overall operation of Avaya Diagnostic Server and the operating system

Do not remove these recommended RPMs because the removal of these RPMs might impact the operation and performance of the application and operating system.

Table 4: RPMs common to both SAL Gateway and SLA Mon server

Package	Required on RHEL 7.x	Required on RHEL 8.x
audit-libs	Yes	Yes
audit-libs-python	Yes	Yes
basesystem	Yes	Yes
cpio	Yes	Yes
cracklib	Yes	Yes
cracklib-dicts	Yes	Yes
db4	No	No
ethtool	Yes	Yes
glib2	Yes	Yes
glibc	Yes	Yes
glibc-common	Yes	Yes
hwdata	Yes	Yes
initscripts	Yes	Yes
iptables-ipv6	No	No
iw	Yes	Yes
kmod	Yes	Yes
krb5-libs	Yes	Yes
libacl	Yes	Yes
libcap	Yes	Yes

Table continues…

Package	Required on RHEL 7.x	Required on RHEL 8.x
libgcc	Yes	Yes
libselinux	Yes	Yes
libsepol	Yes	Yes
libstdc++	Yes	Yes
libxml2	Yes	Yes
libXtst	Yes	Yes
man	Yes	No
man-db	Yes	Yes
mingetty	No	No
module-init-tools	No	No
ncurses	Yes	Yes
net-tools	Yes	Yes
nspr	Yes	Yes
nss	Yes	Yes
openldap	Yes	Yes
pcre	Yes	Yes
popt	Yes	Yes
psmisc	Yes	Yes
readline	Yes	Yes
rpm-python	Yes	Yes
systemd	Yes	Yes
tzdata	Yes	Yes
udev	No	No
wireless-tools	No	No
zlib	Yes	Yes

Table 5: Additional recommended RPMs for SAL Gateway

Package	Required on RHEL 7.x	Required on RHEL 8.x
apr	Yes	Yes
authconfig	Yes	Yes
cryptsetup-luks	No	No
cyrus-sasl	Yes	Yes
dbus	Yes	Yes
dbus-glib	Yes	Yes
device-mapper	Yes	Yes

Table continues…

Package	Required on RHEL 7.x	Required on RHEL 8.x
dhclient	Yes	Yes
dmidecode	Yes	Yes
dmraid	Yes	Yes
elfutils-libelf	Yes	Yes
expat	Yes	Yes
file	Yes	Yes
filesystem	Yes	Yes
gdbm	Yes	Yes
grub	Yes	No
grub2	Yes	Yes
hal	No	No
kbd	Yes	Yes
kpartx	Yes	Yes
libevent	Yes	Yes
libgcrypt	Yes	Yes
libgpg-error	Yes	Yes
libselinux-python	Yes	Yes
libsysfs	Yes	Yes
libuser	Yes	Yes
libxml2-python	Yes	Yes
logrotate	Yes	Yes
lvm2	Yes	Yes
m4	Yes	Yes
mcstrans	Yes	Yes
nc	Yes	No
newt	Yes	Yes
parted	Yes	Yes
pciutils	Yes	Yes
pm-utils	Yes	Yes
policycoreutils	Yes	Yes
redhat-logos	Yes	Yes
rootfiles	Yes	Yes
selinux-policy	Yes	Yes
selinux-policy-targeted	Yes	Yes
slang	Yes	Yes

Table continues…

Package	Required on RHEL 7.x	Required on RHEL 8.x
telnet	Yes	Yes
traceroute	Yes	Yes
usermode	Yes	Yes

Table 6: Additional recommended RPMs for the SLA Mon server

Package	Required on RHEL 7.x	Required on RHEL 8.x
binutils	Yes	Yes
ca-certificates	Yes	Yes
dbus-libs	Yes	Yes
gamin	Yes	Yes
gmp	Yes	Yes
info	Yes	Yes
keyutils-libs	Yes	Yes
libattr	Yes	Yes
libblkid	Yes	Yes
libcom_err	Yes	Yes
libidn	Yes	Yes
libnih	No	No
libusb	Yes	Yes
libutempter	Yes	Yes
libuuid	Yes	Yes
MAKEDEV	No	No
ncurses-base	Yes	Yes
ncurses-libs	Yes	Yes
nss-softokn-freebl	Yes	Yes
nss-sysinit	Yes	Yes
nss-util	Yes	Yes
redhat-release-server	Yes	Yes
sysvinit-tools	Yes	Yes
upstart	No	No
util-linux-ng	No	No

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
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 rsyslog	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.

Installing and enabling iptables on RHEL 7.x and 8.x

About this task

In RHEL 7.x and 8.x, the firewalld service is installed by default. However, you can still use the iptables service for firewall capabilities on RHEL 7.x and 8.x system.

Use this procedure to disable the firewalld service and install and enable the iptables service on an RHEL 7.x and 8.x system.

Procedure

1. Log on to the host server as root.
2. Run the following commands to disable the firewalld service:

   ```
   systemctl stop firewalld
   ```

   ```
   systemctl mask firewalld
   ```

3. Run the following command to check the status of the iptables service:

   ```
   systemctl status iptables
   ```

   If you see an output similar to the following, then the iptables service is not present:

   ```
   not-found (Reason: No such file or directory)
   ```

4. **(Optional)** If the iptables service is not present on the host server, run the following command to install the iptables-related packages:

   ```
   yum install iptables-services -y
   ```

5. Run the following to enable the iptables services to start at every system reboot:

   ```
   systemctl enable iptables
   ```

   ```
   systemctl enable ip6tables
   ```

6. Run the following to start the iptables services:

   ```
   systemctl start iptables
   ```

   ```
   systemctl start ip6tables
   ```

OpenSSL support for SAL remote connectivity

To get maximum performance with SAL remote connectivity, Avaya recommends OpenSSL. For OpenSSL support, the SAL Gateway host must have OpenSSL and Apache Portable Runtime (APR) RPMs installed.

If OpenSSL is unavailable, SAL Gateway 4.0 can function by using JDK SSL. However, Avaya does not recommend the use of JDK SSL because it severely impacts the performance of the remote connections.

The recommended requirements for using OpenSSL:

Operating System	64-bit RHEL 7.x or 8.x
OpenSSL minimum version	1.0.1e or later
APR minimum version	1.3.9 or later

Note:

Do not use OpenSSL versions 1.0.1n and 1.0.1o because these versions are subject to the `Alternative chains certificate forgery (CVE-2015-1793)` vulnerability.

Related links

Enabling OpenSSL on SAL Gateway on page 40

Enabling OpenSSL on SAL Gateway

Procedure

1. Log on to the host server as root.
2. Run the following command to upgrade the OpenSSL RPM:

   ```
   yum update openssl
   ```

3. Run the following command to install the APR RPM:

   ```
   yum install apr
   ```

Related links

OpenSSL support for SAL remote connectivity on page 39

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.

Creating the SAL Gateway user account

About this task

The SAL Gateway user, saluser, owns the file system and services associated with SAL Gateway.

If the target host is a new virtual machine or a server where SAL Gateway was never installed, saluser might not be present. Use this procedure to check for the presence of the saluser account and to create the account on the target host.

Procedure

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

   ```
   grep -c 'saluser:' /etc/passwd
   ```

   The command returns one of the following:

   - `1`: Implies that the saluser account is present on the target host.
   - `0`: Implies that the saluser account is not present on the target host.
3. If saluser is not present, run the following commands to create the user group and user account:

   ```
   /usr/sbin/groupadd salgroup
   ```

   ```
   /usr/sbin/useradd -g salgroup saluser
   ```

SAL Gateway registration

Registering a product with Avaya is an important process to uniquely identify the Avaya product for servicing or troubleshooting them. When you register a new SAL Gateway, Avaya assigns a Solution Element ID and a Product ID to the SAL Gateway. SAL Gateway becomes operational only when you configure SAL Gateway with the correct identifiers.

The following are the different methods to generate the identifiers and register SAL Gateway:

- Through the Global Registration Tool (GRT), you can manually register SAL Gateway and generate the identifiers using the material code `340055` for SAL Gateway. See *Technical Onboarding Help Document* at https://support.avaya.com/registration.
- During SAL Gateway installation in attended mode, you can use the SAL Gateway user interface to automatically generate the identifiers and register SAL Gateway. See Generating the SEID and the Alarm ID of SAL Gateway automatically on page 56
- During SAL Gateway installation in unattended mode, you can choose to install SAL Gateway with the default ID. An error message is displayed on the SAL Gateway user interface after you log in. On clicking the error message, you get the options to configure the correct Solution Element ID. See Selecting the option to specify Solution Element ID on page 54.

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

Procedure

1. In your web browser, type http://plds.avaya.com to go to the Avaya PLDS website.
2. On the PLDS website, enter your Login ID and password.

3. On the Home page, select **Assets**.
4. Select **View Downloads**.
5. Click the search icon (🔍) for Company Name.
6. In the Search Companies dialog box, do the following:

    a. In the **%Name** field, type `Avaya` or the Partner company name.

    b. Click **Search Companies**.

    c. Locate the correct entry and click the **Select** link.
7. Search for the available downloads by using one of the following:
    - In **Download Pub ID**, type the download pub ID.
    - In the **Application** field, click the application name.
8. Click **Search Downloads**.
9. Scroll down to the entry for the download file, and click the **Download** link.
10. Select a location where you want to save the file, and click **Save**.
11. **(Optional)** If you receive an error message, click the message, install Active X, and continue with the download.
12. **(Optional)** 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-<version_no>-<build_no>.tar.gz` file and copy the file to a directory on the target host.

Procedure

1. Log on to the host system as a user with administrator rights.
2. Go to the directory where you have downloaded the installer tarball file, `ADS-Installer-<version_no>-<build_no>.tar.gz`.
3. Do one of the following:
    - To verify the SHA 2 checksum, run the following command:

      ```
      sha256sum ADS-Installer-<version_no>-<build_no>.tar.gz
      ```

- To verify the MD5 checksum, run the following command:

  ```
  md5sum ADS-Installer-<version_no>-<build_no>.tar.gz
  ```

4. Check the output of the command with the SHA2 checksum or MD 5 checksum that is displayed on the downloads page for Avaya Diagnostic Server on the Avaya support site.

   For a successful download, the output must match the checksum that is displayed on the downloads page.

5. If you get a different output for the downloaded software, download the `ADS-Installer-<version_no>-<build_no>.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 to a local system, you must extract the installer file from the downloaded zip file to a local directory of the target host.

Procedure

1. Download the Avaya Diagnostic Server software from PLDS to a local system.
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-<version_no>-<build_no>.tar.gz` file to the new directory.

   You may copy the tarball file to an existing directory. However, ensure that the directory name does not contain any special characters.

4. Change directory to the directory where you copied the tarball file, and run the following command:

   ```
   tar -xvf ADS-Installer-<version_no>-<build_no>.tar.gz
   ```

   The command extracts a directory, `ADS-Installer-<version_no>-<build_no>`, to the directory where you copied the `.tar.gz` file. The new `ADS-Installer-<version_no>-<build_no>` 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 49
Installing Avaya Diagnostic Server in the unattended mode on page 65

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 30. 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.	Yes	
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 161.
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	

Table continues…

Task	Required?	Notes
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	
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 unser interface and unauthorized access to SAL Gateway and SAL Gateway user interface. 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 SAL Policy Manager with SSH Proxy on a different host.	Optional	For more information on SAL Policy Manager, see *Deploying SAL Policy Manager with SSH Proxy*.
Configure encryption settings for Apache Tomcat.	Optional	The Avaya Diagnostic Server installer is packaged with Apache Tomcat. 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.

Table continues…

Task	Required?	Notes
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 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.

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.

Note:

From Avaya Diagnostic Server 3.2 release onwards, Avaya Diagnostic Server does not support Services-VM method of deployment.

If system detects Services-VM while trying to install Avaya Diagnostic Server 4.1, the following error is displayed:

```
Services-VM deployment detected, cannot install or upgrade the
software on SVM setup. Exiting installer.
```

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 Gateway on 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 graphical user interface(GUI) 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 in graphical user interface (GUI) mode.

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, Planning and initial setup.
- 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`
  - `README.txt`

Installing Avaya Diagnostic Server in the attended mode

Starting the Avaya Diagnostic Server installation in the attended mode

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 in graphical user interface (GUI) mode to run the installer in this mode.

Before you begin

Ensure that the host server meets all specifications mentioned in Chapter 3, Planning and initial setup.

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.

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 in graphical user interface (GUI) mode.
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.
6. When the installer displays a message asking you whether to migrate the installation from a backup file, type `n` to perform a fresh installation.

   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.
7. When the installer displays the security message, perform one of the following:
   - To accept the terms and continue with the installation, type `y`.
   - To decline the terms and quit the installation, type `n`.

8. To continue with the installation if the recommended hardware requirements are not met, type `y`.

Next steps

Complete the SAL Gateway installation steps.

Complete the SLA Mon server installation steps.

Installing SAL Gateway

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. Select one of the following options from the **Encryption Method** field:
        - None
        - STARTTLS
        - SSL/TLS

    d. **(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.

   e. In the **Administrator’s Email Address** field, enter the administrator email address where you want to receive email notifications.

   f. **(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 Global Registration Tool (GRT) 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 GRT 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.

Related links

Identify SAL Gateway field descriptions on page 55

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.

Table continues…

Name	Description
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.

Related links

Configuring the SAL Gateway identification information manually on page 55

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 Global Registration Tool (GRT) webpage with an XML response.

   Note:

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

   - If the GRT 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 GRT did not generate the Alarm ID:

     ```
     Unique AlarmId failure error
     ```

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

2. Copy the XML response from `<ART-Response>` tag to `</ART-Response>` tag.
3. On the GRT Response panel of the installer wizard, paste the copied XML response in the **GRT Response** field.

   ⚠ **Caution:**

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

   - Do not include the additional XML tag: `<?xml version="1.0" encoding="UTF-8" standalone="true"?>`
   - 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 proxy settings for SAL Gateway.

Configuring the proxy settings for SAL Gateway

About this task

Use this procedure to configure the proxy server settings for SAL Gateway, if you use a proxy server for Internet access outside the firewall of the customer network. 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 on your web browser, you might require to configure the proxy settings for SAL Gateway too.

If the proxy server is certificate-based, you must add the server certificate to the SAL Gateway truststore.

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, enter values in the following fields and click **Next**:
   - **User**
   - **Password**

   The system completes the settings of the authenticated HTTP proxy server and displays the Model Package Installation panel.

Next steps

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

Related links

Installing the SAL model package in the offline mode on page 60
Installing the SAL model package in the online mode on page 59

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 SAL 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 Manager 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 SAL Policy Manager 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, click **Browse** and select the model package in the `/Models` subdirectory of the directory that gets created when you extract the tar file.
    - 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, select the default `model.zip` package, which is available in the `/Models` subdirectory of the directory that gets created when you extract the tar file. If you select a model package of earlier version, which is not compatible with the Avaya Diagnostic Server 3.0 installer, the installer displays an error message. You cannot continue with the installation unless you select a supported model package.

4. Click **Next**.

   The system displays the Policy Manager Configuration panel.

Next steps

Configure the SAL Policy Manager information.

Configuring the SAL Policy Manager information

About this task

If you have SAL Policy Manager with SSH Proxy installed on your network, use this procedure to configure the details with SAL Gateway. The use of SAL Policy Manager with SSH Proxy is optional.

Procedure

1. On the Policy Manager Configuration panel, perform the following:
   a. In the **Hostname** field, type the fully qualified domain name of the host server where SAL Policy Manager with SSH Proxy is installed.
   b. In the **Port** field, type the port number that SAL Policy Manager uses for incoming communications from 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 user interface 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 pages on the SAL Gateway user interface except the following pages, to which read only permission:

     - Policy Manager
     - 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 pages of the SAL Gateway user interface.

   Note:

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

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.

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

If you have chosen to install both components, complete the SLA Mon server installation steps.

Completing the SLA Mon server installation

About this task

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. Use this procedure to complete the SLA Mon server installation.

In Release 4.0, the SLA Mon server supports privileged access by Avaya Services to the host server through EASG, which is a PKI certificate-based authentication. During installation, you can enable or disable EASG for the SLA Mon server. Enable EASG only if you want Avaya Services access for the SLA Mon server.

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, Postinstallation configuration.
- 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, Postinstallation configuration.

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. Do 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.

3. When the system prompts to reconfigure the firewall rules for the SLA Mon server, do 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 after installation, type `n`.

     The system displays a warning message.
4. When the system prompts to configure syslog for SLA Mon logging, do one of the following:
   - To allow the installer to configure the syslog details, type `y`.
   - To configure the syslog details manually after installation, type `n`.
5. When the system prompts to enable EASG authentication, do one of the following:
   - To enable EASG and accept the following terms, type `y`.

     By enabling Avaya Services Logins, you are granting Avaya access to your system. This is required to maximize the performance and value of your Avaya support entitlements, allowing Avaya to resolve product issues in a timely manner. The product must be registered using the Avaya Global Registration Tool (GRT) at https://grt.avaya.com to be eligible for Avaya remote connectivity. See the Avaya support site at https://support.avaya.com/registration for additional information for registering products and establishing remote access and alarming.
   - To disable EASG and accept the following terms, type `n`.

     By disabling Avaya Services Logins, you are denying Avaya access to your system. This is not recommended, as it can impact Avaya's ability to provide support for the product. Unless the customer is well versed in managing the product themselves, Avaya Services Logins should not be disabled.

   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

Ensure that the host server meets all specifications mentioned in Chapter 3, Planning and configuration.

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.

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`.

The following are some important properties that you must set:

- For the `ADS_AGREELICENSE` property in the response file, replace the value `n` with `y`.
- 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.

- For the SAL Gateway component, ensure that you make the following changes in the response file:
  - Ensure that the value of `AUTOUPGRADE_CUST_SELECT` is `ON` or `OFF`. The default value is `ON`.
  - Update the SMTP server details with correct and complete values. You must provide values for the `SMTP_HOST`, `SMTP_PORT`, `SMTP_ADMIN_EMAIL`, and `SMTP_ENCRYPTION_METHOD` properties.
  - Choose a mode for model package installation by removing the hash sign (#) before the properties that follow one of the following two lines:

    `Model Package Installation fields(Online)`

    Or

    `Model Package Installation fields(Offline)`

    Ensure that the properties for the other mode are commented out. For example, if you choose the Offline mode, you must comment out the properties for the Online mode.
- For the SLA Mon server component, if you want to use a remote WebLM licensing server, replace the value of `WEBLMIP` with the IP address of the external WebLM server.

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 66

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.

Note:

- While SAL Gateway supports IPv4 and IPv6, the SLA Mon server works only on IPv4. If you plan to install Avaya Diagnostic Server with SLA Mon, configure the host for IPv4.
- If you upgrade SAL Gateway, the remote server URL is updated to remote.sal.avaya.com. Ensure that SAL Gateway can connect to this URL before you start the upgrade.

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>*.

Table continues…

Information in the file	Description

`#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.
	You must 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 4.1 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 4.1 component SAL is already installed do`
`you wish to install SLAMon (y/n)`
`ADS_SLAMON_INSTALL=y`
`# ADS 4.1 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.

The following properties are for upgrade scenarios. Update the properties in the following section only if you want to upgrade from Avaya Diagnostic Server 4.0 to 4.1. Based on the software version available in your environment, set one of the 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.	

`#ADS [4.0] 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 to Avaya Diagnostic Server 4.1 with SAL Gateway, set the value of `ADS_SAL_UPGRADE` to one of the following:
	• For only SAL upgrade, 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`

Table continues…

<table>
<tr><th>Information in the file</th><th>Description</th></tr>
<tr><td>#ADS [4.0] component SLAMon is already installed.
Which components to be installed 1) Upgrade SLAMon
2) Upgrade SLAMon and Install SAL
ADS_SLAMON_UPGRADE=1</td><td>To upgrade to Avaya Diagnostic Server 4.1 with SLA Mon, set the value of ADS_SLAMON_UPGRADE to one of the following:
• For only SLA Mon upgrade, 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</td></tr>
<tr><td>#ADS [4.0] components SAL and SLAMon are already
installed Do you wish to Upgrade SAL and SLAMon.
(y/n)
ADS_SAL_SLAMON_UPGRADE=y</td><td>When you have Avaya Diagnostic Server 4.0 with both components on the host, set the value of ADS_SAL_SLAMON_UPGRADE as y to upgrade to Avaya Diagnostic Server 4.1
<b>Note:</b>
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 Diagnostic Server 4.1. 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 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.
<b>Important:</b>
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 <b>sudo</b> 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 <i>Avaya Diagnostic Server Additional Security Configuration Guidance</i> available at http://support.avaya.com.</td></tr>
</table>

Table continues…

Information in the file	Description

`#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`
	To agree to the security implication of having both components coresident, set the value as `y`. If you keep the value as `n`, the installer quits the installation process.

Set the following properties to continue with an upgrade 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 the minimum requirements completely. You cannot install a new component on a server that does not meet the minimum requirements.	

`#ADS [4.0] 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 4.1 is installed with both components.
	To continue with the upgrade even if the host does not meet one or more minimum hardware requirements, including free 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.

Table continues…

Information in the file	Description

`#ADS [4.0] 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 4.1 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 [4.0] 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 4.1 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.

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 free disk space does not meet the recommended requirement.	

`#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 value but greater than the minimum requirement.
	• `ADS_SLAMON_PROCEED_ON_RAM_CHECK_FAIL=n`: To quit the installation if RAM is less than the recommended value.

Table continues…

Information in the file	Description

#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 value but greater than the minimum requirement.
	• 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 value but greater than the minimum requirement.
	• ADS_SAL_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 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 value but greater than the minimum requirement.
	• ADS_SAL_PROCEED_ON_RAM_CHECK_FAIL=n: To quit the installation if RAM is less than the recommended value.

Table continues…

Information in the file	Description

`# 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 value but greater than the minimum requirement.
	• `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 value but greater than the minimum requirement.
	• `ADS_PROCEED_ON_RAM_CHECK_FAIL=n`: To quit the installation if RAM is less than the recommended value.

`#Any local Path of Backup file to be used for migration`
`BACKUP_FILE_PATH=`
	To install a new instance of Avaya Diagnostic Server using the data that is backed up from another instance of Avaya Diagnostic Server, enter the absolute path of the backup file to be used as the value of this property.
	This option facilitates migration from an earlier version of Avaya Diagnostic Server to a new host server.

The following are responses that the installer uses to register remote worker agent during the installation of SLA Mon server component. If you choose to install the Avaya Diagnostic Server with SAL Gateway only, keep the default values.	

`#If following value is true then remote worker agents will register to SLAMon NATTed IP (y/n)`
`SLAMonIPcheck=n`
 	
`#public IP address of SLAMon server to register remote worker agents`
`SLAMonNATTedIP=0.0.0.0`
	Keep the default value `y`.

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.	

Table continues…

Information in the file	Description

`#Importing SLAMon public key into RPM database`
`(y/n)`
`IMPORTKEY=y`
	Keep the default value `y`.

`#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`.

`#SLAMON 3.0 employs enhanced ASG (EASG)`
`authentication, which is a PKI-enhanced version of`
`the dynamic authentication method used in previous`
`releases of SLAMON.`
`#EASG allows Avaya support tools and personnel`
`to authenticate with SLAMON when responding to`
`service requests.`
`#If EASG is not enabled(n), remote support from`
`Avaya automated tools and support personnel will`
`be blocked or impeded.`
`EASGYESNO=y`
	To enable Avaya support tools and personnel to access the SLA Mon component through enhanced Access Security Gateway (EASG) authentication, ensure that the value of `EASGYESNO` is `y`.
	
	If the value is `n`, remote support of SLA Mon from Avaya automated tools and support personnel will be blocked or impeded.

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.

Table continues…

Information in the file	Description

`#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.
	Note:
	From ADS 3.2 release onwards, ADS does not support Services-VM method of deployment.
	If SAL Gateway detects Servies-VM while trying to install to ADS , system displays the following error:
	`Services-VM deployment detected, cannot install or upgrade the software on SVM setup. Exiting installer.`

`# If following values are true then Gateway Installer update the IPTABLE and SYSLOG`
`# For RHEL 7.x/8.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`
`# $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 might not write log records in syslog after the installation.
	Note:
	Complete the syslog configuration as stated in Chapter 5, Post-installation configuration.

Table continues…

Information in the file	Description

`#Automatic Software Update Configuration. To enable the feature, provide "ON"/"OFF" mandatory field`
`AUTOUPGRADE_CUST_SELECT=ON`
	To enable the Automatic Software Update feature, keep the default value, `ON`. To disable the Automatic Software Update feature, change the value to `OFF`.
	When the feature is enabled, software updates including major, minor and service pack releases are downloaded to SAL Gateway automatically. If you do not install the downloaded software packages within the grace period set for them, the packages are installed automatically.
	When the feature is disabled, 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.

Table continues…

Information in the file	Description

`#SMTP Configuration fields please provide valid details mandatory fields`
`SMTP_HOST=`
`SMTP_PORT=`
`SMTP_ADMIN_EMAIL=`
`#SMTP_ENCRYPTION_METHOD default value is NONE and does not support encryption. If encryption is used it can be either STARTTLS or SSLTLS`
`SMTP_ENCRYPTION_METHOD=NONE`
`#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=`
`#password will be removed and not be stored in the file after installation.`
`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.
	• `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.
	• `SMTP_ENCRYPTION_METHOD`: The encryption method used for the SMTP sever.
	The following SMTP properties are optional:
	• `SMTP_USER_NAME`: The name of the user to be authenticated. Enter a value only when 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_PASSWORD`becomes a mandatory field. The `SMTP_PASSWORD` will be deleted from `ADS_Response.properties` file after Installation.
	• `SMTP_SECONDARY_EMAIL`: A secondary email address where you want to receive email notifications.

Table continues…

Information in the file	Description

`# 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=`
	You can replace the default values of `GATEWAY_SOLUTION_ELEMENTID` and `SPIRIT_ALARMID` with the actual IDs that you received from Avaya at SAL Gateway registration. Else, you can install SAL Gateway with the default IDs.
	For the procedure to obtain these IDs from Avaya, see the Registering SAL Gateway section.
	When you install SAL Gateway with the default IDs, you must do one of the following after the installation:
	• Through the SAL Gateway user interface, generate the Solution Element ID and Product ID automatically.
	• If you already have the IDs, configure those ID on the SAL Gateway user interface.
	Unless you configure the correct IDs, the SAL Gateway services, except the UI service, do not start.
	You need not enter a value for `AGENTGATEWAY_IPADRESS`. The installer automatically discovers the actual IP address of the host server.

`# Select the USER_ACCOUNT and USER_GROUP of Agent Gateway mandatory fields`
`AGENTGATEWAY_USERNAME=saluser`
`AGENTGATEWAY_USERGROUP=salgroup`
	For the SAL 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.

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 proxy server is optional and depends on your local network configuration. If you use a proxy server for Internet access outside the firewall of the customer network, you might require to configure the proxy server for SAL Gateway as well.
	To use a proxy server, you can make the following changes:
	• 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.
	Note:
	The `CUSTOMER_PROXY_PASSWORD` will be deleted from `ADS_Response.properties` file after Installation.

Table continues…

Information in the file	Description

`# 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. To choose the OFFLINE mode, ensure that the first two properties in this section are commented out but `MODEL_RADIO_SELECTION=OFFLINE` is not commented out.
	Note:
	The ONLINE and OFFLINE values must be in upper case.

Table continues…

Information in the file	Description

`#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.
	Note:
	You can download the model package from the global URL of the Enterprise server, for example, https://secure.alarming.avaya.com/repository/. You can locate the default model 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-4.1.0.0-751/models`.

`# Policy Manager Configuration Optional fields`
`POLICY_MANAGER_HOSTNAME=`
`POLICY_MANAGER_PORT=`
	You can configure SAL Gateway to use SAL Policy Manager with SSH Proxy for governing remote access requests. You can configure the properties as the following:
	• `POLICY_MANAGER_HOSTNAME`: The FQDN of the Policy Manager host.
	• `POLICY_MANAGER_PORT`: The port number that Policy Manager uses for incoming communications from SAL Gateway.
	If you do not have SAL Policy Manager installed on the network, 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.

Table continues…

Information in the file	Description

`# 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 user interface. You can set one of the following values:
	• `Administrator`: Full permissions to all pages of the unser interface, except a few. Administrator have read-only access to Policy Manager, PKI Configuration, OCSP/CRL Configuration, and Certificate Management pages.
	• `Browse`: Ready-only access to the pages of the user interface.

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

Note:

While SAL Gateway supports both IPv4 and IPv6, the SLA Mon server works only on IPv4. If you plan to install Avaya Diagnostic Server with SLA Mon, configure the host for IPv4.

Related links

Installing Avaya Diagnostic Server in the unattended mode on page 65

Chapter 5: Postinstallation configuration

Postinstallation configuration for SAL Gateway

Updating iptables for SAL Gateway

About this task

For SAL Gateway to function properly, you must update the iptables rules. During the installation, you can select the option for the installer to make the required changes to the iptables rules automatically. If you did not select this option, use this procedure to update the iptables after the installation.

Procedure

1. Log on to the SAL Gateway host as the root user.
2. To update the firewall rules for IPv4, run the following commands:

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

3. To save the iptables configuration, run one of the following commands:
   - On an RHEL 7.x/8.x system:

     ```
     iptables-save
     ```

4. To restart the iptables service, run one of the following commands:
   - On an RHEL 7.x/8.x system:

     ```
     systemctl restart iptables
     ```

5. To check and ensure that the rules are updated, run one of the following commands:
   - On an RHEL 7.x/8.x system:

     ```
     systemctl status iptables
     ```

The following is a snapshot of the sample output containing the updated rules:

```
...
 ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0            state 
RELATED,ESTABLISHED
 ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:7443
 ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0            udp dpt:162
 ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:5107
 ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:5108
...
```

6. To update the firewall rules for IPv6, run the following commands:

   ```
   ip6tables -I INPUT -i lo -j ACCEPT
   ```

   ```
   ip6tables -I INPUT -p tcp -m tcp --dport 5108 -j ACCEPT
   ```

   ```
   ip6tables -I INPUT -p tcp -m tcp --dport 5107 -j ACCEPT
   ```

   ```
   ip6tables -I INPUT -p udp -m udp --dport 162 -j ACCEPT
   ```

   ```
   ip6tables -I INPUT -p tcp -m tcp --dport 7443 -j ACCEPT
   ```

   ```
   ip6tables -I INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
   ```

7. To save the ip6tables configuration, run the following command:

   ```
   service ip6tables save
   ```

8. To restart the ip6tables service, run one of the following commands:

   - On an RHEL 7.x/8.x system:

     ```
     systemctl restart ip6tables
     ```

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. To configure the IPv4 rules for remote administration of SAL Gateway, run the following commands:

   ```
   iptables -I INPUT -p icmp -m icmp --icmp-type any -j ACCEPT
   ```

   ```
   iptables -I INPUT -p tcp -m tcp --dport 22 -j ACCEPT
   ```

3. To save the iptables configuration, run one of the following commands:

   - On an RHEL 7.x/8.x system:

     ```
     iptables-save
     ```

4. To restart the iptables service, run one of the following commands:
   - On an RHEL 7.x/8.x system:

     ```
     systemctl restart iptables
     ```
5. To check and ensure that the rules are updated, run one of the following commands:
   - On an RHEL 7.x/8.x system:

     ```
     systemctl status iptables
     ```

   The following is a snapshot of the sample output containing the updated rules:

   ```
   ...
    ACCEPT     tcp  --  0.0.0.0/0              0.0.0.0/0             tcp dpt:22
    ACCEPT     icmp --  0.0.0.0/0              0.0.0.0/0             icmp type 255
   ...
   ```
6. To configure the IPv6 rules for remote administration of SAL Gateway, run the following commands:

   ```
   ip6tables -I INPUT -p ipv6-icmp -j ACCEPT
   ```

   ```
   ip6tables -I INPUT -p tcp -m tcp --dport 22 -j ACCEPT
   ```
7. To save the ip6tables configuration, run the following command:

   ```
   service ip6tables save
   ```
8. To restart the ip6tables service, run one of the following commands:
   - On an RHEL 7.x/8.x system:

     ```
     systemctl restart ip6tables
     ```

Editing the syslog configuration file for SAL Gateway

About this task

To use syslog to store log messages from SAL Gateway, you must update the `/etc/rsyslog.conf` file. During the installation, you can allow the installer to make the required changes in the syslog configuration file automatically. If the installer did not enable syslog during installation, use this procedure to configure syslog to store log message in the appropriate files.

Use this procedure to enable SAL Gateway to use syslog locally.

Procedure

1. Log on to the SAL Gateway host as the root user.
2. Open the `/etc/rsyslog.d/salsyslog.conf` file in a text editor.

   Note:

   Create a new file, if an existing file is not available.
3. Verify whether the file contains the following entries:

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

4. If the file does not contain the mentioned lines, add the lines to the file.
5. To enable SAL Gateway syslog on the local server, open the /etc/rsyslog.conf file. Ensure that the following lines are present in the file and are uncommented, that is, no pound (#) sign remains at the start of the lines:

   ```
   $ModLoad imudp
   $UDPServerRun 514
   $IncludeConfig /etc/rsyslog.d/*.conf
   ```

   Note:

   If any of these lines are missing, add the lines and update the file.

6. Save and close the file.
7. Restart the rsyslog service using the appropriate command from the following:
   - On an RHEL 7.x and 8.x system:

     ```
     systemctl restart rsyslog
     ```

Configuring the local syslog server for SAL Gateway

About this task

Use this procedure to configure the local syslog server, that stores the log messages from SAL Gateway, to send the logs to a remote syslog server.

Procedure

1. Log on to the SAL Gateway host as a root user.
2. Open the `/etc/rsyslog.conf` file in a text editor.
3. Add the following entry at the end of the last line:

   ```
   *.* @@<remote-host>:514
   ```

   Where, <remote-host> is the hostname or IP address of the remote syslog server.

   Use a single @, if you want the syslog server to use UDP for remote sysloging.

   Use double @, if you want the syslog server to use TCP for remote sysloging.

4. Save and close the file.
5. Restart the rsyslog service using the appropriate command from the following:
   - On an RHEL 7.x/8.x system:

     ```
     systemctl restart rsyslog
     ```

Uploading the SAL Policy Manager certificate to SAL Gateway

About this task

To establish communication between SAL Policy Manager and SAL Gateway, the server certificate of SAL Policy Manager must be present in the truststore of SAL Gateway. If you configured SAL Policy Manager details on SAL Gateway during installation, use this procedure to add the server certificate of Policy Manager to SAL Gateway.

Before you begin

Export the server certificate from SAL Policy Manager, and copy it to the system from where you will access SAL Gateway. For more information about exporting the server certificate from Policy Manager, see *Deploying SAL Policy Manager with SSH Proxy*.

Procedure

1. Log on to the SAL Gateway user interface.
2. On the main menu of the SAL Gateway user interface, click **Security** > **Certificate Management**.
3. On the Certificate Management page, click **Upload**.
4. Click **Browse** to locate and select the certificate.
5. Click **Upload**.

   The system uploads the certificate to the truststore of SAL Gateway.
6. Restart the SAL services to apply the new certificate.

   Note:

   After restarting SAL Gateway, the system displays an error message if the configured Policy Manager is incompatible with SAL Gateway.

   Ensure that you have configured SAL Policy Manager version 4.0 or later.

Importing client certificate

Before you begin

Ensure that you have the client server IP address and port details.

Procedure

1. On the main menu of the SAL Gateway user interface, click **Security** > **Import Client Certificate**.
2. On the Import Client Certificate page, enter the **IP address** and **Port**.
3. Click **Connect**.

   The system connects to the client server and displays the `URL` and certificate `Details`.
4. Verify if the displayed certificate details are correct and can be trusted by the SAL Gateway.
5. Click **Import** to import the client certificate.
6. Click **Yes** to complete the process.

Next steps

Restart the SAL services to apply the new certificates.

Postinstallation 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/TLS protocol configuration for SLA Mon Server

SSL/TLS protocol for the SLA Mon server

The SSL/TLS protocol that the SLA Mon server supports are TLSv1, TLSv1.1, TLSv1.2. The following are the ciphers that the SLA Mon server uses:

```
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA
```

Changing the SSL/TLS protocol and ciphers for the SLA Mon user interface

About this task

Use this procedure to modify the SSL/TLS protocol and ciphers that the SLA Mon server uses for the interaction between the web browser of a user and the SLA Mon user interface.

Procedure

1. Log on to the Linux host server with root privileges.

2. To change the ciphers for the key server, add the following property to the `/var/eqm_data/autoStart.properties` file:

   `keyserver.enabled-ciphers=`*<comma delimited ciphers>*

3. To change the SSL/TLS protocol for the key server, add the following property to the `/var/eqm_data/autoStart.properties` file:

   `keyserver.enabled-ssl-protocols=`*<comma delimited protocols>*

4. To change the ciphers or the protocol for the user interface, open the `/opt/avaya/slamon/tomcat/conf/server.xml` file, and edit the connector for SLA Mon, as shown in the following:

   ```
   <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"
   keyAlias="slamon"
   keystorePass=<removed>
   keystoreFile="/opt/avaya/slamon/misc/slamon-ui-keystore.jks"
   truststorePass=<removed>
   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_CB
   C_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,SSL_RSA_WITH_3DES_EDE_CBC_SHA,SSL_DHE_DSS_WITH_
   3DES_EDE_CBC_SHA"
   />
   ```

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

Managing SSL/TLS certificates of the SLA Mon server UI

Replacing the SSL/TLS certificate of the SLA Mon server user interface

About this task

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

You can also import any client/web browser SSL/TLS certificates to the keystore for the SLA Mon server user interface. If you use such a certificate, you need not regenerate a self-signed certificate. If no client/web browser SSL/TLS certificates are available, use this procedure to use self-signed certificates for the SLA Mon user interface.

Note:

This procedure is for the interaction between the web 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 Linux host as the root user.
2. Run one of the following commands to stop the SLA Mon UI service:
    - On an RHEL 7.x/8.x system:

      ```
      systemctl stop slamonweb
      ```
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>
    ```

    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. **(Optional)** 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 self-signed certificate or the certificate chain signed by a signing authority from a well-known CA, such as VeriSign®, or your in-house CA in response to the CSR:

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

   Ensure that the *<keystore_password>* value you provide for `keypass` and `storepass` is the same as that you used in Step 4.

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 one of the following commands to start the SLA Mon UI service:

   - On an RHEL 7.x/8.x system:

     ```
     systemctl start slamonweb
     ```

Adding an SSL/TLS certificate to the truststore of the SLA Mon server user interface

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 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 one of the following commands to stop the SLA Mon web service:

   - On an RHEL 7.x/8.x system:

     ```
     systemctl stop slamonweb
     ```

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 keystore of the SLA Mon server user interface.

4. Run one of the following commands to restart the web service:
   - On an RHEL 7.x/8.x system:

     `systemctl start slamonweb`

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 the syslog configuration file for SLA Mon

About this task

Use this procedure to configure syslog to store the log messages from the SLA Mon server in the appropriate files.

If you selected not to configure the syslog files at the time of the SLA Mon server installation, you can edit the `/etc/rsyslog.conf` file later to enable logging through syslog.

Procedure

1. Log on to the SLA Mon host as the root user.
2. Open the `/etc/rsyslog.conf` file in a text editor, 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.

3. If the file does not contain the mentioned lines, add the lines to the file.
4. To enable remote logging, ensure that the following lines are present in the file and are uncommented, that is, no pound sign (#) remains at the start of the lines:

   ```
   $ModLoad imudp
   $UDPServerRun 514
   ```

5. Restart the rsyslog service using the appropriate command from the following:
   - On an RHEL 7.x/8.x system:

```
systemctl restart rsyslog
```

Configuring the local syslog server for SLA Mon

About this task

Use this procedure to configure the local syslog server, that stores the log messages from SLA Mon server, to send the logs to a remote syslog server.

Procedure

1. Log on to the SAL Gateway host as a root user.
2. Open the `/etc/rsyslog.conf` file in a text editor.
3. Add the following entry at the end of the last line:

   ```
   *.* @@<remote-host>:514
   ```

   Where, <remote-host> is the hostname or IP address of the remote syslog server.

   Use a single @, if you want the syslog server to use UDP for remote sysloging.

   Use double @, if you want the syslog server to use TCP for remote sysloging.
4. Save and close the file.
5. Restart the rsyslog service using the appropriate command from the following:
   - On an RHEL 7.x/8.x system:

     ```
     systemctl restart rsyslog
     ```

Updating iptables for SLA Mon

About this task

During the SLA Mon server installation, you can select the option for the installer to make the required changes to the iptables rules automatically. If you did not choose this option, use this postinstallation 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 host as root.
2. Run the following commands to update the iptables rules 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. **(Optional)** If you want to enable Remote Worker agent, run the following commands to open the port to communicate with SLA Mon server:

   `/sbin/iptables -A INPUT -p tcp -m tcp --dport 50016 -j ACCEPT` for a Remote Worker phone to reach out to and register with SLA Mon server.

   `/sbin/iptables -A INPUT -p tcp -m tcp --dport 50010 -j ACCEPT` to receive all the event monitoring logs from Remote Worker phone.

   `/sbin/iptables -A INPUT -p tcp -m tcp --dport 50009 -j ACCEPT` to receive all the packet capture session details from Remote Worker phone.

   ```
   /sbin/iptables -A INPUT -p tcp -s localhost --dport 4510 -j ACCEPT
   ```

   ```
   /sbin/iptables -A INPUT -p tcp --dport 4510 -j DROP
   ```

5. Run one of the following commands to save the iptables configuration:

   - On an RHEL 7.x/8.x system:

     ```
     iptables-save
     ```

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

   - On an RHEL 7.x/8.x system:

     ```
     systemctl restart iptables
     ```

   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. On the main menu of the SAL Gateway user interface, click **Devices** > **View/Search**.
4. On the Managed Element page, click **Add New**.

   System displays Managed Element Configuration pop-up window.

5. On the Managed Element Configuration window, in the **Solution Element ID or CI Name** field, type the Solution Element ID of the device that you want to add as a managed element. If you want to add a new third party device, type the CI name.

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

Note:

When you register a device using GRT for support through SAL, the details of the device become available to the SAL Gateway instances present in your network. When you enter a Solution Element ID for which the device information is available to SAL Gateway, SAL Gateway automatically populates additional information, such as SAL model, product type, and product ID, in the respective fields.

6. Perform the following to select the applicable model for the product:
    a. In the **Model** field, click the model that is applicable to the product.

       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. **(Optional)** To view the applicable products under a selected model, click **Show model applicability**.

       The applicable products of the selected model are displayed in a new window.

    c. In the **Product** field, click an appropriate option from the list of supported product versions.
7. 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.
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. To provide Avaya the ability to connect to the managed element remotely, select the **Provide remote access to this device** check box.
11. To enable alarm transfer from the managed element through SAL Gateway, select the **Transport alarms from this device** check box.

    If the model you select does not support alarm transfer, the **Transport alarms from this device** check box is unavailable for selection.
12. Click **Add**.

Next steps

For the configuration changes to take effect immediately, restart the SAL Gateway services through the Apply Configuration Changes page. However, this is optional because the services are restarted automatically at a scheduled time.

Important:

Restarting the SAL Gateway services might terminate established connections and might result in SNMP traps being missed.

Related links

SLA Mon and WebLM models are not present when adding as managed elements to SAL Gateway on page 152

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.

You can also manage the SLA Mon server license from System Manager UI. Click the System Manager link available in the licensing section of the SLA Mon UI to log in to System Manager.

Note:

- The System Manager link is redirected to System Manager login page. If the system displays a blank page or an error, refresh the screen to go to the login page.
- 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:

- ADS 4.1 release onwards, SLA Mon does not support local installation of the WebLM licensing server. It is recommended to use a third party server instead.

- 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 PLDSto 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. Select the **Accept the License Terms & Conditions** option to accept the terms and conditions.
11. 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:

   - On an RHEL 7.x/8.x system: `systemctl start slamonsrvr`

   > **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.

- Post Avaya Diagnostic Server 4.1 installation, the WebLM server certificate gets imported to the truststore, if the WebLM IP address has changed. So the user has to wait for 15 seconds for the process to complete.

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:

   - On an RHEL 7.x/8.x system: `systemctl start slamonweb`

   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
   ```

Note:

Post Avaya Diagnostic Server 4.1 installation, if the WebLM IP address has changed, the WebLM server certificate gets imported to the truststore. So the user has to wait for 15 seconds for the process to complete.

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.

Support for Enhanced Access Security Gateway

SLA Mon supports privileged access by Avaya Services to the host server through Enhanced Access Security Gateway (EASG). EASG ensures that Avaya support tools and personnel can securely access customer systems to provide remote support. EASG is a certificate-based authentication and authorization solution that uses a challenge and response protocol to validate the user and to reduce unauthorized access. An EASG user uses a predetermined user ID to provide service at the customer site. EASG challenges this user ID, and the user must provide a proper response to log in successfully. The EASG user can use the response to a challenge only one time.

You can choose to enable or disable EASG at the time of installing the SLA Mon server. Later, you can use the CLI of the SLA Mon server to enable or disable EASG according to your requirement.

Salient points of access through EASG to the SLA Mon server

- Avaya Services privileged access through EASG opens the host server to shared logins through the CLI of the operating system. EASG supports only Avaya Services logins, including init, inads, and craft. Through these shared logins, 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.
- EASG users can perform the following:
    - Run operations, such as start, stop, restart, and status check, on the SLA Mon services. For example:

      `systemctl status slamonsrvr.service` (On an RHEL 7.x/8.x host)
- EASG 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.

Related links

Enabling or disabling EASG through the CLI interface on page 103

Enabling or disabling EASG through the CLI interface

About this task

Use this procedure to enable or disable EASG for the SLA Mon server. Enable EASG only if you want Avaya Services access for the SLA Mon server.

By enabling Avaya Services Logins, you are granting Avaya access to your system. This is required to maximize the performance and value of your Avaya support entitlements, allowing Avaya to resolve product issues in a timely manner. The product must be registered using the Avaya Global Registration Tool (GRT) at https://grt.avaya.com to be eligible for Avaya remote connectivity. See the Avaya support site at https://support.avaya.com/registration for additional information for registering products and establishing remote access and alarming.

By disabling Avaya Services Logins, you are denying Avaya access to your system. This is not recommended, as it can impact Avaya's ability to provide support for the product. Unless the customer is well versed in managing the product themselves, Avaya Services Logins should not be disabled.

Procedure

1. Log on to the host server CLI as an administrator user.
2. To check the status of EASG, run the following command:

   ```
   EASGStatus
   ```

3. Do one of the following:
   - To enable EASG and accept the terms, run the following command:

     ```
     EASGManage --enableEASG
     ```

   - To disable EASG and accept the terms, run the following command:

     ```
     EASGManage --disableEASG
     ```

Related links

Support for Enhanced Access Security Gateway on page 102

Chapter 6: Verifying the 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 and processes are running properly.

Testing the alarming service of SAL Gateway

About this task

Use this procedure to verify that the alarm transfer and remote access processes of SAL Gateway is running properly. SAL Gateway uses the spiritAgent service to handle alarm transfer and remote access. After a successful installation, this service should be in the running state.

Procedure

1. Log on to the host server as root.
2. Run one of the following commands, and check the outcome of the command:
   - On RHEL 7.x/8.x

     ```
     systemctl status spiritAgent.service
     ```
3. If the service is not running, run one of the following commands to start the service:
   - On RHEL 7.x/8.x:

     ```
     systemctl start spiritAgent.service
     ```
4. Check the status again to verify that the service is running.

Testing SAL Gateway Managed Services

About this task

Use this procedure to verify if the Managed Services are configured on SAL Gateway.

Procedure

1. Log on to the host server with root user credentials.
2. Run one of the following commands, and check the outcome of the command:
   - On RHEL 7.x/8.x

     ```
     systemctl status openvpnAgent.service
     ```

3. If the service is not running, run one of the following commands to start the service:
   - On RHEL 7.x/8.x:

     `systemctl start openvpnAgent.service`
4. Run the following command to restart the spirit agent services:
   - On RHEL 7.x/8.x:

     `systemctl start spiritAgent.service`
5. Check the status again to verify that the service is running.

Testing the SAL Watchdog process

About this task

The SAL Watchdog process 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 process 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:

   ```
   cat /var/log/cron
   ```

   Example output of the command:

   ```
   Jan 27 11:25:01 linpubm206 CROND[2816]: (saluser) CMD (/opt/avaya/SAL/gateway/
   SALWatchdog/scripts/SALWatchdog)
   Jan 27 11:30:01 linpubm206 CROND[3452]: (root) CMD (/usr/lib64/sa/sa1 1 1)
   Jan 27 11:30:01 linpubm206 CROND[3453]: (saluser) CMD (/opt/avaya/SAL/gateway/
   SALWatchdog/scripts/SALWatchdog)
   ```
3. Check when the cron job was run the last time.

   If SALWatchdog was run in the last 5 minutes, you can consider that the process is running properly.

Testing the SAL Gateway user interface service

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 one of the following commands to check the status of the gatewayUI service:
        - On RHEL 7.x/8.x:

          ```
          systemctl status gatewayUI.service
          ```
    c. If the service is not running, run one of the following commands to start the service:
        - On RHEL 7.x/8.x:

          ```
          systemctl start gatewayUI.service
          ```
    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 one of the following commands, and check the outcome of the command:
    - On an RHEL 7.x/8.x system:

      ```
      systemctl status slamonsrvr
      ```

   Expected output sample:

```
SLAMon Server Running (<Process ID>)
```

3. If the service is not running, run one of the following commands to start the service:
   - On an RHEL 7.x/8.x system:

     ```
     systemctl start slamonsrvr
     ```

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 one of the following commands, and check the outcome of the command:
   - On an RHEL 7.x/8.x system:

     ```
     systemctl status slamonweb
     ```

   Expected output sample:

   ```
   Avaya Diagnostic Server Slamon web 3.2 is running (<process id>)
   ```
3. If the service is not running, run one of the following commands to start the service:
   - On an RHEL 7.x/8.x system:

     ```
     systemctl start slamonweb
     ```

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 one of the following commands, and check the outcome of the command:
   - On an RHEL 7.x/8.x system:

     ```
     systemctl status slamondb
     ```

   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 one of the following commands to start the service:
   - On an RHEL 7.x/8.x system:

     ```
     systemctl start slamondb
     ```

Chapter 7: Upgrading Avaya Diagnostic Server

Upgrade paths to Avaya Diagnostic Server 4.1

The Avaya Diagnostic Server 4.1 installer supports a direct upgrade capability from Avaya Diagnostic Server 4.0. For Avaya Diagnostic Server and SAL Gateway releases that do not support a direct upgrade, you must upgrade to 4.0 release of Avaya Diagnostic Server that supports direct upgrade by using the following upgrade path:

Product release	Upgrade path
SAL Gateway 3.3 or earlier	Upgrade to Avaya Diagnostic Server 4.0, then upgrade to Avaya Diagnostic Server 4.1.
SAL Gateway 4.0	Supports direct upgrade to Avaya Diagnostic Server 4.1.

Note:

Some earlier versions of Avaya Diagnostic Server and SAL Gateway do not support direct upgrade because of hardware limitations and unsupported version of the Operating System.

Checklist for upgrading from Avaya Diagnostic Server 4.0 to 4.1

The following checklist provides the high-level steps to upgrade from Avaya Diagnostic Server Release 4.0 to Release 4.1.

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 for Avaya Diagnostic Server 4.1.	See Hardware and software requirements on page 30.	You can choose to upgrade to Avaya Diagnostic Server 4.1 even when the host does not meet the minimum hardware requirements. However, the host must meet a bare-minimum free disk space requirement. See Minimum hardware requirements for upgrade on page 110.	
3	Ensure that the operating system version installed on the host supports upgrade to Avaya Diagnostic Server.	See Supported operating system and Java versions for upgrade on page 110.		
4	Download the Avaya Diagnostic Server 4.1 software package from PLDS, and extract the files to a local directory on the host server.	See Downloading software from PLDS on page 42 and Extracting the Avaya Diagnostic Server software files to a local directory on page 44.		
5	Upgrade to Avaya Diagnostic Server 4.1.	See Upgrading Avaya Diagnostic Server in the attended mode on page 111 or Upgrading Avaya Diagnostic Server in the unattended mode on page 114.	**Note:** Before upgrading to Avaya Diagnostic Server 4.1, ensure that your existing password does not include the following unsupported characters: # % ^ & + ` { } | \. If your existing password includes these characters, then make sure to change the password to exclude the unsupported characters.	
6	Validate that the upgrade operation is successful.	See Upgrade verification checklist on page 116.		

Minimum hardware requirements for upgrade

The minimum hardware requirements to upgrade to Avaya Diagnostic Server 4.1 are the same as the requirements for a clean installation of Avaya Diagnostic Server 4.1. If the upgrade operation involves upgrade of the existing component and installation of a new component, then the host server must meet the minimum hardware requirements for co-hosted components. For information about the hardware requirements, see Chapter 3, Planning and initial setup.

However, you can upgrade Avaya Diagnostic Server even without the minimum hardware requirements when the host meets a bare-minimum free disk space requirement as mentioned in the following table.

Important:

You cannot install a new component during an upgrade on a host that meets just the bare minimum free space requirement. Avaya provides you this option so that you can upgrade from an earlier version of 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 to the full capacity.

Only SAL Gateway	1024 MB of free disk space
Only SLA Mon server	2048 MB of free disk space: • 1024 MB in `/opt` • 1024 MB in `/var/lib/`
Cohosted components	3072 MB of free disk space: • 2048 MB in `/opt` • 1024 MB in `/var/lib/`

Supported operating system and Java versions for upgrade

See the following table to identify whether an upgrade to Avaya Diagnostic Server 4.1 is possible with the existing software versions installed on the host system.

Supported Java versions	Supported operating systems
OpenJDK JRE 8	RHEL 7.x/RHEL 8.x

Note:

- Avaya Diagnostic Server 4.1 does not support JRE 1.7 (Java 1.7). To install or upgrade to Avaya Diagnostic Server 4.1, ensure that you have upgraded JRE 1.7 (Java 1.7) to JRE 1.8 (Java 1.8).

After upgrading from JRE 1.7 (Java 1.7) to JRE 1.8 (Java 1.8), immediately upgrade SAL Gateway to 4.1. Upgrading the JRE disables the watchdog, so an immediate upgrade to 4.0 requires you to re-enable the watchdog.

Upgrading Avaya Diagnostic Server in the attended mode

About this task

Use this procedure to upgrade to Avaya Diagnostic Server Release 4.1 in the attended mode from Avaya Diagnostic Server Release 4.0. You must log on to the RHEL server through KVM or a virtual console in graphical user interface (GUI) mode to run the installer in the attended mode.

Important:

If the SAL Gateway component of the existing Avaya Diagnostic Server release is pointing to non-Avaya SAL Core Server or Remote Server, upgrade is not possible.

Before you begin

- Verify if Avaya Diagnostic Server release 4.1 installer file is already available in the following locations:
  - If auto upgrade is attempted, then installer file gets extracted in `d`
  - If auto upgrade is not attempted, extract the `opt/avaya/ads/Upgrade/packages/INSTALLER/ADS-MAJOR-4.1.0/ADS-MAJOR-4.1.0.tar.gz` installer file.
- If the Avaya Diagnostic Server Release 4.1 installer file is not available, download the Avaya Diagnostic Server software file. Copy and extract the `ADS-Installer-`*`<version_no>`*`-`*`<build_no>`*`.tar.gz` file to a directory on the host server.
- Ensure that the host server meets the minimum hardware requirements.
- Ensure that the operating system and Java versions installed support upgrade.
- Ensure that the host server meets all other system requirements mentioned in Chapter 3, Planning and initial setup.

Note:

Before upgrading to Avaya Diagnostic Server 4.1, ensure that your existing password does not include the following unsupported characters: # % ^ & + ` { } | \. If your existing password includes these characters, then make sure to change the password to exclude the unsupported characters.

Procedure

1. Log on to the host server through KVM or a virtual console in graphical user interface (GUI) mode 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 have 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:

   - If Avaya Diagnostic Server 4.0 is available with the SAL Gateway component, type one of the following options:
     - `1`: To upgrade to Avaya Diagnostic Server 4.1 with only the SAL Gateway component.
     - `2`: To upgrade to Avaya Diagnostic Server 4.1 with SAL Gateway and to install the SLA Mon component.
   - If Avaya Diagnostic Server 4.0 is available with the SLA Mon component, type one of the following options:
     - `1`: To upgrade to Avaya Diagnostic Server 4.0 with only the SLA Mon component.
     - `2`: To upgrade to Avaya Diagnostic Server 4.0 with SLA Mon and to install the SAL Gateway components.
   - If you want to register a remote worker agent on SLA Mon server, type `y` when the installer prompts you to configure the SLAMon server NATTed public IP address.
   - If Avaya Diagnostic Server 4.0 is available with both components, type `y` when the installer prompts you to upgrade to Avaya Diagnostic Server 4.0 with both components.
   - If Avaya Diagnostic Server 4.0 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.

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 113
Completing the SLA Mon server upgrade on page 114
Completing the SLA Mon server installation on page 63

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:

- From ADS 3.2 release onwards, ADS does not support Services-VM method of deployment.

  If SAL Gateway detects Services-VM while trying to install to ADS 4.1 , system displays the following error:

  ```
  Services-VM deployment detected, cannot install or upgrade the
  software on SVM setup. Exiting installer.
  ```

- You can upgrade the redundant SAL Gateway instances one by one without affecting the redundancy configuration. After both SAL Gateway instances are upgraded 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 Gateway instances 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**.
3. 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

Upgrade verification checklist on page 116

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.

Important:

If the SAL Gateway component of the existing Avaya Diagnostic Server release is pointing to non-Avaya SAL Core Server or Remote Server, upgrade is not possible.

Before you begin

- Verify if Avaya Diagnostic Server release 4.1 installer file is already available in the following locations:
  - If auto upgrade is attempted, then installer file gets extracted in `/opt/avaya/ads/Upgrade/packages/INSTALLER/ADS-MINOR-4.1.0/installer/ADS-Installer-4.1.0.0-898`
  - If auto upgrade is not attempted, extract the `opt/avaya/ads/Upgrade/packages/INSTALLER/ADS-MAJOR-4.1.0/ADS-MAJOR-4.1.0.tar.gz` installer file.
- If the Avaya Diagnostic Server release 4.1 installer file is not available, download the Avaya Diagnostic Server software file. Copy and extract the `ADS-Installer-`*`<version_no>`*`-`*`<build_no>`*`.tar.gz` file to a directory on the host server.
- Ensure that the host server meets the minimum hardware requirements.
- Ensure that the operating system and Java versions installed support upgrade.
- Ensure that the host server meets all other system requirements mentioned in Chapter 3, Planning and initial setup.

  Note:

  Before upgrading to Avaya Diagnostic Server 4.1, ensure that your existing password does not include the following unsupported characters: # % ^ & + ` { } | \. If your existing password includes these characters, then make sure to change the password to exclude the unsupported characters.
- Ensure that you have updated the response file, `/`*`<folder_path_to_extracted package>`*`/ADS-Installer-`*`<version_no>`*`-`*`<build_no>`*`/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.
  - For configuring a remote worker agent, ensure that the value for `SLAMonIPcheck` property is `y` and you have entered the correct IP address in `SLAMonNATTedIP=0.0.0.0` field.

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 have 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 66
Upgrade verification checklist on page 116

Upgrade verification checklist

No.	Task	Description	✔
1	For the SAL Gateway component, ensure that the SAL Gateway services are running.	For more information, see Chapter 6, Verifying the implementation.	
2	For the SLA Mon component, ensure that the SLA Mon services are running.	For more information, see Chapter 6, Verifying the 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 again.	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 152.	

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 does not save the SLA Mon server license or the password. After a restore operation, you must reinstall the license on the WebLM server.
>
> The backup process does not take a backup of the SNMP agent service related files. After a restore operation, you must reconfigure the SNMP agent details on SAL Gateway.

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>
   ```

   Replace *<backup_folder_path>* with the absolute path of the folder where the `ADS_<version_no>_backup.tar` file is located. Do *not* include the backup file name to the path. 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 free disk space available on the server. If the target server has sufficient free 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

Log on to the web interfaces of the Avaya Diagnostic Server components to validate that the configuration information persists after the restore operation.

For the additional steps to be performed after the restore operation, see the checklist mentioned under Related links.

Related links

Checklist of tasks to be performed after a restore operation on page 120

Checklist of tasks to be performed after a restore operation

After you complete a restore operation of Avaya Diagnostic Server, you must complete the following tasks:

No.	Task	Description	✔
1	For the SLA Mon server, reinstall the license on the WebLM server.	The backup process in Avaya Diagnostic Server does not save the WebLM server license information or the password. If you restored data on a different host server and the MAC address is changed, get a new license for the SLA Mon server. Install the new license on the WebLM server. The earlier license is no longer valid. See Installing the SLA Mon server license on WebLM on page 98.	
2	After installing the SLA Mon server license, restart the slamonsrvr service and then the slamonweb service.	Use the following commands to restart service: • `systemctl restart <service_name>` Use the following commands to check the service status: • `systemctl status <service_name>`	

Table continues…

No.	Task	Description	✔
3	(Optional) If you were using SLA Mon SSO through SMGR earlier, and wish to continue using SSO functionality then change the `cesweb.properties` to accept the SSO request and restart the slamonweb service.	Use the following commands: • Navigate to `/opt/avaya/slamon/tomcat/webapps/slamon/WEB-INF/classes/` • In the `cesweb.properties` file, change the `cesweb.sso.add_nav_link_to_smgr=false` value to `true` • Save the `cesweb.properties` file. • Restart the slamonweb service using the following command: `systemctl restart slamonweb.service` or `service slamonweb restart`	
4	For SAL Gateway, reconfigure the SNMP agent details.	The backup process does not take a backup of the SNMP agent service related files. For more information about configuring the SNMP agent, see Chapter 12, Installing and configuring Net-SNMP. For information about configuring the SNMP subagent details on the SAL Gateway user interface, see *Administering Avaya Diagnostic Server SAL Gateway*.	

Table continues…

No.	Task	Description	✔
5	If you restored data on a different server and the server IP address is different from the existing server, perform the following: 1. Through the web interface, change the SAL Gateway IP address configuration. 2. Rediscover SLA Mon agents.	After updating the SAL Gateway IP address, ensure that the new SAL Gateway IP address is added as the trap or alarm destination in all managed devices. Otherwise, the alarm transfer service will be severely impacted. For more information about changing the SAL Gateway IP address configuration, see *Administering Avaya Diagnostic Server SAL Gateway*. For more information about discovering SLA Mon agents, see *Administering Avaya Diagnostic Server SLA Mon*. ✱ **Note:** To avoid changing the IP address configuration, install the target server with the existing IP address on a private network. After the restore operation is successful, take the old server offline and make the new server available on the public network.	

Chapter 9: Migration of Avaya Diagnostic 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 still support the remote access and the alarm transfer features offered by SAL Gateway. But, to install the SLA Mon server component to use the network monitoring features, you will require a host with higher hardware specifications.

Avaya Diagnostic Server 4.0 comes with a migration utility script. You can use this script to take a backup of Avaya Diagnostic Server 3.2.1/3.3. Using the backup file, you can then install Avaya Diagnostic Server 4.0 on a new compatible host.

You can run the script only on Avaya Diagnostic Server 3.2.1/3.3. Therefore, you must upgrade any earlier version of Avaya Diagnostic Server or SAL Gateway to Avaya Diagnostic Server 3.2.1/3.3 before you can migrate to another server.

Note:

- The migration utility does not support migration from Avaya Diagnostic Server 4.0 to Avaya Diagnostic Server 4.0. You can use the existing backup and restore utility of Avaya Diagnostic Server to migrate Avaya Diagnostic Server 4.0 to another host. See Chapter 8, Backing up and restoring Avaya Diagnostic Server.

Migration checklist

The following checklist provides the high-level steps to migrate from Avaya Diagnostic Server 3.2.1/3.3 to Avaya Diagnostic Server 4.0 on a different server:

No.	Task	Description	✔
1	Ensure that you have upgraded to Avaya Diagnostic Server 3.2.1/3.3 on the current host server.	The migration utility script that you need to run for backup is supported on Avaya Diagnostic Server 3.2.1/3.3 only.	
2	Take the full backup of Avaya Diagnostic Server, and copy the backup file to the new target host.	See Backing up Avaya Diagnostic Server data using a migration utility on page 126.	
3	Ensure that the new target host meets the hardware and software prerequisites for a fresh installation of Avaya Diagnostic Server 4.0.	See Chapter 3, Planning and initial setup. **Note:** • Use same IP address and host name for migration. • Maintain the new server on a private network until you complete the migration steps.	
4	Ensure that the SAL Gateway user, saluser, is present on the target host.	The SAL Gateway user owns the file system and services associated with SAL Gateway. Check whether saluser is present on the target host. If saluser is not present, create the user account before you install Avaya Diagnostic Server 4.0 on the new host. See Creating the SAL Gateway user account on page 41.	
5	Start a clean installation of Avaya Diagnostic Server 4.0 on the new host server using the backup file.	The installation must be a clean installation, that is, no SAL Gateway or SLA Mon component exists on the server. See Migrating Avaya Diagnostic Server data in the attended mode on page 127 or Migrating Avaya Diagnostic Server data in the unattended mode on page 128.	

Table continues…

No.	Task	Description	✔
6	Validate that the migration of data is successful on the new server.	Log on to the web interfaces of the components to check whether the configuration information persists after the migration. If you do not see the migrated SLA Mon agents online, restart all SLA Mon services, including slamonsrvr, slamonweb, and slamondb. For SAL Gateway, reconfigure the SNMP agent details. See Chapter 11, Installing and configuring Net-SNMP. For information about configuring the SNMP subagent details on the SAL Gateway user interface, see *Administering Avaya Diagnostic Server SAL Gateway*. ✱ **Note:** You need to configure the SNMP agent details because the migration utility cannot take a backup of the SNMP agent service related files.	
7	Configure iptables rules for SAL Gateway and SLA Mon server.	The migration activity does not automatically update the required iptables rules on the new host. You must update the iptables rules for the communication ports used by SAL Gateway and SLA Mon server. See Updating iptables for SAL Gateway on page 83 and Updating iptables for SLA Mon on page 94.	
8	Reconfigure old subnet iptables rules for OpenVPN enabled SAL Gateway.	1. Run the following command to check postrouting rules: `-t nat -v -L POSTROUTING -n` 2. Verify the following iptable rule is present:`OLD_SUBNET_TO_BE_DELETED` 3. Delete the old subnet rule using the following command:`iptables -t nat -D POSTROUTING -d <sourceSubnet> -j SNAT --to-source <gatewayIP>` 4. Run the following command to verify if the old subnet rule is removed: `-t nat -v -L POSTROUTING -n`	

Table continues…

No.	Task	Description	✔
9	Upload the proxy server certificate to SAL Gateway.	If a proxy server is configured for SAL Gateway and the proxy server has a certificate, you must upload the proxy server certificate to SAL Gateway.	
10	Take the old server offline, or at least stop all services related to Avaya Diagnostic Server on the server.		
11	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 Gateway instances with the same SEID or UUID. Running two SAL Gateway instances simultaneously with the same UUID leads to erroneous alarm transfer and remote access handling.	

Backing up Avaya Diagnostic Server data using a migration utility

About this task

Use this procedure to back up Avaya Diagnostic Server 3.2.1/3.3 using the migration utility. You can use the backup file to migrate Avaya Diagnostic Server to a different server as Avaya Diagnostic Server 4.0.

Before you begin

- Ensure that the Avaya Diagnostic Server version is 3.2.1/3.3. The migration utility script that you need to run for backup is supported on Avaya Diagnostic Server 3.2.1/3.3 only. For any earlier version, upgrade to Avaya Diagnostic Server 3.2.1/3.3 before you run the migration utility.
- Ensure that you extract a copy of the Avaya Diagnostic Server 4.0 software package on the server from where you want to migrate the Avaya Diagnostic Server data.
- If the folder where you want to save the backup file does not exist, create the folder on the host server. This procedure considers `/tmp/backup` as the backup folder.

Procedure

1. Log on to the host server of the existing Avaya Diagnostic Server instance as root.
2. Navigate to `“/opt/avaya/ads/backuprestore”` and ensure that the `migration_backup.sh` file is present in the directory.

3. Run the script as the following:

   ```
   ./migration_backup.sh /tmp/backup
   ```

   The script creates the backup file, `ADS_<version>_backup.tar`, in the `/tmp/backup` directory. For example, if you run the script on a 3.2.1 or 3.3 host, the backup file created is `ADS_3.2_backup.tar` or `ADS_3.3_backup.tar` respectively.

4. Run the following command to transfer the backup file to a folder in the new target host:

   ```
   scp -r /tmp/backup/<backup_filename>
   root@<target_machine_IP>:<destination_folder_path>
   ```

   When prompted, provide the password for the root user of the target machine.

Migrating Avaya Diagnostic Server data in the attended mode

About this task

Use this procedure to migrate Avaya Diagnostic Server data from one server to a new server through attended installation of Avaya Diagnostic Server 4.0.

Before you begin

- Ensure that the backup file is copied to a local directory of the target host.
- Ensure that the SAL Gateway user, saluser, is present on the target host.

Procedure

1. Log on to the target host as root through KVM or a virtual console in graphical user interface (GUI) mode, and start the installation in the attended mode.

   See Chapter 4, Deploying Avaya Diagnostic Server.

2. Continue with the installation steps similar to a fresh installation until the installer asks you whether you want to migrate from a backup file.

3. Type `y`, and press **Enter**.

4. When the installer prompts you to provide the backup file path, type the full path of the backup file.

   If the backup file is correctly created, the installer starts installing Avaya Diagnostic Server with the details extracted from the backup file. The installer does not need any further inputs from you to complete the installation.

Migrating Avaya Diagnostic Server data in the unattended mode

About this task

Use this procedure to migrate Avaya Diagnostic Server data from one server to a new server through unattended installation of Avaya Diagnostic Server 4.0.

Before you begin

- Ensure that the backup file is copied to a local directory of the target host.
- Ensure that you make the following changes in the response file, `ADS_Response.properties`:
  - For the `ADS_AGREELICENSE` property in the response file, replace the value `n` with `y`.
  - For the `BACKUP_FILE_PATH` property, set the value as the full path of the backup file.
  - For the `ADS_COMPONENT_TO_INSTALL` property, set the value as `3` to install Avaya Diagnostic Server with both SAL Gateway and SLA Mon components.

  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`.
- Ensure that the SAL Gateway user, saluser, is present on the target host.

Procedure

1. Log on to the target host as root.
2. Start the installation in the unattended mode.

   See Chapter 4, Deploying Avaya Diagnostic Server.

   If the backup file path is correct, the installer starts installing Avaya Diagnostic Server with the details extracted from the backup file. The installer does not need any further inputs from you to complete the installation.

Creating the SAL Gateway user account

About this task

The SAL Gateway user, saluser, owns the file system and services associated with SAL Gateway.

If the target host is a new virtual machine or a server where SAL Gateway was never installed, saluser might not be present. Use this procedure to check for the presence of the saluser account and to create the account on the target host.

Procedure

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

   ```
   grep -c 'saluser:' /etc/passwd
   ```

   The command returns one of the following:

   - `1`: Implies that the saluser account is present on the target host.
   - `0`: Implies that the saluser account is not present on the target host.
3. If saluser is not present, run the following commands to create the user group and user account:

   ```
   /usr/sbin/groupadd salgroup
   ```

   ```
   /usr/sbin/useradd -g salgroup saluser
   ```

Chapter 10: 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 in graphical user interface (GUI) mode to run the uninstaller in this mode.

✱ **Note:**

If SAL Gateway is running in managed services mode then after uninstallation, `vpnuser` is not removed.

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 in graphical user interface (GUI) mode.

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 131
Completing the SLA Mon server uninstallation on page 132

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 130

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 130

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 11: Installing and configuring Net-SNMP

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 7.x/8.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

About this task

Use this procedure to install and configure the Net-SNMP master agent.

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 136
Configuring the master agent for SNMP v2c on page 138
Configuring the master agent for SNMP v3 on page 138
Defining an SNMP v3 user on page 139

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 one of the following commands to stop the snmpd service:

   - 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.

   - On an RHEL 7.x/8.x system:

     ```
     systemctl stop snmpd
     ```

     The system does not display any output irrespective of the status of the snmpd service. In any case, 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:

   On an RHEL 7.x/8.x system:

   ```
   tcp 0 0 0.0.0.0:705 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 136
Configuring the master agent for SNMP v2c on page 138
Configuring the master agent for SNMP v3 on page 138

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 136

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 136
[Defining an SNMP v3 user]() on page 139

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. Locate and open the following file in a text editor:

   `/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.

Note:

For RHEL 7.x/8.x, the password length should be minimum eight characters. Otherwise, the snmpd service will not start and will display the following error:

```
Error: Could not generate the authentication key from the
supplied phrase.
```

Related links

SNMP master agent configuration on page 136

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 7.x/8.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 140
Configuring the firewall for IPv6 on page 142

Configuring the firewall for IPv4

About this task

You can use this procedure to configure the firewall or iptables on an RHEL 7.x/8.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:
   - For RHEL 7.x/8.x:

     ```
     systemctl status iptables.service
     ```

   If the firewall is stopped or disabled, the system displays one of the following outputs for RHEL 7.x/8.x:

   ```
     iptables.service - IPv4 firewall with iptables
     Loaded: loaded (/usr/lib/systemd/system/iptables.service; enabled; vendor
   preset: disabled)
     Active: inactive (dead) since Fri 2017-02-10 06:58:33 IST; 3s ago
     Process: 3796 ExecStop=/usr/libexec/iptables/iptables.init stop (code=exited,
   status=0/SUCCESS)
     Process: 23650 ExecStart=/usr/libexec/iptables/iptables.init start
   (code=exited, status=0/SUCCESS)
    Main PID: 23650 (code=exited, status=0/SUCCESS

   Feb 09 11:38:18 linpubc238.gl.avaya.com systemd[1]: Starting IPv4 firewall with
   iptables...
   Feb 09 11:38:18 linpubc238.gl.avaya.com iptables.init[23650]: iptables: Applying
   firewall rules: [  OK  ]
   Feb 09 11:38:18 linpubc238.gl.avaya.com systemd[1]: Started IPv4 firewall with
   iptables.
   Feb 10 06:58:32 linpubc238.gl.avaya.com systemd[1]: Stopping IPv4 firewall with
   iptables...
   Feb 10 06:58:32 linpubc238.gl.avaya.com iptables.init[3796]: iptables: Setting
   chains to policy ACCEPT: filter [  OK  ]
   Feb 10 06:58:33 linpubc238.gl.avaya.com iptables.init[3796]: iptables: Flushing
   firewall rules: [  OK  ]
   Feb 10 06:58:33 linpubc238.gl.avaya.com iptables.init[3796]: iptables: Unloading
   modules: [  OK  ]
   Feb 10 06:58:33 linpubc238.gl.avaya.com systemd[1]: Stopped IPv4 firewall with
   iptables.
   ```

   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:

   For RHEL 7.x/8.x:

   ```
   iptables –L
   ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:snmp
   ACCEPT     udp  --  anywhere             anywhere             udp dpt:snmp
   ```

   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:

   For RHEL 7.x/8.x:

   ```
   systemctl restart iptables.service
   ```

Related links

Firewall (iptables) configuration on page 140
Disabling SELinux for the master agent on page 143

Configuring the firewall for IPv6

About this task

You can use this procedure to configure the firewall or iptables on an RHEL 7.x/8.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 140
Disabling SELinux for the master agent on page 143

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 40. 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 one of the following commands to start the snmpd service:
   - You must get the following output:

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

     Note:

     The snmpd service must start with an `OK` message.
   - On an RHEL 7.x/8.x system:

     ```
     systemctl start snmpd
     ```

     No output is displayed on RHEL 7.x/8.x system. To confirm the status, run the following command:

     ```
     systemctl status snmpd.service
     ```
3. Run the one of the following commands to ensure that the master agent service snmpd starts when the system boots:
   - On an RHEL 7.x/8.x system:

     ```
     systemctl enable snmpd.service
     ```
4. Run the following command to verify that the **chkconfig** command was successful:
   - On an RHEL 7.x/8.x system:

     ```
     systemctl enable snmpd.service
     ```

     You must get the following output:

     ```
     snmpd.service enabled
     ```

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.

Procedure

1. Log in as root to the SAL Gateway host.
2. Run the one of the following commands to restart the subagent service:
   - On an RHEL 7.x/8.x system:

```
systemctl start snmpAgent
```

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 138.
Authorization Protocol	`MD5`
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 12: 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.

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:

- On an RHEL 7.x/8.x system:

  ```
  systemctl stop spiritAgent
  ```

  ```
  systemctl stop gatewayUI
  ```

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, and gatewayUI, 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 147

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
   ```

Avaya Diagnostic Server auto upgrade failure

Condition

While trying to auto upgrade Avaya Diagnostic Server 3.3.x to Avaya Diagnostic Server Release 4.0, the upgrade process failed.

Solution

1. Log on to the host server through KVM or a virtual console in graphical user interface (GUI) mode as root.
2. Verify if the installer file is extracted in `/opt/avaya/ads/Upgrade/packages/INSTALLER/ADS-MAJOR-4.0.0/installer/ADS-Installer-4.0.0.0-751`
3. Follow the manual upgrade procedure. See Upgrading Avaya Diagnostic Server in the attended mode on page 111 or Upgrading Avaya Diagnostic Server in the unattended mode on page 114

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 13: 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.

Chapter 14: 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		
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 the customer site.	Solution architects, implementation engineers, support personnel, and customers
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 SAL Policy Manager with SSH Proxy	Provides information about configuring, administering, and using SAL Policy Manager with SSH Proxy to control and monitor remote sessions to Avaya products at the customer site.	Solution architects, implementation engineers, support personnel, and customers
Implementation		
Deploying SAL Policy Manager with SSH Proxy	Describes the implementation requirements and procedures to deploy the SAL Policy Manager with SSH Proxy software.	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

Table continues…

Title	Description	Audience
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 158

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select the appropriate release number.

   The **Choose Release** field is not available if there is only one release for the product.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list only displays the documents for the selected category.
7. Click **Enter**.

Related links

Documentation on page 157

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.

- 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 159

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 without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any 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 system displays the Avaya Support page.
3. Click **Support by Product** > **Product Specific Support**.
4. In **Enter Product Name**, enter the product, and press `Enter`.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Related links

Support on page 159

Appendix A: Installing Java Runtime Environment

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

Example command output:

```
openjdk version "1.8.0_312" OpenJDK Runtime Environment (build
1.8.0_312-b07) OpenJDK 64-Bit Server VM (build 25.312-b07, mixed mode)
```

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 the 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. Update or insert the `JAVA_HOME` variable in the file as the following:

      ```
      export JAVA_HOME=/<java_install_path>/jre1.8.0_<version>
      ```

      For example, if `/usr/java8/jre1.8.0_21` is the location of the installed JRE, update the line as:

      ```
      export JAVA_HOME=/usr/java8/jre1.8.0_21
      ```

   c. Save and close the `/home/saluser/.bashrc` file.
2. Perform the following to update the Java environment variable for root:

   ✱ **Note:**

   Any assignment or export of environment variable must be in a single line in the .bash_profile or .bashrc file of the root user.

   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>/jre1.8.0_<version>
      ```

   c. Add the following lines in the file:

      ```
      PATH=$PATH:$JAVA_HOME/bin/:$HOME/bin:/usr/bin:/usr/sbin:/bin
      export JAVA_HOME
      export PATH
      ```

   d. Save and close the file.
3. Ensure that `/etc/alternatives` is updated to use the correct JRE version supported by Avaya Diagnostic Server.

   Since RHEL 7.x or 8.x comes with Java JDK as part of the suite, the host might have multiple Java versions. You must ensure that the correct Java version is used by Avaya Diagnostic Server.

Next steps

Restart the services of each Avaya Diagnostic Server component.

Appendix B: 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 C: 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.

Appendix D: Configuring SLA Mon server behind NAT or DMZ

About this task

With SLA Mon 3.1.1 release, a product installed with SLA Mon agent can work outside the enterprise network as a Remote Worker agent. For a Remote Worker phone to be registered and discovered by SLA Mon server, it must be hosted behind a Network Address Translation (NAT) or in a Demilitarized Zone (DMZ), accessible by a public IP address. The public IP address used by the Remote Worker phones is the IP address of the routers that these phones are connected to when outside the enterprise network.

Before you begin

- Ensure that SLA Mon 3.1 service pack 1 is installed.
- The additional IP table rules are configured, at the server edge and network edge.
- The public IP address of remote worker phones are added at network edge to a white list of IP addresses.
- Once SLA Mon server is hosted either in a DMZ or behind NAT, the public IP address is updated in the application.

Procedure

1. Log on to the SLA Mon Server as a root user.
2. Run the following command to navigate to the `agentcom-slamon.conf` file:

   ```
   cd /opt/avaya/slamon/bundleconf
   ```
3. Run the following command to open the `agentcom-slamon.conf` file:

   ```
   vi agentcom-slamon.conf
   ```
4. Locate the entry **keyServer.protocols** in the file.
5. Remove the hash (#) character in front of the entry to uncomment the **server.publicIP** line.
6. Type **`!wq`** to save the file and exit the editor.
7. Run the following commands to restart the SLA Mon services:
   - **`service slamonweb stop`**
   - **`service slamonsrvr stop`**

- **`service slamondb restart`**
- **`service slamonsrvr start`**
- **`service slamonweb start`**

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.

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