Deploying Avaya Diagnostic Server using VMware® in the Virtualized Environment

Release 3.0
Issue 4
May 2021

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.

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

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

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

Support tools

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

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

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

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

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

Avaya Diagnostic Server is VMware Ready.

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.

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 7
Purpose 7
Revision history 7
Chapter 2: Architecture overview 8
Avaya Aura® Virtualized Environment overview 8
Virtualized components 8
Chapter 3: Planning and configuration 10
Planning 10
Server hardware and resources 11
Avaya Diagnostic Server virtual appliance resource requirements 11
VMware software requirements 12
WebLM 12
Specifications of bundled software in the OVA 13
Capacity of Avaya Diagnostic Server in a virtualized environment 13
Chapter 4: Initial setup and predeployment 14
Registering for PLDS 14
Downloading software from PLDS 14
Registering SAL Gateway 15
Chapter 5: Deploying the Avaya Diagnostic Server OVA 17
Avaya Diagnostic Server OVA deployment overview 17
Deployment checklist 17
Deploying the Avaya Diagnostic Server OVA to vCenter 18
Properties field descriptions 21
Deploying the Avaya Diagnostic Server OVA directly to the ESXi server 22
Deployment of cloned and copied OVAs 23
Chapter 6: Initial configuration 24
Starting the virtual machine 24
Configuring the Avaya Diagnostic Server parameters and the network parameters 24
Configuring the virtual machine automatic startup settings 25
Chapter 7: Software installation 27
Software installation checklist 27
Installing Avaya Diagnostic Server in the unattended mode 27
ADS_Response.properties file 29
Installing a service pack in the unattended mode 44
Chapter 8: Post-installation verification and testing 46
Verification of the SAL Gateway implementation 46
Testing the alarming service of SAL Gateway 46
Testing the SAL Gateway UI 46
Testing the SAL Watchdog service 47

Verification of the SLA Mon implementation 48
Testing the slamonsrvr service 48
Testing the slamonweb service 49
Testing the slamondb service 49
Chapter 9: Postinstallation customer responsibilities 50
Chapter 10: Upgrading Avaya Diagnostic Server virtual appliance 51
Upgrade from SAL Gateway 2.2 virtual appliance 51
Migration checklist for SAL Gateway 2.2 virtual appliance 51
Exporting managed element data 53
Importing managed elements to SAL Gateway 54
Upgrade from the Avaya Diagnostic Server 2.0 virtual appliance 56
Migrate from Avaya Diagnostic Server 2.5 virtual appliance 57
Migration of Avaya Diagnostic Server 57
Checklist for migration from Avaya Diagnostic Server 2.5 57
Backing up Avaya Diagnostic Server data using a migration utility 60
Migrating Avaya Diagnostic Server data in the unattended mode 60
Validating an upgrade operation 61
Chapter 11: Maintenance procedures 63
Backup and restore overview 63
Backing up the virtual machine 63
Restoring a virtual machine from a backup 64
Creating a snapshot 65
Restoring a snapshot 65
Chapter 12: Troubleshooting 67
Replace with your title 67
FAQ 67
Chapter 13: Resources 70
Documentation 70
Viewing Avaya Mentor videos 71
Support 71
Appendix A: VMware best practices for performance 72
BIOS 72
Intel Virtualization Technology 72
Dell PowerEdge Server 73
HP ProLiant Servers 73
VMware Tools 74
Timekeeping 74
Configuring timing 75
VMware networking best practices 76
Thin vs. thick deployments 77
Best practices for VMware features 78
VMware Snapshots 78

VMware vMotion..... 79
VMware High Availability..... 80
Hyperthreading..... 80
Appendix B: Password management..... 81
Password policies..... 81
Resetting the password of an operating system account..... 81
Resetting the password of the admin user..... 82
Resetting the password of the root user..... 82
Glossary..... 83

Chapter 1: Introduction

Purpose

This document provides procedures for deploying the Avaya Diagnostic Server virtual appliance in the Avaya Aura® Virtualized Environment. The document includes installation, configuration, initial administration, troubleshooting, and basic maintenance checklists and procedures.

This document does not include optional or customized aspects of a configuration.

The primary audience for this document is anyone who installs, configures, and verifies Avaya Diagnostic Server in a VMware® vSphere™ 5.5, 6.0 or 6.5 virtualization environment at a customer site. The audience includes implementation engineers, field technicians, business partners, solution providers, and customers.

Revision history

Issue	Date	Summary of changes
Release 3.0, issue 1	August 2017	The first issue of the document in this release.
Release 3.0, issue 2	January 2018	Added a new topic. See Software installation checklist on page 27. Updated a topic. See Resetting the password of the root user on page 82
Release 3.0, issue 3	April 2019	Updated the following topics:. • See VMware software requirements on page 12 • See Password policies on page 81
Release 3.0, issue 4	November 2019	Updated the IOPS value. See Avaya Diagnostic Server virtual appliance resource requirements on page 11

Chapter 2: Architecture overview

Avaya Aura® Virtualized Environment overview

Avaya Aura® Virtualized Environment integrates real-time Avaya Aura® applications with VMware® virtualized server architecture.

Using Avaya Aura® Virtualized Environment, customers with a VMware IT infrastructure can upgrade to the next release level of collaboration using their own VMware infrastructure. For customers who need to add more capacity or application interfaces, Avaya Aura® applications on VMware offer flexible solutions for expansion. For customers who want to migrate to the latest collaboration solutions, Avaya Aura® Virtualized Environment provides a hardware-efficient simplified solution for upgrading to the latest Avaya Aura® release and adding the latest Avaya Aura® capabilities.

The Virtualized Environment project applies only for Avaya Appliance Virtualization Platform and customer VMware®, and does not include any other industry hypervisor.

Note:

This document uses the following terms, and at times, uses the terms interchangeably.

- server and host
- reservations and configuration values

Deployment considerations

The following manage the deployment to the blade, cluster, and server:

- Avaya Appliance Virtualization Platform from System Manager Solution Deployment Manager or the Solution Deployment Manager client
- VMware® vCenter and VMware® vSphere

Virtualized components

Software component	Description
ESXi Host	The physical machine running the ESXi Hypervisor software.

Table continues…

Software component	Description
ESXi Hypervisor	A platform that runs multiple operating systems on a host computer at the same time.
vSphere Client	vSphere Client is an application that installs and manages virtual machines. vSphere Client connects to a vCenter server or directly to an ESXi host if a vCenter Server is not used. The application is installed on a personal computer or accessible through a web interface.
vCenter Server	vCenter Server provides centralized control and visibility at every level of the virtual infrastructure. vCenter Server provides VMware features such as High Availability and vMotion.
Appliance Virtualization Platform	Avaya-provided virtualization turnkey solution that includes the hardware and all the software including the VMware hypervisor.
Solution Deployment Manager	Centralized software management solution of Avaya that provides deployment, upgrade, migration, and update capabilities for the Avaya Aura® virtual applications.
Open Virtualization Appliance (OVA)	The virtualized OS and application packaged in a single file that is used to deploy a virtual machine.

Chapter 3: Planning and configuration

Planning

As an Avaya customer, ensure that you complete the following before deploying the Avaya Diagnostic Server open virtual appliance (OVA):

#	Action	Notes	✔
1	Register for the Avaya Product Licensing and Delivery System (PLDS) website at https://plds.avaya.com.	See Registering for PLDS on page 14.	
2	Download the Avaya Diagnostic Server OVA file from PLDS.	To log on to the PLDS website, use your Avaya Single Sign On (SSO) login, which is associated with the Sold-To number that identifies the location where you want to install Avaya Diagnostic Server.	
3	Ensure that you have all required hardware for the VMware environment.	See Server hardware and resources on page 11.	
4	Ensure that you plan the staging and verification activities and the virtualization environment has enough resources to be assigned for the Avaya Diagnostic Server virtual appliance. **Note:** Accept the default SAL GatewayID during the Avaya Diagnostic Server installation. After the installation, you can generate the ID through the SAL Gateway user interface.	See Avaya Diagnostic Server virtual appliance resource requirements on page 11.	
5	If you do not have an existing WebLM server, download the WebLM OVA from PLDS and deploy it.	The Avaya Diagnostic Server virtual appliance does not come with an embedded WebLM server. To run the SLA Mon server component, you must deploy and use an external WebLM server.	

Table continues…

#	Action	Notes	✔
6	Ensure that you configure the time and NTP settings on the ESXi server.	If you do not complete this task before you deploy and configure the OVA, the deployed virtual machine might not start correctly.	

Server hardware and resources

VMware offers compatibility guides that list servers, system, I/O, storage, and backup compatibility with VMware infrastructure. For more information about VMware-certified compatibility guides and product interoperability matrices, see http://www.vmware.com/resources/guides.html.

The VMware-certified servers must be running ESXi 5.5, ESXi 6.0, ESXi 6.5, ESXi 6.7, or ESXi 7.0 with any updates.

Avaya Diagnostic Server virtual appliance resource requirements

Before you deploy the Avaya Diagnostic Server virtual appliance, you must ensure that the following minimal set of resources is available on the ESXi host. These resources are specified in the Avaya Diagnostic Server OVA.

VMware Resource	Value
vCPU	4
CPU speed	2.3 GHz
Memory	8 GB
Storage reservation	250 GB
Shared NIC	2@ 1000 Mbps
IOPS	1200

If you cannot guarantee the availability of the required resources on the ESXi host, do not deploy the Avaya Diagnostic Server virtual appliance on that host.

You might deploy the Avaya Diagnostic Server virtual appliance on a host that does not have the resources to allocate to the virtual machine to start. If CPU resources are limited, the system displays the `Insufficient capacity on each physical CPU`, or a similar message after the start-up request. To correct such limitations, you can adjust the virtual machine properties, such as CPU reservations.

Sometimes, the CPU adjustments might not correct the start-up conditions. You might have to adjust other virtual machine resources as required.

Important:

Modifying the allocated resources might have a direct impact on the performance, capacity, and stability of the Avaya Diagnostic Server virtual appliance. To run at full capacity, ensure that the virtual machine meets these resource size requirements. Removing or downsizing reservations might put this requirement at risk.

For Avaya Diagnostic Server to perform at maximum capacity, maintain the resource allocation for the virtual machine to have 4 vCPUs with CPU speed of 2.3 GHz or higher.

VMware software requirements

The following are the supported VMware software versions:

- VMware vSphere ESXi 5.5
- VMware vSphere ESXi 6.0
- VMware vSphere ESXi 6.5 update 2
- VMware vSphere ESXi 6.7 update 1
- VMware vSphere ESXi 6.7 update 2
- VMware vSphere ESXi 6.7 update 3
- VMware vCenter Server 5.5
- VMware vCenter Server 6.0
- VMware vCenter Server 6.5 update 2
- VMware vSphere Client 5.5
- VMware vSphere Client 6.0
- VMware vSphere ESXi 6.5
- VMware vCenter Server 6.7
- VMware vSphere ESXi 7.0
- VMware vCenter Server 7.0

WebLM

Avaya provides a web-based license manager (WebLM) to manage licenses of one or more Avaya software products.

To track and manage licenses in an organization, WebLM requires a license file from the Avaya Product Licensing and Delivery System (PLDS) website at https://plds.avaya.com.

The license file is in XML format and contains information about the product such as the licensed capacities of each feature that you purchase. You activate the license file in PLDS and install the license file on the WebLM server.

You must run WebLM as a separate VMware virtual machine or use the WebLM running on System Manager. For more information about WebLM administration, see *Administering Avaya Aura® System Manager*.

Specifications of bundled software in the OVA

The Avaya Diagnostic Server OVA contains the application software, operating system, and other required software components, along with preinstalled VMware tools.

The following are the specifications of the software components included as part of the Avaya Diagnostic Server OVA.

Operating system	CentOS 7.3, 64-bit
Java	OpenJDK JRE 1.8.0_141
Application installer	Avaya Diagnostic Server 3.0 and Avaya Diagnostic Server service pack 1

Capacity of Avaya Diagnostic Server in a virtualized environment

The capacity of Avaya Diagnostic Server in VMware virtualization environment is the same as the capacity of a software-only implementation of Avaya Diagnostic Server. To run at full capacity, the virtual machine must meet the required specifications and the resource allocation. Also, the alarm flow, remote sessions, and network conditions must be normal. For the capacity matrix of Avaya Diagnostic Server, see *Deploying Avaya Diagnostic Server*. Download the latest version of the document at http://support.avaya.com/.

Chapter 4: Initial setup and predeployment

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

When you place an order for an Avaya PLDS-licensed software product, PLDS creates the license entitlements of the order and sends an email notification to you. The email includes a license activation code (LAC) and instructions for accessing and logging into PLDS. Use the LAC to locate and download the purchased license entitlements.

In addition to PLDS, you can download the product software from http://support.avaya.com using the **Downloads and Documents** tab at the top of the page.

Note:

Only the latest service pack for each release is posted on the support site. Previous service packs are available only through PLDS.

Procedure

1. Enter http://plds.avaya.com in your Web browser to access the Avaya PLDS website.
2. Enter your login ID and password.
3. On the PLDS home page, select **Assets**.
4. Click **View Downloads**.
5. Click on the search icon (magnifying glass) for **Company Name**.
6. In the **%Name** field, enter **Avaya** or the Partner company name.
7. Click **Search Companies**.
8. Locate the correct entry and click the **Select** link.
9. Enter the Download Pub ID.
10. Click **Search Downloads**.
11. Scroll down to the entry for the download file and click the **Download** link.
12. In the **Download Manager** box, click the appropriate download link.

    Note:

    The first link, **Click to download your file now**, uses the Download Manager to download the file. The Download Manager provides features to manage the download (stop, resume, auto checksum). The **click here** link uses your standard browser download and does not provide the download integrity features.
13. If you use Internet Explorer and get an error message, click the **install ActiveX** message at the top of the page and continue with the download.
14. Select a location where you want to save the file and click **Save**.
15. If you used the Download Manager, click **Details** to view the download progress.

Registering SAL Gateway

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

About this task

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

Procedure

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

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

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

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

6. Click **Next**.

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

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

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

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

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

Next steps

- Complete the SAL Gateway installation process.
- Perform the technical onboarding process for devices that require support through the new SAL Gateway. See *Global Registration Tool 3 – Technical Onboarding User Guide* at https://support.avaya.com/registration.
- Add the devices as managed elements to your SAL Gateway using the SEIDs provided.

Chapter 5: Deploying the Avaya Diagnostic Server OVA

Avaya Diagnostic Server OVA deployment overview

The Avaya Diagnostic Server 3.0 OVA supports the following two virtualization environments:

- Avaya Aura® Virtualized Appliance (VA): Avaya-provided server and Avaya Appliance Virtualization Platform
- Avaya Aura® Virtualized Environment (VE): Customer-provided VMware infrastructure

This document covers the deployment in a customer-provided VMware virtualized environment. The Avaya Diagnostic Server OVA supports two modes of deployment on a VMware vSphere 5.5, 6.0, or 6.5 environment. Based on the VMware environment at the customer site, select one of the following two methods of deployment:

- vCenter deployment through a vSphere client
- Direct deployment to the ESXi server through a vSphere client

For information about deploying the Avaya Diagnostic Server OVA in the Avaya Aura® Virtualized Appliance environment by using Avaya Aura® System Manager Solution Deployment Manager, see *Deploying Avaya Diagnostic Server using Avaya Aura® System Manager in the VMware® Virtualized Environment*.

Deployment checklist

Use the following checklist for deploying the Avaya Diagnostic Server virtual appliance.

No.	Action	Link/Notes	✔
1	Ensure that the ESXi host server is ready.		

Table continues…

No.	Action	Link/Notes	✔
2	Deploy the OVA.	See Deploying the Avaya Diagnostic Server OVA to vCenter on page 18 or Deploying the Avaya Diagnostic Server OVA directly to the ESXi server on page 22.	
3	Change the default passwords of the operating system accounts.	The Avaya Diagnostic Server virtual appliance has administrator and root users with default passwords. You must change the passwords for these user accounts immediately after the deployment of the OVA. See Resetting the password of an operating system account on page 81 and Password policies on page 81. **Caution:** You must change and control the root and administrator user passwords according to the password control policy of the company. Avaya is not responsible for password control and not liable for any adverse outcomes that might result from inadequate password control and failure to change the default passwords. Because the root password belongs to the customer, Avaya cannot reset or recover the root password if lost or forgotten. Also, due to hardening of operating system, no known way exists to reset or recover the root password.	
4	Install Avaya Diagnostic Server 3.0 and service pack 1 on the virtual machine.	See Installing Avaya Diagnostic Server in the unattended mode on page 27 and Installing a service pack in the unattended mode on page 44.	

Deploying the Avaya Diagnostic Server OVA to vCenter

If you have a vCenter server to administer your VMware infrastructure, use this procedure to deploy the Avaya Diagnostic Server OVA to your VMware infrastructure. In the vCenter

deployment, you get the options to provide the Avaya Diagnostic Server configuration information through the deployment wizard windows.

Procedure

1. Connect to the vCenter server through the vSphere client.
2. Select **File** > **Deploy OVF Template**.
3. In the Deploy OVF Template window, perform one of the following to select the OVA file, and click **Next**:
   - If the OVA file is downloaded at a location accessible from your computer, click **Browse** to select the location.
   - If the OVA file is located on an HTTP server, enter the full URL in the **Deploy from a file or URL** field.
4. In the OVF Template Details window, verify the details about the Avaya Diagnostic Server OVA template, and click **Next**.
5. In the End User License Agreement window, read the license agreement, click **Accept**, and click **Next**.

   You must accept the license agreement to continue with the deployment.
6. Perform the following to specify the location for the deployment:
   a. In the Name and Location window, in the **Name** field, type a unique name for the new virtual machine.
   b. From the **Inventory Location** field, select the inventory location to deploy the virtual machine.
   c. Click **Next**.

      If you did not select a host when you started the deployment process, the wizard displays the Host/Cluster window.
   d. Select the host or cluster where you want to deploy the virtual machine, and click **Next**.

      If the host or cluster has resource pools, the wizard displays the Resource Pool window.
   e. Select the resource pool you want to use, and click **Next**.
7. In the Storage window, select the data store location to store the virtual machine files, and click **Next**.
8. In the Disk Format window, choose one of the following disk formats, and click **Next**.
   - **Thick Provision Lazy Zeroed**: Allocates the required disk space during the creation of the virtual disk for the Avaya Diagnostic Server virtual appliance.
   - **Thick Provision Eager Zeroed**: Allocates the required disk space during the creation of the virtual disk for the Avaya Diagnostic Server virtual appliance. Also, the allocated blocks are zeroed out at the time of creation. Eager zeroed takes longer time to create the disk space than lazy zeroed.

- **Thin Provision**: Does not allocate the required space in advance. In this option, the virtual disk grows as required during the normal course of operation in the virtual machine.

For more information about virtual disk, see Thin vs. thick deployments on page 77.

9. In the Properties window, perform the following to configure the Avaya Diagnostic Server specifications:

   Important:

   For the Avaya Diagnostic Server components to function correctly, you must replace the default values in this window with correct values that match your environment.

   You must provide correct SMTP details to receive software update notifications from Avaya.

   You must complete all mandatory fields to ensure successful deployment of the Avaya Diagnostic Server virtual appliance. You can identify the mandatory fields from the asterisk (*) next to the field name.

   a. In the **Timezone setting** field, set the appropriate time zone of the location where you are deploying the Avaya Diagnostic Server virtual appliance. Avaya Diagnostic Server
   b. In the **Hostname** field, enter a host name or fully qualified domain name for the Avaya Diagnostic Server virtual appliance.
   c. In the Network Properties section of the Properties window, complete the following fields according to your network settings:
      - **Default Gateway**
      - **DNS**
      - **Public IP Address**
      - **Public Netmask**
      - **OOBM Selection**
      - **Out Of Band Management IP Address**
      - **Out Of Band Management Netmast**

   For more information about the fields, see Properties field descriptions.

   Note:

   If OOBM is enabled during deployment, then you must configure the OOBM IP address in SAL Gateway.

10. Click **Next**.
11. **(Optional)** In the Ready to Complete window, select the **Power on after deployment** check box to start the virtual machine automatically after the deployment.

    If you do not select this check box, you can start the virtual machine manually after the deployment.

12. In the Ready to Complete window, verify the properties in the Deployment settings section, and click **Finish**.

    The deployment process takes approximately 8 to 10 minutes to complete. If the OVA file location is an HTTP server, the deployment process might take more time.

Next steps

If you did not select the option to start the virtual machine automatically, start the virtual machine.

Install Avaya Diagnostic Server 3.0 and service pack 1 on the virtual machine.

Related links

Starting the virtual machine on page 24

Properties field descriptions

When you deploy the Avaya Diagnostic Server virtual appliance to your VMware infrastructure through a vCenter server, you get the options to provide the network configuration information for the virtual appliance through the Properties window of the deployment wizard.

The following table provides the descriptions of the fields available in the Application section of the Properties page.

Name	Description
Timezone setting	The appropriate time zone for the location where you deploy the Avaya Diagnostic Server virtual appliance.
Hostname	The host name or fully qualified domain name of the Avaya Diagnostic Server virtual appliance.

The following table provides the descriptions of the fields available in the Network Properties section of the Properties page.

Name	Description
Default Gateway	The IP address of the default gateway on your network.
DNS	The comma-separated addresses of the Domain Name Servers (DNS) for the virtual machine.
Public IP Address	The IP address of the public network interface.
Public Netmask	The netmask or prefix for the public network interface.
OOBM Selection	The field to indicate whether to use Out Of Band Management (OOBM) network for the virtual appliance. You can select one of the following: • **Yes**: To use OOBM network. • **No**: Not to use OOBM network.
Out of Band Management IP Address	The IP address of the OOBM network interface.
Out of Band Management Netmask	The netmask or prefix for the OOBM network interface.

Deploying the Avaya Diagnostic Server OVA directly to the ESXi server

About this task

Use this procedure to deploy the Avaya Diagnostic Server OVA directly to an ESXi server through a vSphere client.

Procedure

1. Connect to the ESXi host server through the vSphere client.
2. Select **File** > **Deploy OVF Template**.
3. In the Deploy OVF Template window, perform one of the following to select the OVA file, and click **Next**:
   - If the OVA file is downloaded at a location accessible from your computer, click **Browse** to select the location.
   - If the OVA file is located on an http server, enter the full URL in the **Deploy from a file or URL** field.
4. In the OVF Template Details window, verify the details about the Avaya Diagnostic Server OVA template, and click **Next**.
5. In the End User License Agreement window, read the license agreement, click **Accept**, and click **Next**.

   You must accept the license agreement to continue with the deployment.
6. In the Name and Location window, in the **Name** field, type a unique name for the new virtual machine, and click **Next**.
7. In the Disk Format window, choose one of the following disk formats, and click **Next**.
   - **Thick Provision Lazy Zeroed**: Allocates the required disk space during the creation of the virtual disk for the Avaya Diagnostic Server virtual appliance.
   - **Thick Provision Eager Zeroed**: Allocates the required disk space during the creation of the virtual disk for the Avaya Diagnostic Server virtual appliance. Also, the allocated blocks are zeroed out at the time of creation. Eager zeroed takes longer time to create the disk space than lazy zeroed.
   - **Thin Provision**: Does not allocate the required space in advance. In this option, the virtual disk grows as required during the normal course of operation in the virtual machine.

   For more information about virtual disk, see Thin vs. thick deployments on page 77.
8. **(Optional)** In the Ready to Complete window, select the **Power on after deployment** check box to start the virtual machine automatically after the deployment.

   If you do not select this check box, you can start the virtual machine manually after the deployment.

9. In the Ready to Complete window, verify the deployment settings, and click **Finish**.

   The deployment process takes approximately 8 to 10 minutes to complete. If the OVA file location is an HTTP server, the deployment process might take more time.

Next steps

If you did not select the option to start the virtual machine automatically, start the virtual machine manually.

Start the virtual machine console, and configure the network parameters for the virtual machine.

Install Avaya Diagnostic Server 3.0 and Service Pack 1 on the virtual machine.

Related links

Starting the virtual machine on page 24

Configuring the Avaya Diagnostic Server parameters and the network parameters on page 24

Deployment of cloned and copied OVAs

Do not create a copy of the virtual machine or clone the virtual machine. Avaya strongly discourages cloning of virtual machine to avoid improper configuration setting that might cause communication issues with SAL core server.

If you still want to clone a virtual machine, ensure that the following configuration is correct on cloned virtual machine:

- MAC address
- Solution Element ID (SEID) of SAL Gateway
- Alarm ID
- IP address

Chapter 6: Initial configuration

Starting the virtual machine

Use this procedure to start the virtual machine.

Procedure

1. In the vSphere client, right-click the virtual machine, and click **Power** > **Power On**.
2. In the vSphere client, right click the virtual machine, and click **Open Console**.

Result

The console displays the system startup messages and the system starts the system services. After the startup process is complete, the system displays a message to log on to the virtual machine.

If you deploy the virtual machine directly on the ESXi host server, the system displays messages to set the network parameters whenever you start the virtual machine. At the very first startup of the virtual machine, the system also prompts to set the configuration parameters of Avaya Diagnostic Server.

Configuring the Avaya Diagnostic Server parameters and the network parameters

If you deploy the Avaya Diagnostic Server virtual appliance directly on an ESXi host server, the virtual appliance is deployed with some default configuration values. When you start the virtual machine for the first time, you must configure the network parameters.

Note:

At each subsequent restart of the virtual machine that you deployed directly on an ESXi host, you get the options to reconfigure the virtual machine. You can either continue with the configuration or skip the configuration in the subsequent restarts.

About this task

Use this procedure to configure the network parameters after starting the virtual machine for the first time.

Procedure

1. After you start the virtual machine for the first time, open the virtual machine console.

   As a part of the startup, the system prompts you to configure the network parameters.

2. If required, select the appropriate option in the configuration wizard to change the following network settings:

   - The Public IP address of the default gateway on your network.

     Note:

     Set the Public IP address and Public netmask before entering the default gateway information for the virtual machine.

   - The host name of the virtual machine.
   - The domain name server (DNS) information.
   - The Public IP address allocated to the virtual machine.
   - The OOBM network details for the virtual machine.

3. When the system prompts you to configure the time zone, perform the following:

   a. From the menu options in the configuration wizard, select the continent or ocean, and then select the country where the deployment site is located.

      If the selected country has multiple time zones, you get menu options to further identify the location for the correct configuration of the time zone.

   b. **(Optional)** For a country with multiple time zones, select the appropriate location.

   c. Confirm the time zone selection.

4. Confirm the configuration changes.

   The system configures the virtual appliance components according to the settings you entered.

Related links

Properties field descriptions on page 21

Configuring the virtual machine automatic startup settings

About this task

This procedure does not apply for deployments and upgrades of applications running on Appliance Virtualization Platform.

When a vSphere ESXi host restarts after a power failure, the virtual machines that are deployed on the host do not start automatically. You must configure the virtual machines to start automatically.

In high availability (HA) clusters, the VMware HA software ignores the startup selections.

Before you begin

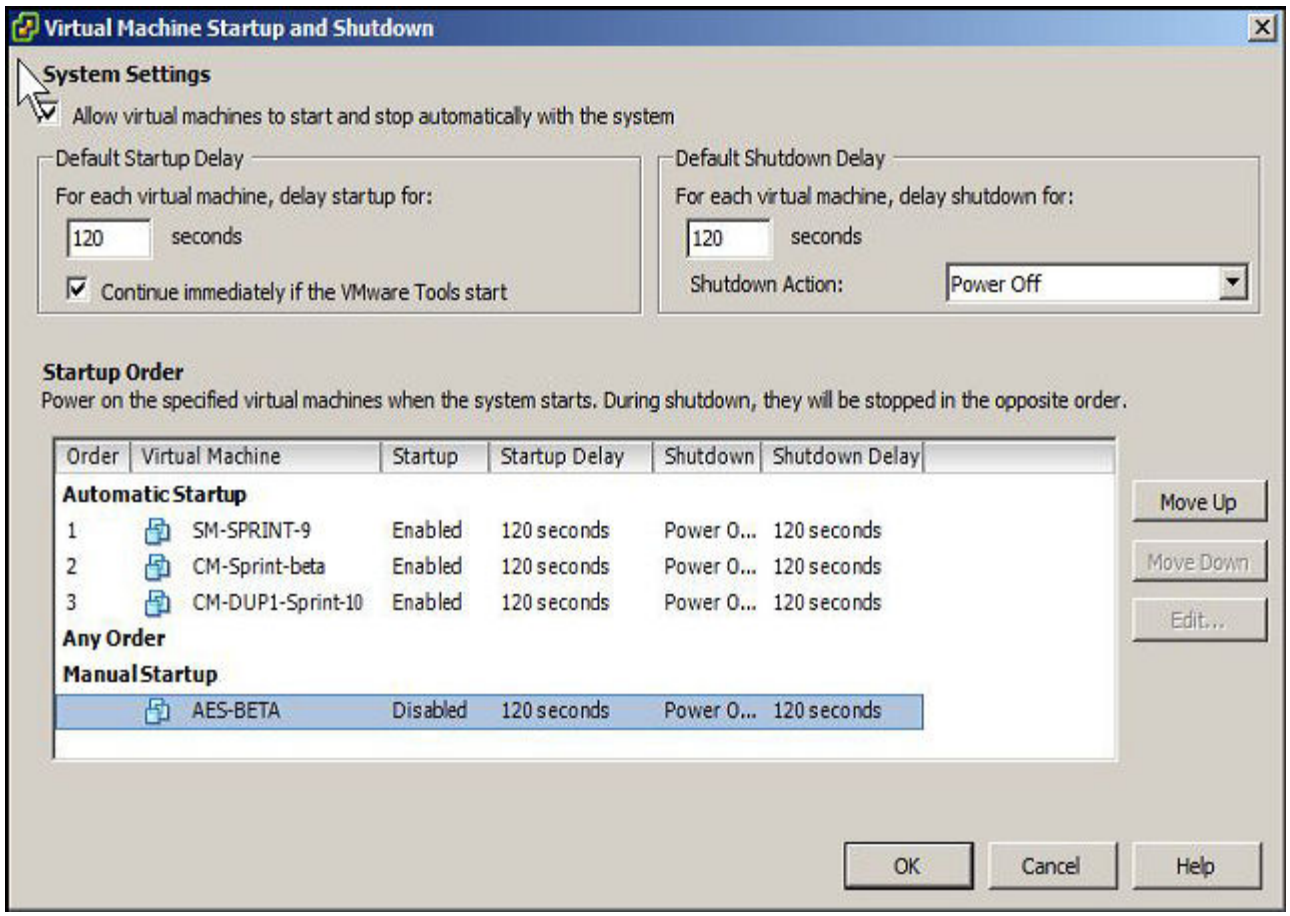
Verify with the system administrator that you have the proper level of permissions to configure the automatic startup settings.

Procedure

1. In the vSphere Client inventory, select the host where the virtual machine is located.
2. Click the **Configuration** tab.
3. In the **Software** section, click **Virtual Machine Startup/Shutdown**.
4. Click **Properties** in the upper-right corner of the screen.
5. In the **System Settings** section, select **Allow virtual machines to start and stop automatically with the system**.
6. In the **Manual Startup** section, select the virtual machine.
7. Use the **Move up** button to move the virtual machine to the **Automatic Startup** section.
8. Click **OK**.

Example

The following is an example of the **Virtual Machine Startup/Shutdown** screen.



Chapter 7: Software installation

Software installation checklist

Ensure to follow the sequence mentioned in this checklist for the software installation.

#	Action	Link/Notes	✔
1	Install Avaya Diagnostic Server base software.	See Installing Avaya Diagnostic Server in the unattended mode on page 27.	
2	Install available latest Avaya Diagnostic Server service pack.	See Installing a service pack in the unattended mode on page 44.	
3	Configure SAL Gateway using the SAL Gateway user interface.	See *Administering Avaya Diagnostic Server SAL Gateway*.	

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.

You can find the Avaya Diagnostic Server installer at the `/installer` directory on the virtual machine.

Note:

The Avaya Diagnostic Server virtual appliance supports only the unattended mode of installation.

Before you begin

Update the `ADS_Response.properties` file with the required input responses for the installation properties and the preferences. You must replace the default or representative values in the file with values that suit the installation environment. The 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`, and `SMTP_ADMIN_EMAIL` 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 virtual machine on which you want to install Avaya Diagnostic Server using the administrator's credentials.
2. Change the user to root using the **`su root`** command.
3. Go to the `/installer` directory where the Avaya Diagnostic Server software package is available.
4. Run the following command to extract the installer files:

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

   The command extracts a directory `ADS-Installer-<version_no>-<build_no>`.
5. Change directory to `ADS-Installer-<version_no>-<build_no>`.
6. Open the `ADS_Response.properties` file in a Linux text editor, and update the file with the required input responses for the installation properties and the preferences.
7. From the `ADS-Installer-<version_no>-<build_no>` directory, 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.

Next steps

Install the latest Avaya Diagnostic Server service pack available.

Related links

ADS_Response.properties file on page 29

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.

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

Information in the file	Description
`#Agree ADS end user license agreement` `ADS_AGREELICENSE=n`	To continue with the installation, change the value to `y`. **Important:** Ensure that you read the End User License Agreement (EULA) for installing and using Avaya Diagnostic Server. The complete EULA text is available in the `README.txt` file in the installer directory, `ADS-Installer-<version_no>-<build_no>`.
`#Following value will tell the installer which component to be installed (1) SAL gateway, 2) SLA Mon server, 3) Both` `ADS_COMPONENT_TO_INSTALL=1`	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 3.0 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 3.0 component SAL is already installed do you wish to install SLAMon (y/n)`
`ADS_SLAMON_INSTALL=y`
`# ADS 3.0 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 2.5 to 3.0. 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.	

Table continues…

Information in the file	Description
`#ADS [1.0/2.x] component SAL is already installed. Which components to be installed 1) Upgrade SAL 2) Upgrade SAL and Install SLAMON ADS_SAL_UPGRADE=1`	To upgrade from Avaya Diagnostic Server 2.5 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`
`#ADS [1.0/2.x] component SLAMon is already installed. Which components to be installed 1) Upgrade SLAMon 2) Upgrade SLAMon and Install SAL ADS_SLAMON_UPGRADE=1`	To upgrade from Avaya Diagnostic Server 2.5 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`
`#ADS [1.0/2.x] components SAL and SLAMon are already installed Do you wish to Upgrade SAL and SLAMon. (y/n) ADS_SAL_SLAMON_UPGRADE=y`	When you have Avaya Diagnostic Server 2.5 with both components on the host, set the value of `ADS_SAL_SLAMON_UPGRADE` as `y` to upgrade to Avaya Diagnostic Server 3.0. **Note:** If some earlier versions of SAL Gateway and SLA Mon server are installed on the host, set this property as `y` to upgrade both components as part of Avaya Diagnostic Server 3.0. The installer does not support upgrade of only one component when both components are installed.

Table continues…

Information in the file	Description

`#Following properties are for upgrade scenarios.`
 	
`# SAL 2.0, 2.1, or 2.2 is installed. Which component to be installed 1) Upgrade SAL 2) Upgrade SAL and install SLAMon.`
`SAL_UPGRADE_TO_ADS=1`
	To upgrade from SAL 2.x to Avaya Diagnostic Server 3.0, set the value of `SAL_UPGRADE_TO_ADS` to one of the following:
	• For only SAL upgrade, the value must be `1`.
	Example: `SAL_UPGRADE_TO_ADS=1`
	• For SAL upgrade and SLA Mon installation, the value must be `2`.
	Example: `SAL_UPGRADE_TO_ADS=2`
	Note:
	You can ignore this property because upgrade is supported only from Avaya Diagnostic Server 2.5 to 3.0.

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

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 [2.5] 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 2.5 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 [2.5] 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 2.5 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 [2.5] 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 2.5 is installed with the SLA Mon component. To continue with the upgrade even if the host does not meet one or more minimum hardware requirements for Avaya Diagnostic Server with SLA Mon, set the value as `y`. If you keep the value as `n`, the installer quits the upgrade process when a minimum hardware check fails.
`# SAL 2.0, 2.1, or 2.2 is installed. Do you want to proceed with upgrade of SAL if minimum hardware checks fail. (y/n) SAL_UPGRADE_TO_ADS_PROCEED_ON_HW_CHECKS_FAIL=n`	The installer uses this property when SAL Gateway 2.0, 2.1, or 2.2 is installed on the host. To continue with the upgrade even if the host does not meet one or more minimum hardware requirements for Avaya Diagnostic Server with SAL Gateway, set the value as `y`. If you keep the value as `n`, the installer quits the upgrade process when a minimum hardware check fails. **Note:** You can ignore this property because upgrade is supported only from Avaya Diagnostic Server 2.5 to 3.0.
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.	

Table continues…

Information in the file	Description
`#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.
`#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.

Table continues…

Information in the file	Description
`# Proceed with installation of SAL if recommended requirement for RAM is not met (y/n)` `ADS_SAL_PROCEED_ON_RAM_CHECK_FAIL=n`	The installer uses this property when you choose to install Avaya Diagnostic Server with SAL Gateway only. You can set the property as the following: • `ADS_SAL_PROCEED_ON_RAM_CHECK_FAIL=y`: To continue with the installation of SAL Gateway if RAM is less than the recommended 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.
`# 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.

Table continues…

Information in the file	Description
`#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. You can take the backup by using a utility that comes with the 3.0 software package. You can run this utility only on Avaya Diagnostic Server 2.5 or later. For more information, see Chapter 8, Migration of Avaya Diagnostic Server.
The following are responses that the installer uses while installing the SLA Mon server component. If you choose to install the Avaya Diagnostic Server with SAL Gateway only, keep the default values.	
`#Importing SLAMon public key into RPM database (y/n)` `IMPORTKEY=y`	Keep the default value `y`.

`#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`.

Table continues…

Information in the file	Description

`#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.

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

`# If following values are true then Gateway Installer update the IPTABLE and SYSLOG`
`# For RHEL 6.x and 7.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.

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

`Avaya Enterprise Configuration mandatory fields`
`PRIMARY_AVAYA_ENTERPRISE_IDENTIFIER=Enterprise-production`
`PRIMARY_AVAYA_ENTERPRISE_URL=secure.alarming.avaya.com`
`PRIMARY_AVAYA_ENTERPRISE_PORT=443`
`PRIMARY_REMOTE_ENTERPRISE_URL=remote.sal.avaya.com`
`PRIMARY_REMOTE_ENTERPRISE_PORT=443`
	Unless explicitly instructed, do *not* change the default values of these properties.

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.

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-3.0.0.0-103/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.
`BYPASS_ALARMREMOTESERVER_CHECKS=false`	Unless explicitly instructed by Avaya, do *not* change the default value of this property. SAL Gateway 3.0 does not support any Core Server and Remote Server of BusinessPartners. When value of the property is `false`, which is the default value, and the installed version of SAL Gateway is configured to communicate with such non-Avaya Core Server or Remote Server, the installer exits the upgrade process.

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.

Installing a service pack in the unattended mode

About this task

You can install a Avaya Diagnostic Server service pack on the Avaya Diagnostic Server virtual appliance by running the installer in the unattended mode.

You can find the Avaya Diagnostic Server Service Pack 1 installer at the `/installer` directory on the virtual machine.

Note:

The Avaya Diagnostic Server virtual appliance supports only the unattended mode of installation.

Procedure

1. Log on to the virtual machine on which Avaya Diagnostic Server is installed as an administrator.
2. Change the user to root using the **su root** command.
3. Go to the `/installer` directory where the service pack is available.
4. Run the following command to extract the Release 3.0 service pack 1 installer files:

   tar `-xvf ADS-ServicePack-3.0.1.0-494.tar.gz`

   The command extracts the directory `ADS-ServicePack-3.0.1.0-494`.
5. Change the directory to `ADS-ServicePack-3.0.1.0-494`.
6. Open the `ADS_Response.properties` file in a text editor, and agree to the end user license agreement by changing the value of `ADS_AGREELICENSE` to `y`.
7. Run the following command to start the installation in the unattended mode:

   ./install.sh `-unattended`

   After a successful installation of the service pack, the system sends an email indicating the installation status to the SAL Gateway administrator.

Chapter 8: Post-installation verification and testing

Verification of the SAL Gateway implementation

You can run a number of tests to verify that the implementation of the SAL Gateway component of Avaya Diagnostic Server is successful. The verification involves ensuring that the SAL Gateway services, which include alarming, remote access, SAL Watchdog, and SAL Gateway UI, are running properly.

Testing the alarming service of SAL Gateway

About this task

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

Procedure

1. Log on to the Avaya Diagnostic Server virtual appliance as admin, and switch to the root user.
2. Run the following command, and check the outcome of the command:

   ```
   systemctl status spiritAgent
   ```

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

   ```
   systemctl start spiritAgent
   ```

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

Testing the SAL Gateway UI

About this task

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

Procedure

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

   `https://<IP address of the SAL Gateway virtual appliance>:7443`

   If the host server is registered under DNS, you can replace the host IP with the DNS host name.

   If you configured to use an OOBM network during the OVA deployment, the IP address of SAL Gateway is configured as the OOBM IP address. In such case, use the OOBM IP address in the URL.

   The browser must display the SAL Gateway login page.
3. If the SAL Gateway login page does not open, perform the following:
   a. Log on to the SAL Gateway virtual machine as admin, and switch to the root user.
   b. Run the following command to check the status of the gatewayUI service:

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

      `systemctl start gatewayUI`
   d. Check the status again to verify that the service is running properly.

Testing the SAL Watchdog service

About this task

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

Note:

Until Release 2.5, SALWatchdog used to run as a service. From Release 3.0 onwards, SAL Watchdog is run as a cron job at every 5 minutes.

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`
3. Check when the cron job was run the last time.

Note:

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

Example

```
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)
```

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 that the SLA Mon server service is running.

Procedure

1. Log on to the Avaya Diagnostic Server virtual machine as admin, and switch to the root user.
2. Run the following command and check the outcome of the command:

   `systemctl status slamonsrvr`

   Expected output sample:

   ```
   slamonsrvr Running
   ```

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

   `systemctl start slamonsrvr`

Testing the slamonweb service

About this task

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

Procedure

1. Log on to the Avaya Diagnostic Server virtual machine as admin, and switch to the root user.
2. Run the following command and check the outcome of the command:

   systemctl status slamonweb

   Expected output sample:

   ```
   slamonweb (pid 19669) is running...
   ```

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

   systemctl start slamonweb

Testing the slamondb service

About this task

Use this procedure to confirm that the database service for the SLA Mon server is running.

Procedure

1. Log on to the Avaya Diagnostic Server virtual machine as admin, and switch to the root user.
2. Run the following command and check the outcome of the command:

   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 the following command to start the service:

   systemctl start slamondb

Chapter 9: Postinstallation customer responsibilities

The customer owns the following postinstallation responsibilities:

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

Chapter 10: Upgrading Avaya Diagnostic Server virtual appliance

Upgrade from SAL Gateway 2.2 virtual appliance

A direct upgrade from an existing SAL Gateway virtual appliance to an Avaya Diagnostic Server virtual appliance is not supported. Instead, you can migrate data from the SAL Gateway 2.2 virtual appliance to the Avaya Diagnostic Server 3.0 virtual appliance. The migration process involves manual operations of exporting data, deploying the Release 3.0 OVA, and importing the exported data to the new virtual appliance.

Related links

Migration checklist for SAL Gateway 2.2 virtual appliance on page 51

Migration checklist for SAL Gateway 2.2 virtual appliance

The following checklist provides the steps to migrate from SAL Gateway 2.2 virtual appliance to the Avaya Diagnostic Server 3.0 virtual appliance:

No.	Task	Description	✔
1	Log on to the SAL Gateway 2.2 user interface.	Access the SAL Gateway user interface by opening the following URL on a web browser: `https://<SALGateway_VM_IP_address>:7443/`	
2	Through the SAL Gateway user interface, export the managed element data configured on the existing SAL Gateway to a .csv file.	On the Managed Element page, click **Export**, and save the .csv file to a folder on your local computer. For more information, see Exporting managed element data on page 53.	

Table continues…

No.	Task	Description	✔
3	Deploy the Avaya Diagnostic Server 3.0 OVA.	See Chapter 5, Deploying the Avaya Diagnostic Server OVA. **Important:** For an upgrade or migration operation, deploy the target server with the same IP address and host name as in the old server.	
4	On the new virtual appliance, install Avaya Diagnostic Server 3.0 with the SAL Gateway component.	If required, you may choose to install the SLA Mon™ server component also. After the Avaya Diagnostic Server 3.0 installation, install the available service pack 1 for 3.0. See Chapter 7, Software installation.	
5	Take the older version of SAL Gateway offline.	Through Solution Deployment Manager or vCenter, stop or delete the virtual machine. **Note:** Do *not* use the uninstaller script to uninstall SAL Gateway on a virtualized environment.	
6	Log on to the user interface of the new SAL Gateway 3.0 instance.		
7	Through the SAL Gateway user interface, import the .csv file that contains the managed element data that was exported from the earlier instance of SAL Gateway.	See Importing managed elements to SAL Gateway on page 54.	

Table continues…

No.	Task	Description	✔
8	Verify the configuration details of the imported managed elements.	Do the following as required: • If the model associated with an imported device supports multiple products, ensure that the correct product type is selected for that managed element. When the model supports multiple products, the device is added to SAL Gateway with the default product for that model. For example, if the model assigned to the device is CM_Media_Server_<version>, this model supports more than one product. When imported, the device is added as CM Media Server, which is the default product for the model. Edit the configuration of such managed devices to select the correct product. • Wherever required, make the changes to device configuration related to SNMP v3, inventory collection, and device credentials for inventory collection.	
9	Validate the migration.	See Validating an upgrade operation on page 61.	

Related links

Upgrade from SAL Gateway 2.2 virtual appliance on page 51

Exporting managed element data

About this task

You can export the managed element data configured on SAL Gateway to your local system. You can import the exported data to a different SAL Gateway, for example, when setting up a second SAL Gateway for redundancy.

The export functionality is supported on SAL Gateway release 2.x onwards. You can import data exported from SAL Gateway 2.x and later to SAL Gateway release 3.0 and later.

Procedure

1. On the main menu of the SAL Gateway user interface, click **Devices** > **View/Search**.
2. On the Managed Element page, click **Export**.

   The system exports the data related to the managed elements to a comma separated values (.csv) file.
3. Save the .csv file to a folder on your local computer.

You can open the .csv file using Microsoft Excel.

The .csv file contains the following details about the managed elements:

- Host Name
- Solution Element ID
- Model
- IP Address
- Remote Access
- Product ID
- Alarm Flag
- Last Inventory
- Inventory Collection Hours

The following configuration details related to the managed elements are not exported to the .csv file:

- SNMP v3 details, if configured.
- Inventory collection enablement configuration.
- Device credentials configured for inventory collection, if any.

Importing managed elements to SAL Gateway

About this task

You can use a comma separated values (.csv) file that contains the configuration data of managed elements to import the managed elements to SAL Gateway.

The import functionality is supported on SAL Gateway release 3.0 onwards. You can import data exported from SAL Gateway 2.x and later to SAL Gateway 3.0 and later.

You can export the configuration data of managed elements from one SAL Gateway instance and import the data to another SAL Gateway instance. For example, when setting up a second SAL Gateway for redundancy, you can import the data exported from the first SAL Gateway to the second one. You can also import the .csv file to the same SAL Gateway to retrieve the managed element configurations. You can import the exported .csv file data as it is or, if required, you can modify, delete, or add entries in the file.

Before you begin

Ensure the following:

- The .csv file, which contains the information of the devices you want to import, is available on the system from where you are accessing SAL Gateway.
- The device information in the .csv file are correct and complete. SAL Gateway does not import the devices with incomplete or incorrect information.

You can open and edit the .csv file using Microsoft Excel. The .csv file contains the following details about the devices:

- Host Name
- Solution Element ID
- Model
- IP Address
- Remote Access
- Product ID
- Alarm Flag
- Last Inventory
- Inventory Collection Hours

Import of devices using the .csv file does not import the following configuration details related to the devices:

- SNMP v3 details.
- Inventory collection enablement flag.
- Device credentials for inventory collection.
- The product type when the model supports more than one products and the product is not the default product for that model.

After the import operation, you must therefore verify the configurations of the devices. Wherever required, make the necessary changes to the mentioned configurations from the respective pages on the user interface.

Procedure

1. On the main menu of the SAL Gateway user interface, click **Devices** > **View/Search**.
2. On the Managed Element page, click **Import**.
3. In the Import CSV File window, click **Browse** to locate and select the .csv file that you want to import.
4. Click **Upload**.

   The window displays the number of devices to be imported and their Solution Element IDs. If the file contains some incorrect or incomplete device information, an error summary report is displayed for those Solution Element IDs. SAL Gateway does not import the devices with incomplete or incorrect information.
5. **(Optional)** For the Solution Element IDs with error messages, correct the information in the .csv file and upload the file again.
6. Click **Apply**.

   The devices that pass the validation checks are imported to SAL Gateway as managed elements.

   If the .csv file contains the Solution Element ID of SAL Gateway and its configuration details in the file are different from the existing configuration, those changes are not

applied. To change the SAL Gateway configuration, you can navigate to the Gateway Configuration page. If the file contains a record of any other SAL Gateway instance, then that record is not imported.

7. Verify the configuration details of the imported managed elements, and do the following as required:
   a. **(Optional)** If the model associated with an imported device supports multiple products, ensure that the correct product type is selected for that managed element.

      When the model supports multiple products, the device is added to SAL Gateway with the default product for that model. For example, if the model assigned to the device is CM_Media_Server_<version>, this model supports more than one product. When imported, the device is added as CM Media Server, which is the default product for the model. Edit the configuration of such managed devices to select the correct product.

   b. **(Optional)** Wherever required, make the configuration changes related to SNMP v3, inventory collection, and device credentials for inventory collection.

Upgrade from the Avaya Diagnostic Server 2.0 virtual appliance

Upgrade the SAL Gateway component

To upgrade SAL Gateway, you must export the element data from the existing SAL Gateway instance and import the data to the 3.0 virtual appliance using the SAL Gateway user interface.

Upgrading the SLA Mon™ component

To upgrade SLA Mon™, you must perform a software upgrade from the existing Avaya Diagnostic Server 2.0 to Avaya Diagnostic Server 2.5.

After you upgrade to Avaya Diagnostic Server 2.5, migrate to Avaya Diagnostic Server 3.0 virtual appliance.

Related links

Exporting managed element data on page 53
Importing managed elements to SAL Gateway on page 54
Checklist for migration from Avaya Diagnostic Server 2.5 on page 57

Migrate from Avaya Diagnostic Server 2.5 virtual appliance

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 3.0 comes with a migration utility script. You can use this script to take a backup of Avaya Diagnostic Server 2.5.x. Using the backup file, you can then install Avaya Diagnostic Server 3.0 on a new compatible host.

You can run the script only on Avaya Diagnostic Server 2.5.x. Therefore, you must upgrade any earlier version of Avaya Diagnostic Server or SAL Gateway to Avaya Diagnostic Server 2.5 before you can migrate to another server.

Note:

The migration utility does not support migration from Avaya Diagnostic Server 3.0 to Avaya Diagnostic Server 3.0. You can use the existing backup and restore utility of Avaya Diagnostic Server to migrate Avaya Diagnostic Server 3.0 to another host. See Chapter 9, Backing up and restoring Avaya Diagnostic Server.

Checklist for migration from Avaya Diagnostic Server 2.5

The following checklist provides the high-level steps to migrate from Avaya Diagnostic Server 2.5 to Avaya Diagnostic Server 3.0 on a different server:

No.	Task	Description	✔
1	Ensure that you have upgraded to Avaya Diagnostic Server 2.5 on the current host server.	The migration utility script that you need to run for backup is supported on Avaya Diagnostic Server 2.5.x only.	

Table continues…

No.	Task	Description	✔
2	Deploy the Avaya Diagnostic Server 3.0 OVA.	See Chapter 5, Deploying the Avaya Diagnostic Server 3.0. The newly deployed virtual machine is the target host for the migration. Do *not* yet install the Avaya Diagnostic Server 3.0 software. **Note:** Maintain the new server on a private network until you complete the migration steps.	
3	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 60.	
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 3.0 on the new host.	
5	Start a clean installation of Avaya Diagnostic Server 3.0 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 unattended mode on page 60.	

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 in *Deploying Avaya Diagnostic Server*. 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 *Deploying Avaya Diagnostic Server*.	
8	Take the old server offline, or at least stop all services related to Avaya Diagnostic Server on the server.		
9	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 2.5 using the migration utility. You can use the backup file to migrate Avaya Diagnostic Server to a different server as Avaya Diagnostic Server 3.0.

Before you begin

- Ensure that the Avaya Diagnostic Server version is 2.5.x. The migration utility script that you need to run for backup is supported on Avaya Diagnostic Server 2.5.x only. For any earlier version, upgrade to Avaya Diagnostic Server 2.5 before you run the migration utility.
- Ensure that you extract a copy of the Avaya Diagnostic Server 3.0 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 2.5 instance as root.
2. Navigate to the extracted directory from the Avaya Diagnostic Server 3.0 software package, 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 2.5 host, the backup file created is `ADS_2.5_backup.tar`
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 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 3.0.

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.

Note:

The `ADS_Response.properties` 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.

Procedure

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

   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.

Next steps

Log on to the web interfaces of the Avaya Diagnostic Server components to validate that the configuration information persists after the migration. If you do not see the migrated SLA Mon agents online, restart all SLA Mon services. For more information about configuring SNMP, see *Deploying Avaya Diagnostic Server* and *Administering Avaya Diagnostic Server SAL Gateway*. Update the IP tables rules for the communication ports used by SAL Gateway and SLA Mon server.

Validating an upgrade operation

After you upgrade from a SAL Gateway virtual appliance to an Avaya Diagnostic Server virtual appliance, you must check whether the network configuration and the SAL Gateway configuration are properly restored. Additionally, you must check that all the services are running on the new virtual machine.

About this task

Use the following steps to validate that the upgrade process is successful.

Procedure

1. Log on to the Avaya Diagnostic Server virtual machine as admin, and switch to the root user.
2. Run the following command to check the version of the new Avaya Diagnostic Server virtual appliance:

   `swversion -v`

The version number of the Avaya Diagnostic Server virtual appliance is Avaya Diagnostic Server 3.0.

3. Run the following commands to view and verify that the network configuration parameters, including IP address and host name, are restored properly:

   ifconfig

   hostname

   less /etc/hosts

4. Run the following commands to verify that the SAL Gateway services are up and running:

   systemctl status spiritAgent

   systemctl status gatewayUI

5. Log on to the SAL Gateway web interface, and check the SAL Gateway configuration.
6. Run the following commands to verify that the SLA Mon services are up and running:

   systemctl status slamonsrvr

   systemctl status slamondb

   systemctl status slamonweb

   To report a problem with the upgrade operation or to contact Avaya Support for assistance, visit the Avaya Support website at http://support.avaya.com.

Chapter 11: Maintenance procedures

Backup and restore overview

You can use the backup and restore capabilities of the virtual machines that run on VMware for long-term backup and recovery of the Avaya Diagnostic Server virtual machine.

As a customer, you have the responsibility to run the backup at periodic intervals. Alternatively, you can schedule a job to run the backup at a periodic interval and copy the backup archive to an external system for preserving the data in the event of a system failure.

Backing up the virtual machine

About this task

Use this procedure to back up the virtual machine.

Procedure

1. Open a virtual machine console, or connect to the virtual machine using an SSH client.
2. Log in as admin, and switch to the root user.
3. Run the following command:

   `backup`

   The system displays the directory location where the backup archive is saved.

   You can find the latest backup archive file at the `/vm-data/backup/archives/` directory. The archive file is saved with a file name similar to `vmbackup_xxxxxxxx.tar.gz`.
4. Copy the backup archive to an external server to prevent loss of data in the event of a system failure.

   To copy the file to a remote server, you can use the following methods:

   - To a Linux remote system: Use the Linux **`scp`** command.

     `scp` *<archive_file> <username>@<remote_server_ip>:<directory_path>*
   - To a Windows remote system: Use WinSCP or a similar file transfer utility.

5. **(Optional)** To use WinSCP to transfer a backup file, ensure that the backup file has the right ownership or permissions. As direct login to the virtual appliance as root is not allowed, perform the following as the root user before using WinSCP:
   a. Copy the backup file to the `/tmp` directory.
   b. From the `/tmp` directory, run the following command to change the file permissions:

      chmod 644 <backup_filename>

      You can now use WinSCP to connect and log in to the virtual appliance as an administrator user and copy the file from the `/tmp` directory.

Restoring a virtual machine from a backup

About this task

Use this procedure to restore a virtual machine from a backup archive.

Procedure

1. Deploy the virtual machine.

   Important:

   While deploying the new virtual machine, configure the same host name as the earlier virtual appliance that you want to restore.
2. Start the virtual machine.
3. Log on to the virtual machine as admin, and switch to the root user.
4. Copy the backup archive file to a directory on the virtual machine.

   To copy the file from a remote system, you can use the following methods:

   - From a Linux remote system: Use the Linux **scp** command.

     scp *<user>@<VM_IP_or_hostname>:<file_path on remote_server>*

   - From a Windows remote system: Use WinSCP or a similar file transfer utility.
5. From the virtual machine console, run the following command:

   restore *<Archive_file_path_on_VM>*

Creating a snapshot

Caution:

Do not perform any activity on the virtual application until the snapshot backup is complete. Snapshot operations can adversely affect service.

Before you begin

Verify with the system administrator that the required privilege **Virtual machine.State.Create snapshot** is available on the virtual machine.

Note:

Differences exist between the vSphere Web Client versions. You might need to modify the following steps accordingly.

Procedure

1. To select a virtual machine using the vSphere Web Client:
   a. Search for a virtual machine and select it from the search results list.
   b. Stop the application that is running on the virtual machine or make the application out-of-service.
   c. Right-click the virtual machine and select **Snapshot** > **Take Snapshot**.
2. To select a virtual machine using the vSphere Client:
   a. Stop the application that is running on the virtual machine or make the application out-of-service.
   b. Click **Inventory** > **Virtual Machine** > **Snapshot** > **Take Snapshot**.
3. In the **Name** field, enter a name for the snapshot.
4. In the **Description** field, enter a description for the snapshot.
5. Disable **Snapshot the virtual machine's memory**.
6. Enable **Quiesce guest file system (Needs VMware Tools installed)**.
7. Click **OK**.

   The system displays `Completed` when the snapshot backup is complete.

Restoring a snapshot

Use this procedure to return the memory, settings, and state of the virtual machines to the state when you took the snapshot. The power and data states of the virtual machines return to the state when you took the parent snapshot.

Important:

Do not perform any activity on the virtual application until the snapshot restoration is complete.

Before you begin

Verify with the system administrator that the required privilege **Virtual machine.State.Revert to snapshot** is available on the virtual machine.

Note:

Differences exist between the vSphere Web Client versions. You might need to modify the steps accordingly.

Procedure

1. Click **Inventory** > **Virtual Machine**.
2. Right-click the virtual machine name on which you want to restore the snapshot, and click **Snapshot**.
3. Open **Snapshot Manager**.
4. Select the snapshot version that you want to restore.
5. Click **Go to**.
6. In the **Recent Tasks** window, verify the **Status** of the **Revert snapshot** task.

   Wait until the message `Completed` displays.

Chapter 12: Troubleshooting

Replace with your title

FAQ

Q.	Do I require a console access while rebooting the Avaya Diagnostic Server virtual machine?
A.	No. A console access is not necessary while you reboot the virtual machine. However, depending on the deployment scenario and the user needs, having a console access can be useful. If the Avaya Diagnostic Server virtual appliance was deployed through vCenter, then you do not require a console access during the rebooting. If the Avaya Diagnostic Server virtual appliance was deployed directly on an ESXi host using a vSphere client, then with a console access, you can reconfigure the virtual appliance during the boot process. When you reboot a Avaya Diagnostic Server virtual appliance that is deployed directly on an ESXi host, a script runs during the boot process that waits for user inputs. You can utilize the script to reconfigure the virtual appliance. The script waits for user input for 30 seconds before proceeding with the normal boot process. If you do not provide input within 30 seconds, the script considers that you do not want to reconfigure the virtual appliance. To be able to utilize the script, you require a console access. In absence of a console access, the script waits for 30 seconds and then continues with the normal boot process. This process is applicable only in the case of direct deployment.
Q.	How do I manage the system date and time?
A.	The Avaya Diagnostic Server virtual appliance uses NTP to synchronize the system time with an NTP server. For information about configuring NTP servers on the Avaya Diagnostic Server virtual appliance, see Configuring timing on page 75.
Q.	Can I use the Ethernet interface other than eth0 for the Avaya Diagnostic Server virtual appliance?
A.	No. Currently the Avaya Diagnostic Server virtual appliance can work only with eth0.
Q.	Can I use DHCP for the network parameters for the Avaya Diagnostic Server virtual appliance?

Table continues…

A.	Even though the Avaya Diagnostic Server virtual appliance supports DHCP, Avaya does not recommend using DHCP for the Avaya Diagnostic Server virtual appliance. The Avaya Diagnostic Server virtual appliance might have SAL Gateway running on the machine, which onboards the devices in the customer network. For onboarding, SAL Gateway uses the IP address of the virtual machine. If you use DHCP for configuring the network parameters of the virtual machine, then chances are that the IP address of the virtual machine might change. In such cases, you must again onboard all the devices, which were already onboard, one by one with the new IP address. Configure static parameters for the networking of the Avaya Diagnostic Server virtual appliance so that you do not encounter similar issues.
Q.	I have installed the Avaya Diagnostic Server virtual appliance using DHCP through vCenter. How do I change to static configuration?
A.	Perform the following steps to apply static configuration for networking to the Avaya Diagnostic Server virtual appliance installed using vCenter: 1. Open a virtual machine console, or connect to the virtual machine through an SSH client. 2. Log in as admin, and switch to the root user. 3. Run the following command: `/opt/vmware/share/vami/vami_ovf_process -s eth0` 4. Shut down the virtual machine using the vCenter administration. 5. Edit the virtual machine settings. 6. Provide static configuration for the networking parameters in the Properties page. 7. Start the virtual machine using the vCenter administration.
Q.	Why do I get an `VM communication interface: [FAILED]` error on the virtual machine console during the first boot?
A.	Ignore these errors. During the first boot, the system recreates the initial ram disk (initrd) to include the VMware Tools modules, which causes these errors. These errors have no service impact. The errors do not occur on subsequent reboots.
Q.	Why do I get an `Unloading iptables modules: [FAILED]` error during the restore operation?
A.	Ignore this error. Apart from the SAL Gateway services, other processes in the Avaya Diagnostic Server virtual appliance use the iptables modules. During the restore process, the system tries to restart the iptables service. The restart attempt fails because these shared modules cannot be unloaded while other processes are still running. Failure to unload the iptables modules has no service impact.
Q.	How do I find the version of the Avaya Diagnostic Server virtual appliance?

Table continues…

A.	Perform the following steps to find the version of the Avaya Diagnostic Server virtual appliance: 1. Open a virtual machine console, or connect to the virtual machine through an SSH client. 2. Log in as admin. 3. Run the following command: **`sudo swversion`** The system displays a verbose output. 4. To see only the version of SAL Gateway, run the following command: **`sudo swversion -s`** 5. To see only the version of the SLA Mon server, run the following command: **`sudo swversion -l`** 6. To see only the version of the Avaya Diagnostic Server virtual appliance, run the following command: **`sudo swversion -v`** 7. To see only the version of the Avaya Diagnostic Server software, run the following command: **`sudo swversion -a`**
Q.	I got an error while running the **`restore`** command. What should I do?
A.	Try to run the **`restore`** command again. If the error persists, visit the Avaya Support website at http://support.avaya.com to contact Avaya.
Q.	Why pressing Control+C does not work during the configuration of the virtual machine on the virtual machine console?
A.	The script for configuring network parameters for a direct deployment on an ESXi host indicates that pressing Control+C opens the main menu. However, this script runs while the virtual machine is still booting. Therefore, the Control+C key press sequence does not work. This issue is a known issue.
Q.	Will there be any service outage if I run the storage or host vMotion?
A.	Running the storage or host vMotion does not affect any service that is currently running on the Avaya Diagnostic Server virtual appliance. Any remote connections created before running the storage or host vMotion continue to work. However, when the storage or host vMotion is in progress, you might not be able to establish new remote connections to managed devices. This outage lasts only until the storage or host vMotion is complete. After the storage or host vMotion completes successfully, you can establish new connections.

Chapter 13: 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
Design		
Avaya Aura® Virtualized Environment Solution Description	Describes the virtualized environment solution from a functional view. Includes a high-level description of the solution, topology diagrams, customer requirements, and design considerations.	Sales engineers, solution architects, and implementation engineers
Implementation		
Deploying Avaya Diagnostic Server	Describes the implementation requirements and procedures to deploy Avaya Diagnostic Server in a non-virtualized environment.	Sales engineers, solution architects, implementation engineers, and customers
Deploying Avaya Diagnostic Server using Avaya Aura® System Manager in the VMware Virtualized Environment	Describes the implementation requirements and procedures to deploy Avaya Diagnostic Server in Avaya Aura® virtualized environment.	Sales engineers, solution architects, implementation engineers, and customers
Administration		
Administering Avaya Diagnostic Server with SLA Mon™	Provides information about configuring and administering Avaya Diagnostic Server for the remote diagnostics of Avaya endpoints and network condition monitoring through the SLA Mon server.	Solution architects, implementation engineers, support personnel, and customers
Administering Avaya Diagnostic Server with SAL Gateway	Provides information about configuring and administering SAL Gateway for remote servicing and alarm transfer facilities of Avaya products at a customer site.	Solution architects, implementation engineers, support personnel, and customers

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.

Appendix A: VMware best practices for performance

The following sections define the required best practices for the Avaya Diagnostic Server virtualization environment. For standard virtualization best practices for VMware vSphere 5.0, see Performance Best Practices for VMware vSphere 5.0. For standard virtualization best practices for VMware vSphere 5.1, see Performance Best Practices for VMware vSphere 5.1.

BIOS

For optimal performance, turn off power saving server options. See the technical data provided by the manufacturer for your particular server regarding power saving options.

For information about how to use BIOS settings to improve the environment for latency-sensitive workloads for an application, see the technical white paper at http://www.vmware.com/files/pdf/techpaper/VMW-Tuning-Latency-Sensitive-Workloads.pdf.

The following sections describe the recommended BIOS settings for:

- Intel Virtualization Technology
- Dell PowerEdge Servers
- HP ProLiant Servers

Intel Virtualization Technology

Intel CPUs require EM64T and Virtualization Technology (VT) support in the chip and in the BIOS to run 64–bit virtual machines.

All Intel Xeon processors include:

- Intel Virtualization Technology
- Intel Extended Memory 64 Technology
- Execute Disable Bit

Ensure that VT is enabled in the host system BIOS. The feature is also known as VT, Vanderpool Technology, Virtualization Technology, VMX, or Virtual Machine Extensions.

Note:

The VT setting is locked as either **On** or **Off** when the server starts. After enabling VT in the system BIOS, save your changes to the BIOS settings and exit. The BIOS changes take effect after the host server reboots.

Other suggested BIOS settings

Servers with Intel Nehalem class and newer Intel Xeon CPUs offer two more power management options: C-states and Intel Turbo Boost. These settings depend on the OEM make and model of the server. The BIOS parameter terminology for current Dell and HP servers are described in the following sections. Other server models might use other terminology for the same BIOS controls.

- Disabling C-states lowers latencies to activate the CPUs from halt or idle states to a fully active state.
- Intel Turbo Boost steps up the internal frequency of the processor if the workload requires more power. The default for this option is **enabled**. Do not change the default.

Dell PowerEdge Server

When the Dell server starts, press F2 to display the system setup options.

- Set the Power Management Mode to **Maximum Performance**.
- Set the CPU Power and Performance Management Mode to **Maximum Performance**.
- In Processor Settings, set:
  - **Turbo Mode** to **enable**.
  - **C States** to **disabled**.

HP ProLiant Servers

The following are the recommended BIOS settings for the HP ProLiant servers:

- Set the Power Regulator Mode to **Static High Mode**.
- Disable **Processor C-State Support**.
- Disable **Processor C1E Support**.
- Disable **QPI Power Management**.
- Enable **Intel Turbo Boost**.

VMware Tools

The VMware Tools utility suite is built into the application OVA. The tools enhance the performance of the guest operating system on the virtual machine and improve the management of the virtual machine.

VMware tools provide:

- VMware Network acceleration
- Host to Guest time synchronization
- Disk sizing

For more information about VMware tools, see *Overview of VMware Tools* at http://kb.vmware.com/kb/340.

Important:

Do not upgrade the VMware tools software that is packaged with each OVA unless instructed to do so by Avaya. The supplied version is the supported release and has been thoroughly tested.

Timekeeping

For accurate timekeeping, use the Network Time Protocol (NTP) as a time source instead of the ESXi hypervisor.

The NTP servers can be local or over the Internet. If the NTP servers are on the Internet, the corporate firewall must open UDP port 123 so that the NTP service can communicate with the external NTP servers.

The VMware tools time synchronization method is disabled at application deployment time to avoid dueling clock masters. You must configure the NTP service first because the applications are not receiving clock updates from the hypervisor. To verify that VMware Tools Timesync is disabled, run the command `/usr/bin/vmware-toolbox-cmd timesync status`.

In certain situations, the ESXi hypervisor pushes an updated view of its clock into a virtual machine. These situations include starting the virtual machine and resuming a suspended virtual machine, If this view differs more than 1000 seconds from the view that is received over the network, the NTP service might shutdown. In this situation, the guest OS administrator must manually set the guest clock to be the same or as close as possible to the network time source clock. To keep the NTP service active, the clock on the ESXi host must also use an accurate clock source, such as the same network time source that is used by the guest operating system. The VMware recommendation is to add **tinker panic 0** to the first line of the **ntp.conf** file so that the NTP can adjust to the network time even with large differences.

If you use the names of the time servers instead of the IP address, you must configure the Domain Name Service in the guest OS before you administer the NTP service. Otherwise, the NTP service

cannot locate the time servers. If you administer the NTP service first, you must restart the NTP service after administering the DNS service.

After you administer the NTP service in the application, run the `ntpstat` or `/usr/sbin/ntpq -p` command from a command window. The results from these commands:

- Verify if the NTP service is getting time from a network time source.
- Indicate which network time source is in use.
- Display how closely the guest OS matches the network time.
- Display how often the guest OS checks the time.

The guest OS polls the time source every 65 to 1024 seconds. Larger time intervals indicate that the guest clock is tracking the network time source closely. If the time source is **local**, then the NTP service is not using a network time source and a problem exists.

If the clock value is consistently wrong, look through the system log for entries regarding **ntpd**. The NTP service writes the activities it performs to the log, including when the NTP service loses synchronization with a network time source.

For more information, see *Timekeeping best practices for Linux guests* at http://kb.vmware.com/kb/1006427. The article presents best practices for Linux timekeeping to achieve best timekeeping results. The article includes:

- specifics on the particular kernel command line options to use for the Linux operating system of interest.
- recommended settings and usage for NTP time sync, configuration of VMware Tools time synchronization, and Virtual Hardware Clock configuration.

Configuring timing

The Avaya Diagnostic Server virtual machine relies on NTP for timekeeping. The Avaya Diagnostic Server virtual machine has an *NTP* service running that you can configure to synchronize with an external NTP server.

Important:

To maintain the system time of the Avaya Diagnostic Server virtual machine, you must configure NTP on the Avaya Diagnostic Server virtualized environment. Timekeeping is also important for managing and isolating alarms that SAL Gateway forwards.

About this task

Use this procedure to configure the NTP service on the Avaya Diagnostic Server virtual machine.

Procedure

1. Connect to the virtual machine through an SSH client.
2. Log in as admin, and switch to the root user.
3. Run the following command to stop the NTP service:

```
service ntpd stop
```

4. Open the `/etc/ntp.conf` file in a text editor.
5. Add the following line at the top of the file:

```
tinker  panic  0
```

6. If you do not want to use the CentOS NTP servers, comment out the following lines:

```
server  0.centos.pool.ntp.org
server  1.centos.pool.ntp.org
server  2.centos.pool.ntp.org
```

7. After those lines, add the NTP servers for time synchronization as the following:

```
server <IP/hostname>
server <IP/hostname>
```

8. Comment out the following two lines:

```
server  127.127.1.0     # local clock
fudge  127.127.1.0 stratum 10
```

9. Save and close the `/etc/ntp.conf` file.
10. Run the following command to start the NTP service:

```
service ntpd start
```

Next steps

If the NTP servers are on the Internet, you must configure the corporate firewall to open the UDP port 123 so that the NTP service can communicate with the external NTP servers.

VMware networking best practices

You can have many different configurations for networking in a VMware environment. The information in this section includes a number of best practices and recommendations from the perspective of Avaya.

This section is not a substitute for the actual VMware documentation. If you do not have experience with VMware networking, you must review the VMware networking best practices before deploying any applications on an ESXi host.

The following are the suggested best practices for configuring a network that supports applications deployed on VMware hosts:

- Create a vSphere standard or distributed switch with dedicated NICs for each service to achieve greater security and performance. If separate switches are not possible, use port groups with different VLAN IDs.
- Configure the vMotion connection in such as way that the connection is located on a separate network that is devoted to vMotion.
- To protect sensitive VMs, deploy firewalls in the VM that route between virtual networks with uplinks to physical networks and pure virtual networks with no uplinks to physical networks.

- Specify VM NIC hardware type **vmxnet3** for best performance. Avaya .ova files are built using **vmxnet3** by default.
- Connect all physical NICs that are connected to the same vSphere standard or distributed switch to the same physical network.
- Configure all VMkernal vNICs to the same IP Maximum Transmission Unit (MTU).

References

Title	Link
Performance Best Practices for VMware vSphere™ 5.0	http://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.0.pdf
Performance Best Practices for VMware vSphere® 5.1	http://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.1.pdf
VMware vSphere Basics	http://pubs.vmware.com/vsphere-50/index.jsp?topic=%2Fcom.vmware.vsphere.introduction.doc_50%2FGUID-F7A7E6C0-FA25-4806-8921-0438F1B2AEAE.html

Thin vs. thick deployments

When creating a virtual disk file, VMware ESXi uses a thick type of virtual disk by default. The thick disk pre-allocates all of the space specified during the creation of the disk. For example, if you create a 10 megabyte disk, all 10 megabytes are pre-allocated for that virtual disk.

In contrast, a thin virtual disk does not pre-allocate all of the space. Blocks in the VMDK file are not allocated and backed by physical storage until they are written during the normal course of operation. A read to an unallocated block returns zeroes, but the block is not backed with physical storage until it is written. Consider the following when implementing thin provisioning in your VMware environment:

- Thin provisioned disks can grow to the full size specified at the time of virtual disk creation, but do not shrink. Once the blocks have been allocated, they cannot be un-allocated.
- By implementing thin provisioned disks, you are able to over-allocate storage. If storage is over-allocated, thin virtual disks can grow to fill an entire datastore if left unchecked.
- If a guest operating system needs to make use of a virtual disk, the guest operating system must first partition and format the disk to a file system it can recognize. Depending on the type of format selected within the guest operating system, the format may cause the thin provisioned disk to grow to full size. For example, if you present a thin provisioned disk to a Microsoft Windows operating system and format the disk, unless you explicitly select the Quick Format option, the Microsoft Windows format tool writes information to all of the sectors on the disk, which in turn inflates the thin provisioned disk to full size.

Thin provisioned disks can over-allocate storage. If the storage is over-allocated, thin virtual disks can grow to fill an entire datastore if left unchecked. You can use thin provisioned disks, but you must use strict control and monitoring to maintain adequate performance and ensure that storage

is not completely consumed. If operational procedures are in place to mitigate the risk of performance and storage depletion, then thin disks are a viable option.

Best practices for VMware features

VMware Snapshots

A snapshot preserves the state and data of a virtual machine at a specific point in time. You can create a snapshot before upgrading or installing a patch.

The best time to take a snapshot is when no applications in the virtual machine are communicating with other computers. The potential for problems is greatest if the virtual machine is communicating with another computer. For example, if you take a snapshot while the virtual machine is downloading a file from a server on the network, the virtual machine continues downloading the file and communicating its progress to the server. If you revert to the snapshot, communications between the virtual machine and the server are confused and the file transfer fails.

Caution:

Snapshot operations can adversely affect service. Before performing a snapshot operation, you must stop the application that is running on the virtual machine or place the application out-of-service. When the snapshot operation is complete, start or bring the application back into service.

Snapshots can:

- Consume large amounts of data resources.
- Increase CPU loads on the host.
- Affect performance.
- Affect service.

To prevent adverse behaviors, consider the following recommendations when using the Snapshot feature:

- *Do not* rely on VMware snapshots as a robust backup and recovery method. Snapshots are not backups. The snapshot file is only a change log of the original virtual disk.
- *Do not run a virtual machine off of a snapshot.* Do not use a single snapshot for more than 24 to 72 hours.
- Take the snapshot, make the changes to the virtual machine, and delete or commit the snapshot after you verify the virtual machine is working properly. These actions prevent snapshots from growing so large as to cause issues when deleting or committing the snapshots to the original virtual machine disks.

- When taking a snapshot, *do not* save the memory of the virtual machine. The time that the host takes to write the memory to the disk is relative to the amount of memory that the virtual machine is configured to use. Saving the memory can add several minutes to the time taken to complete the operation. If the snapshot is active, saving memory can make calls appear to be active or in progress and can cause confusion to the user. To create a clean snapshot image from which to boot, do the following when you create a snapshot:
  - In the **Take Virtual Machine Snapshot** window, clear the **Snapshot the virtual machine's memory** check box.
  - Select the **Quiesce guest file system (Needs VMware Tools installed)** check box to ensure that all write instructions to the disks are complete. You have a better chance of creating a clean snapshot image from which to boot.
- If you are going to use snapshots for a long time, you must consolidate the snapshot files regularly to improve performance and reduce disk usage. Before merging the snapshot delta disks back into the base disk of the virtual machine, you must first delete stored snapshots.

Note:

If a consolidation failure occurs, end-users can use the actual Consolidate option without opening a service request with VMware. If a commit or delete operation does not merge the snapshot deltas into the base disk of the virtual machine, a warning is displayed in the UI.

Related resources

Title	Link
Best practices for virtual machine snapshots in the VMware environment	Best Practices for virtual machine snapshots in the VMware environment
Understanding virtual machine snapshots in VMware ESXi and ESX	Understanding virtual machine snapshots in VMware ESXi and ESX
Working with snapshots	Working with snapshots
Configuring VMware vCenter Server to send alarms when virtual machines are running from snapshots	Send alarms when virtual machines are running from snapshots
Consolidating snapshots in vSphere 5.x	Consolidating snapshots in vSphere 5.x

VMware vMotion

VMware uses the vMotion technology to migrate a running virtual machine from one physical server to another physical server without incurring downtime. The migration process, also known as a hot migration, migrates running virtual machines with zero downtime, continuous service availability, and complete transaction integrity.

With vMotion, you can:

- Schedule migration to occur at predetermined times and without the presence of an administrator.

- Perform hardware maintenance without scheduled downtime.
- Migrate virtual machines away from failing or under-performing servers.

Before using vMotion, you must:

- Ensure that each host that migrates virtual machines to or from the host uses a licensed vMotion application and the vMotion is enabled.
- Ensure that you have identical vSwitches. You must enable vMotion on these vSwitches.
- Ensure the Port Groups are identical for vMotion.
- Use a dedicated NIC to ensure the best performance.

VMware High Availability

VMware High Availability (HA) is a viable option for recovery of Avaya Diagnostic Server in the VMware environment. If you have configured VMware HA on the ESXi host on which a Avaya Diagnostic Server virtual appliance is installed, failure of this ESXi host results in Avaya Diagnostic Server virtual appliance being moved to a standby ESXi host. After the cold boot of Avaya Diagnostic Server virtual appliance on the standby ESXi host is complete, Avaya Diagnostic Server resumes to provide all the usual features and services.

Keep the following points in mind while configuring to use VMware HA:

- All virtual machines and the configuration files of the virtual machine must be on a shared storage, such as Fibre Channel SAN, iSCSI SAN, or SAN iSCI NAS.
- To have reliable failure detection for HA clusters, the console network must have redundant network paths. The reason is that VMware HA monitors the heartbeat between hosts on the console network for failure detection.
- VMware HA uses the virtual machine priority to decide the order of restart.

Hyperthreading

VMware® recommends that you enable hyperthreading on the ESXi host as hyperthreading can enhance the processor performance. Hyperthreading is enabled by default on the ESXi host. For the procedure to enable hyperthreading, see the VMware® ESXi host documentation.

Appendix B: Password management

Password policies

Adhere to the following rules while you set up a new password:

- The password must be *at least 8 characters long*.
- The passwords must contain:
  - Minimum one English uppercase letter: A, B, C, ... Z
  - Minimum one English lowercase letter: a, b, c, ... z
  - Minimum one numeral: 0, 1, 2, ... 9
  - Minimum one non-alphanumeric special character, such as: ! @ # $ & %
  - Minimum four characters that are different from the previous password

Note:

The root user password expires every 90 days. After the password is expired, reset the password to log in to the system.

Resetting the password of an operating system account

About this task

Use this procedure to reset the password of an operating system account.

Procedure

1. Log on to the virtual appliance through the VMware console or SSH as admin.
2. Use the **su -** command to switch to the root user.
3. Run the following command to reset the password of a specific account:

   `passwd <account_name>`

   When the system prompts, type the new password.
4. Run the following command to reset the password of the root user:

   `passwd`

   When the system prompts, type the new password.

Related links

Password policies on page 81

Resetting the password of the admin user

Procedure

1. Log on to the virtual appliance through the VMware console as root.
2. Run the following command to reset the password of the admin user:

   ```
   passwd admin
   ```

3. When the system prompts, type the new password.

   Henceforth, use the new password to log in as the admin user

Resetting the password of the root user

About this task

If you forget the password of the root user, use this procedure to reset the password.

Procedure

1. Boot the virtual appliance through the VMware console.
2. During the booting process, press **e** within 5 seconds.
3. Select the entry that starts with `linux16`.
4. Edit the line as the following:
   a. Remove `console=ttyS0`
   b. Change `ro` to `rw`
   c. Add `init=/bin/sh`
5. Press **Ctrl+x** and let the booting process continue.
6. Run the following command:

   ```
   passwd
   ```

7. When the system prompts, type the new password.
8. Run the following command to reboot the system and complete the process:

   ```
   #exec /sbin/init 6
   ```

Glossary

AFS	Authentication File System. AFS is an Avaya Web system that allows you to create Authentication Files for secure Avaya Global Services logins for supported non-Communication Manager Systems.
Application	A software solution development by Avaya that includes a guest operating system.
Avaya Appliance	A physical server sold by Avaya running a VMware hypervisor that has several virtual machines, each with its virtualized applications. The servers can be staged with the operating system and application software already installed. Some of the servers are sold as just the server with DVD or software downloads.
Blade	A blade server is a stripped-down server computer with a modular design optimized to minimize the use of physical space and energy. Although many components are removed from blade servers to save space, minimize power consumption and other considerations, the blade still has all of the functional components to be considered a computer.
ESXi	A virtualization layer that runs directly on the server hardware. Also known as a *bare-metal hypervisor.* Provides processor, memory, storage, and networking resources on multiple virtual machines.
Hypervisor	A hypervisor is also known as a Virtual Machine Manager (VMM). A hypervisor is a hardware virtualization technique which runs multiple operating systems on the same shared physical server.
MAC	Media Access Control address. A unique identifier assigned to network interfaces for communication on the physical network segment.
OVA	Open Virtualization Appliance. An OVA contains the virtual machine description, disk images, and a manifest zipped into a single file. The OVA follows the Distributed Management Task Force (DMTF) specification.
PLDS	Product Licensing and Download System. The Avaya PLDS provides product licensing and electronic software download distribution.

Reservation	A reservation specifies the guaranteed minimum required amounts of CPU or memory for a virtual machine.
RFA	Remote Feature Activation. RFA is an Avaya Web system that you use to create Avaya License Files. These files are used to activate software including features, capacities, releases, and offer categories. RFA also creates Authentication Files for secure Avaya Global Services logins for Communication Manager Systems.
SAN	Storage Area Network. A SAN is a dedicated network that provides access to consolidated data storage. SANs are primarily used to make storage devices, such as disk arrays, accessible to servers so that the devices appear as locally attached devices to the operating system.
Snapshot	The state of a virtual appliance configuration at a particular point in time. Creating a snapshot can affect service. Some Avaya virtual appliances have limitations and others have specific instructions for creating snapshots.
Storage vMotion	A VMware feature that migrates virtual machine disk files from one data storage location to another with limited impact to end users.
vCenter Server	An administrative interface from VMware for the entire virtual infrastructure or data center, including VMs, ESXi hosts, deployment profiles, distributed virtual networking, and hardware monitoring.
virtual appliance	A virtual appliance is a single software application bundled with an operating system.
VM	Virtual Machine. Replica of a physical server from an operational perspective. A VM is a software implementation of a machine (for example, a computer) that executes programs similar to a physical machine.
vMotion	A VMware feature that migrates a running virtual machine from one physical server to another with minimal downtime or impact to end users. vMotion cannot be used to move virtual machines from one data center to another.
VMware HA	VMware High Availability. A VMware feature for supporting virtual application failover by migrating the application from one ESXi host to another. Since the entire host fails over, several applications or virtual machines can be involved. The failover is a reboot recovery level which can take several minutes.
vSphere Client	The vSphere Client is a downloadable interface for administering vCenter Server and ESXi.

Index

A

admin user
reset password ... 82
ADS_Response.properties ... 29
automatic restart
virtual machine ... 25
Avaya applications
networking ... 76
Avaya Diagnostic Server
capacity ... 13
migration ... 57
unattended installation ... 27

B

backing up Avaya Diagnostic Server
migration utility ... 60
back up virtual application ... 63
best practices
performance ... 72
BIOS ... 72
BIOS for HP servers ... 73
BIOS settings
for Dell servers ... 73
bundled software specifications ... 13

C

capacity of Avaya Diagnostic Server ... 13
change history ... 7
checklist
Avaya Diagnostic Server 2.5 migration ... 57
deployment procedures ... 17
planning procedures ... 10
Services-VM migration ... 51
software installation ... 27
clones
virtual appliances ... 23
components
virtualized ... 8
VMware ... 8
configure
Avaya Diagnostic Server parameters ... 24
network parameters ... 24
configuring
timing ... 75
virtual machine automatic restart ... 25
creating a snapshot ... 65
customer responsibilities
postinstallation ... 50
customer VMware ... 8

D

database service, slamon
test ... 49
data migration ... 57
deploying clones ... 23
deploying OVA
directly to ESXi ... 22
to vCenter ... 18
deployment
thick ... 77
thin ... 77
deployment procedures
checklist ... 17
document changes ... 7
document purpose ... 7
downloading software
using PLDS ... 14

E

exporting
managed element ... 53

F

FAQ ... 67
field descriptions
properties page ... 21
forgot root password ... 82

G

Gateway UI
testing ... 46

H

high availability ... 80
hyperthreading ... 80

I

importing
managed elements ... 54
input response file ... 29
installing Avaya Diagnostic Server
unattended ... 27
installing service pack
unattended ... 44
Intel Virtualization Technology ... 72
intended audience ... 7

L

license manager 12

M

managed element
exporting from SAL Gateway 53
importing to SAL Gateway 54
managing
licenses 12
migrate from Avaya Diagnostic Server 2.0 virtual appliance 56
migrating
unattended mode 60
migration checklist
Avaya Diagnostic Server 2.5 57
Services-VM 51
migration to another server 57
migration utility
backing up Avaya Diagnostic Server 60

N

networking Avaya applications 76
networking best practices 76
network parameters
configure 24
NTP time source 74

O

os account password
resetting 81
overview 8
backup and restore 63
OVA deployment 17

P

password policies 81
password reset 81
performance best practices 72
planning procedures
checklist 10
PLDS 14
downloading software 14
postinstallation customer responsibilities 50
properties page
field descriptions 21
purpose of document 7

R

recover root password 82
register
register *(continued)*
SAL Gateway 15
registering 14
related documentation 70
requirements
virtual machine resources 11
reset password
admin user 82
os accounts 81
reset root password 82
resource requirements 11
response file 29
restoring
virtual machine 64
restoring a snapshot 65
root user
reset password 82

S

SAL Gateway
register 15
test alarming services 46
SAL Gateway implementation
verify 46
SAL Gateway parameters
configure 24
SAL Gateway virtual appliance
upgrade to Avaya Diagnostic Server virtual appliance 51
server hardware 11
server resources 11
service pack
unattended installation 44
Services-VM migration checklist 51
SLA Mon server implementation
verify 48
slamonsrvr service
test 48
slamonweb service
test 49
snapshot
creating 65
restoring 65
snapshots 78
specifications
bundled software 13
starting virtual machine 24
support 71
supported VMware versions 12

T

test
alarming service 46
slamon database service 49
slamonsrvr service 48
slamonweb service 49

testing
Gateway UI 46
SAL Watchdog service 47
thick deployment 77
thin deployment 77
timekeeping 74
configuring 75

U

upgrade from Avaya Diagnostic Server 2.0 virtual appliance 56
upgrade from SAL Gateway virtual appliance 51
upgrade operation
validating 61

V

validating
upgrade operation 61
verify
SAL Gateway implementation 46
SLA Mon server implementation 48
videos 71
virtual appliance
backup 63
restore 64
Virtualized components 8
Virtualized Environment 8
virtual machine
automatic restart configuration 25
starting 24
virtual machine resource requirements 11
vMotion 79
VMware components 8
VMware software
supported 12
VMware Tools 74
VT support 72

W

WebLM 12